Präsentiert von:

netskope

Security Service Edge (SSE)

für dummies®

Vorbereitung der IT auf die Zukunft der Cloud-Sicherheit

Bereitstellung von CASB, SWG, ZTNA und Firewall auf einer einzigen Plattform

Nutzung von SSE als Teil einer SASE- und Zero-Trust-Architektur

Netskope Sonderausgabe

Jason Clark

Steve Riley

Über Netskope

Netskope ist ein weltweit führendes Unternehmen im Bereich Cybersecurity, das die Themen Cloud-, Daten- und Netzwerksicherheit neu definiert und Unternehmen bei der Anwendung von Zero-Trust-Prinzipien unterstützt. Die Netskope Intelligent Security Service Edge (SSE)-Plattform ist schnell, einfach zu bedienen und schützt Menschen, Geräte und Daten ganz unabhängig von ihrem Standort. Netskope hilft Unternehmen dabei, Risiken zu reduzieren, ihre Effektivität zu erhöhen und einen einmaligen Einblick in alle Cloud-, Web- und privaten Anwendungsaktivitäten zu erhalten. Tausende von Kunden, darunter mehr als 25 der Fortune-100-Unternehmen, vertrauen auf Netskope und sein leistungsstarkes NewEdge-Netzwerk, um Bedrohungen zu minimieren und zur Umsetzung technologischer, organisatorischer und netzwerkbasierter Veränderungen sowie gesetzlicher Anforderungen.

Weitere Informationen über Netskope und den SASE-Ansatz finden Sie unter www.netskope.com.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Security Service Edge (SSE)

für dummies®

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Security Service Edge (SSE)

Netskope Sonderausgabe

Jason Clark und Steve Riley

für dummies®

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Secure Service Edge (SSE) für Dummies®, Sonderausgabe von Netskope

Veröffentlicht von
John Wiley & Sons, Inc.
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

Copyright © 2022 John Wiley & Sons, Inc., Hoboken, New Jersey

Kein Teil dieser Publikation darf ohne die vorherige schriftliche Genehmigung des Verlags elektronisch oder mechanisch, in Form einer Fotokopie, Aufnahme, durch Scannen oder anderweitig reproduziert, auf einem Datenträger gespeichert oder übertragen werden, es sei denn, dies ist unter Abschnitt 107 oder 108 des US-amerikanischen Urheberrechts (Copyright Act von 1976) zulässig. Genehmigungsanfragen an den Verlag sind an die Abteilung für Rechte und Lizenzen zu richten: Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, Fax (201) 748-6008 oder online unter http://www.wiley.com/go/permissions.

Marken: Wiley, die Bezeichnung „Für Dummies", das Dummies-Mann-Logo, The Dummies Way, Dummies.com, Making Everything Easier und darauf bezogene Gestaltungen sind Marken oder eingetragene Marken von John Wiley & Sons, Inc. und/oder seiner Tochtergesellschaften in den Vereinigten Staaten oder anderen Ländern und dürfen nicht ohne schriftliche Genehmigung verwendet werden. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber. John Wiley & Sons, Inc. steht mit keinem in diesem Buch genannten Produkt oder Anbieter in Beziehung.

HAFTUNGSBESCHRÄNKUNG/GEWÄHRLEISTUNGSAUSSCHLUSS: DER VERLAG UND DIE AUTOREN GEBEN KEINE ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN IN BEZUG AUF DIE INHALTLICHE RICHTIGKEIT UND VOLLSTÄNDIGKEIT DIESES WERKES UND LEHNEN AUSDRÜCKLICH ALLE GEWÄHRLEISTUNGEN AB, INSBESONDERE IMPLIZIERTE GEWÄHRLEISTUNGEN HINSICHTLICH DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. GEWÄHRLEISTUNGEN KÖNNEN NICHT DURCH VERKAUFSVERTRETER, SCHRIFTLICHES VERKAUFSMATERIAL ODER WERBEAUSSAGEN FÜR DIESES WERK GESCHAFFEN ODER VERLÄNGERT WERDEN. DIE TATSACHE, DASS IN DIESEM WERK AUF EINE ORGANISATION, EINE INTERNETSEITE ODER EIN PRODUKT IN FORM EINES ZITATS UND/ODER EINER MÖGLICHEN QUELLE FÜR WEITERE INFORMATIONEN BEZUG GENOMMEN WIRD, BEDEUTET NICHT, DASS DER VERLAG UND DIE AUTOREN DEN VON DIESER ORGANISATION ODER DEN AUF DIESER INTERNETSEITE ODER VON DIESEM PRODUKT ZUR VERFÜGUNG GESTELLTEN INFORMATIONEN ODER SERVICES BZW. DEN VON IHNEN GEGEBENEN EMPFEHLUNGEN ZUSTIMMT. DIESES WERK WIRD MIT DEM AUSDRÜCKLICHEN HINWEIS VERKAUFT, DASS DER VERLAG KEINE PROFESSIONELLEN DIENSTLEISTUNGEN ERBRINGT. DIE HIERIN ENTHALTENEN EMPFEHLUNGEN UND STRATEGIEN SIND UNTER UMSTÄNDEN NICHT FÜR IHRE SITUATION GEEIGNET. GEGEBENENFALLS SOLLTE DIE HILFE EINES PROFESSIONELLEN DIENSTLEISTERS IN ANSPRUCH GENOMMEN WERDEN. AUSSERDEM SOLLTE DER LESER BEDENKEN, DASS SICH DIE IN DIESEM WERK AUFGEFÜHRTEN INTERNETSEITEN IN DEM ZEITRAUM ZWISCHEN DER ENTSTEHUNG DIESES WERKES UND DEM ZEITPUNKT DES LESENS MÖGLICHERWEISE GEÄNDERT HABEN ODER NICHT MEHR EXISTIEREN. WEDER DER VERLAG NOCH DIE AUTOREN HAFTEN FÜR HIERAUS ENTSTEHENDE SCHÄDEN, ENTGANGENENE GEWINNE ODER ANDERE KOMMERZIELLE SCHÄDEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SONDER-, NEBEN-, FOLGE- ODER ANDERE SCHÄDEN.

Allgemeine Informationen zu unseren sonstigen Produkten und Services oder zur Erstellung eines individuellen *Für Dummies*-Buches für Ihr Unternehmen oder Ihre Organisation erhalten Sie von unserer Abteilung Business Development in den USA telefonisch unter Tel. 877-409-4177 oder per E-Mail unter info@dummies.biz. Alternativ können Sie uns auch auf www.wiley.com/go/custompub besuchen. Für Informationen zur Lizenzierung der *Für Dummies*-Marke für Produkte oder Services kontaktieren Sie bitte BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-89723-1 (pbk); ISBN 978-1-119-89724-8 (ebk)

Danksagung des Verlags

Die folgenden Personen haben dabei geholfen, dieses Buch auf den Markt zu bringen:

Project Editor: Elizabeth Kuball

Acquisitions Editor: Ashley Coffey

Senior Managing Editor: Rev Mengle

Business Development Representative: Jeremith Coward

Production Editor: Tamilmani Varadharaj

Besondere Unterstützung: Nicole Sholly

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Inhaltsverzeichnis

EINFÜHRUNG 1
Über dieses Buch 1
Dumme Annahmen 2
In diesem Buch verwendete Symbole 2
Zusätzliche Informationen 2

KAPITEL 1: **Neue Herausforderungen benötigen einen neuen Sicherheitsansatz** 3
Wohin sich die Sicherheit entwickelt 3
Die Transformation der Sicherheit 6
Auf dem Weg zu himmlischer Sicherheit 7

KAPITEL 2: **Wie das herkömmliche Sicherheitsmodell von der Cloud verdrängt wurde** 9
Als die Firewall noch über die Sicherheit herrschte 10
Wie Unternehmen von der Cloud profitieren 11
Einzelprodukte sind keine Lösung für komplexe Probleme 12
Integrierte Sicherheit ist unverzichtbar 13
Die Sicherheit muss den Daten folgen 14
SSE: Die Sicherheitsanforderungen auf der SASE-Reise 15
Wir brauchen Sicherheit für die Zukunft, nicht für die Vergangenheit 16

KAPITEL 3: **Security Service Edge: Die Zukunft der Cloud-basierten Sicherheit** 17
Warum wir SSE brauchen 18
Wie SSE Sicherheitsdienste zusammenbringt 20
Die saubere Analyse komplexer Daten 21
Gemeinsam genutzte Dienste 21
SSE: Wesentliche Vorteile 22
Die Möglichkeiten von SSE: bald auch für Ihr Sicherheitsteam! 24
Verbesserte Klassifizierung zur Unterstützung von DLP 24
Security Posture Management für die Cloud und SaaS 25
Erkennung und Neutralisierung von Bedrohungen 25
Digital Experience Management (DEM) 26
Auch Netzwerke müssen sich weiterentwickeln 26
Vorteile der SSE-Sicherheit 28

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

KAPITEL 4: **Wie SASE mit Zero Trust erfolgreich realisiert werden kann** 29
Von Zero Trust zum kontinuierlichen adaptiven Vertrauen 30
Vier einfache Schritte auf dem Weg zu SSE 33
Schritt 1: Migration mobiler Mitarbeiter, um mehr Transparenz zu erhalten 33
Schritt 2: Migration aller übrigen Mitarbeiter und unternehmensweite Datenklassifizierung 34
Schritt 3: Implementierung von kontinuierlichem adaptiven Vertrauen und erweiterten Diensten 35
Schritt 4: Proaktives Risikomanagement mit dynamischer Analyse und Risikoeinstufung 36
Netzwerktransformation und andere Sicherheitsbereiche 36
Die Vorteile von SSE für Ihr Geschäft 38

KAPITEL 5: **Ungefähr 10 do's & don'ts, die wir Ihnen auf dem Weg zu SSE mitgeben möchten** 39
Stellen Sie die Daten in den Mittelpunkt 40
Nutzen Sie die Vorteile der Integration 40
Denken Sie daran, dass auch Angreifer in die Cloud wandern 40
Machen Sie Sicherheit zu einem wichtigen Teil der Unternehmensstrategie 41
Vermeiden Sie Silodenken 41
Übernehmen Sie keine alten Regeln 42
Unterschätzen Sie das Rechenzentrum nicht 42
Haben Sie keine Angst vor Veränderungen 42

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Einführung

Selbst Experten konnten bis vor Kurzem nicht vorhersehen, wie schnell viele Unternehmen den Wechsel in die Cloud vollziehen würden. Aufgrund dieser unerwarteten Geschwindigkeit sind die meisten von ihnen weiterhin auf Sicherheitsplattformen angewiesen, die in einer Zeit entwickelt wurden, in der das On-Premises-Rechenzentrum noch den Ton angab. Die Corona-Pandemie hat diese Entwicklung noch beschleunigt und Unternehmen mit zusätzlichen Herausforderungen konfrontiert. CISOs stehen unter zunehmendem Druck, Mitarbeiter im Homeoffice zu schützen, von denen viele auch in Zukunft nicht mehr täglich ins Büro kommen werden.

Doch es gibt auch eine gute Nachricht. Secure Access Service Edge (SASE) ist ein technologischer Rahmen, der den Weg für eine Cloud-basierte Sicherheitsarchitektur ebnet, mit der Unternehmen ihre Mitarbeiter an jedem Ort effektiv schützen können. Security Service Edge (SSE) ist die Kombination der wichtigsten Sicherheitsdienste innerhalb einer SASE-Architektur. SSE stellt die erforderlichen Funktionen für die Implementierung von Sicherheitsdiensten zur Verfügung, die Unternehmen zum Schutz von Mitarbeitern an Remote-Standorten, von Cloud-basierter Technologie und von bestehenden On-Premises-Infrastrukturen und Anwendungen benötigen.

SASE ist ein Rahmenwerk. SSE ist eine Reihe von Diensten, die sich Unternehmen heute zunutze machen können. In diesem Buch erklären wir, was SSE ist, und betrachten die Grundlagen dieses Ansatzes, der innovative Konzepte wie Zero Trust, adaptive kontextbasierte Sicherheit und neue Netzwerkarchitekturen beinhaltet. Außerdem zeigen wir Ihnen, wie bekannte Dienste im Rahmen von SSE mit neuen, fortschrittlichen Technologien kombiniert werden, die das Sicherheitsniveau erheblich verbessern können.

Über dieses Buch

Es ist an der Zeit, die Sicherheitslandschaft zu modernisieren. IT-Sicherheitskräfte und andere Mitarbeiter, die sich mit SSE vertraut machen, bereiten sich damit auf die Umgestaltung der Unternehmenssicherheit vor und tragen dazu bei, dass sich Security von einem Engpass zu einem Enabler der digitalen Transformation entwickelt. Dieses Buch erläutert die Grundlagen von SASE und SSE und bietet eine Roadmap, die Ihnen dabei helfen soll, dieser neuen Sicherheit das Beste abzugewinnen. Um die Vorteile der Cloud voll ausschöpfen zu können,

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

müssen Unternehmen ihre Sicherheit von Grund auf umgestalten. Dieses Buch soll Ihnen dabei helfen, sich auf diesen Prozess vorzubereiten.

Dumme Annahmen

Sie sind mit Internet und dem Thema Sicherheit vertraut und wissen, dass das herkömmliche Sicherheitsmodell zunehmend an seine Grenzen stößt. Ihnen ist außerdem bekannt, dass die Cloud trotz ihres produktivitätssteigernden Potenzials ein gefährlicher Ort ist, an dem Zugangsinformationen gestohlen werden können und die Daten von Privatpersonen und Unternehmen nicht immer ausreichend geschützt sind. Es liegt in Ihrem Interesse, diese Situation für Ihr Unternehmen, Ihre Mitarbeiter, Aktionäre, Kunden und Geschäftspartner zu verbessern und die von SASE und SSE gebotenen Möglichkeiten zu nutzen.

In diesem Buch verwendete Symbole

In diesem Buch werden verschiedene Symbole verwendet, um auf wichtige Informationen aufmerksam zu machen.

TIPP

Das Tipp-Symbol weist auf Empfehlungen und andere Informationen hin, die Ihnen das Leben leichter machen können.

ERINNERN

Das Erinnerungssymbol hebt besonders wichtige Fakten hervor.

WARNUNG

Bitte beachten Sie alles, was mit dem Warnsymbol gekennzeichnet ist, um sich unnötige Kopfschmerzen zu ersparen.

Zusätzliche Informationen

Weitere Informationen über Lösungen von Netskope finden Sie unter www.netskope.com Wenn Sie sich ausführlicher mit dem Thema Security Service Edge (SSE) befassen möchten, besuchen Sie bitte `www.netskope.com/security-defined/security-service-edge-sse`.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- Erforschen wir die Zukunft der Security
- Lernen wir, wie sich der digitale Wandel auf die Sicherheit auswirkt
- Entdecken wir, wie man eine sorgenfreie Sicherheit erreichen kann

Kapitel 1
Neue Herausforderungen benötigen einen neuen Sicherheitsansatz

Unternehmen wechseln zu Cloud-Anwendungen, um von den deutlichen Vorteilen der Cloud wie Geschwindigkeit, Effizienz und Transparenz zu profitieren. Um Daten, Menschen und Anwendungen in der Cloud wirklich zu schützen, kann die Sicherheit nicht mehr aus einfachen Entscheidungen wie „akzeptieren“ oder „ablehnen“ bestehen und sich vor allem auf den Schutz des Unternehmensperimeters konzentrieren. Dieser Ansatz stammt noch aus der Zeit, als das Netzwerk höchste Priorität hatte und sich die meisten Mitarbeiter an einem Ort befanden. Die Security muss intelligenter werden und detaillierten Kontext nutzen, um genau den richtigen Schutz für Ihr Unternehmen zu entwickeln, unabhängig davon, wo sich Ihre Mitarbeiter befinden. Sicherheit muss jederzeit den Daten folgen und sie muss einfach anzuwenden sein, damit sie den Geschäftsbetrieb nicht verlangsamt.

Wohin sich die Sicherheit entwickelt

Jetzt ist ein guter Zeitpunkt, um sich mit dem Thema Sicherheit zu befassen. Die Leistungsfähigkeit und Qualität der Cyber-Sicherheitstechnologie machen derzeit enorme Fortschritte. Noch nie mussten sich Sicherheitsexperten so schnell mit so vielen Veränderungen

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

auseinandersetzen. Und noch nie hatten sie eine so gute Gelegenheit wie jetzt, Sicherheit zu einem strategischen Businessfaktor umzugestalten. Daten, Anwendungen und Mitarbeiter sind in die Cloud gewandert - die Sicherheit muss folgen.

Unternehmen, die eine Cloud-basierte Sicherheitsstrategie einführen, um die digitale Transformation zu ermöglichen, werden schneller und sicherer Innovationen hervorbringen als Unternehmen, deren Sicherheitsstrategie in den Ideen von gestern verwurzelt ist. Wir stehen vor einer neuen Ära, in der Sicherheitsexperten den Angreifern endlich einen Schritt voraus sind und ihre Unternehmen unterstützen, wenn die Cloud-basierte digitale Transformation auf Hochtouren läuft.

Bestehende Sicherheitssysteme in die Cloud zu verlagern ist aufwändig und bringt oftmals nicht den gewünschten Erfolg. Durch den Secure Access Service Edge (SASE)-Ansatz verändert sich die Sicherheit, um dem Cloud-basierten, hybriden Arbeitsplatz gerecht zu werden.

WARNUNG

Die Best-of-Breed-Sicherheitsprodukte und -Dienstleistungen der Vergangenheit sind in der Cloud zum Scheitern verurteilt. Ebenso wenig funktioniert es, alte Sicherheitstechnologien nachzurüsten und als „Cloud-fähig" zu bezeichnen.

Anbieter von Sicherheitstechnologien bringen neue Cloud-native Produkte und Dienste auf den Markt, die Schutz bieten, wenn Daten gespeichert und Anwendungen auf einer Infrastruktur ausgeführt werden, die Unternehmen nicht selbst kontrollieren. Neue Sicherheitstechnologien müssen nicht nur den *Zugang* zu Daten schützen, sondern auch die *Nutzung* dieser Daten.

Es ist hilfreich, die Cloud-fähige Sicherheit anhand von vier grundlegenden Ideen zu betrachten:

- **SASE** ist der Rahmen für die Implementierung einer Cloud-basierten, konvergierten Infrastruktur für Netzwerk- und Sicherheitsfunktionen. SASE kombiniert dabei Konzepte wie Zero Trust, SD-WAN und Security Service Edge (SSE). Dies führt zu einer neuen Sicherheits- und Netzwerkstrategie, die die Cloud und die neue Work-from-anywhere-Umgebung schützt und steuert. Experten stimmen darin überein, dass diese neue Architektur umfassende Sicherheit für eine Cloud-zentrierte Welt bietet. (Eine vollständige Einführung finden Sie in unserem *Designing a SASE Architecture For Dummies*).
- **SSE** bedeutet, dass alle für SASE erforderlichen Sicherheitskomponenten, die zuvor aus separaten Anwendungen, Produkten oder Diensten von verschiedenen Anbietern bestanden, in einer

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

einheitlichen, integrierten Plattform zusammengeführt werden. Dies ermöglicht mehr Funktionen und größere Effizienz, während gleichzeitig die Komplexität und Kosten reduziert werden. SSE steht für tief integrierte Sicherheitsfunktionen, die sich wechselseitig erkennen und ergänzen, gut zusammenarbeiten und von einem einzigen Anbieter bezogen werden. SSE definiert darüber hinaus eine Reihe von erweiterten Fähigkeiten, die wir als „echtes SSE" bezeichnen (siehe Kapitel 3).

- Der **User-Kontext** bestimmt, wie die integrierten Sicherheitsfunktionen von SSE als Kontrollmechanismus eingesetzt werden, um Daten, Anwendungen und Personen jederzeit zu schützen. Der Kontext ermöglicht ein tiefes Verständnis dafür, *wer* die Person ist, *was* sie zu tun versucht und *warum* sie es versucht, ebenso wann und und wie. Er erlaubt zudem die Anwendung adaptiver Sicherheitsrichtlinien zur Risikominderung in Echtzeit. Früher waren „erlauben" und „blockieren" die einzigen Optionen. Jetzt unterstützt umfangreicher Kontext Abstufungen in der Zugriffskontrolle, wie z. B. „erlauben unter Bedingungen", um Sicherheit zu bieten, ohne dabei die Produktivität zu beeinträchtigen. Die Qualität und der Umfang des Kontexts ist ein entscheidendes Unterscheidungsmerkmal zwischen den einzelnen Sicherheitsanbietern.
- **Zero-Trust** unterscheidet echte adaptive Sicherheit von einer einfachen bedingten Authentifizierung auf der Grundlage von Vertrauen. Das Ziel besteht nicht nur darin, jeder Person genau den Zugang und die Berechtigung zu gewähren, die sie zur Ausführung einer bestimmten Aufgabe benötigt – entsprechend dem Vertrauensniveau, das sich aus einer Echtzeitbewertung der Identität des Mitarbeiters und der Zugangsmethode ergibt. Adaptiver Zugang erfordert Einblicke in das, was *nach* dem Login passiert: Informationen über die Umgebung, die im Laufe der Zeit variieren, bisheriges und aktuelles Verhalten sowie die Eigenschaften der Daten selbst. Bei Netskope betrachten wir Zero Trust als Einstiegspunkt (kein Vertrauen zu Beginn jeder Interaktion) und streben das Ziel eines *kontinuierlichen, adaptiven Vertrauens* an, bei dem das Maß des Vertrauens den Informationen, die wir aus der Umgebung erhalten, entsprechen.

Dieses Buch erklärt, wie diese Konzepte in einem effektiv implementierten SSE zusammenfließen und eine sorgenfreie Sicherheit ermöglichen (siehe Kapitel 3). Unternehmen profitieren endlich von Cloud-basierter Sicherheit mit allem, was nötig ist, um in einer Cloud-zentrierte Welt Daten und Anwendungen zu schützen, auf die Mitarbeiter zugreifen, die weiterhin verteilt oder nicht ab einem zentralen Bürostandort arbeiten.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Die Transformation der Sicherheit

Die explosionsartige Entwicklung in verschiedenen Bereichen der digitalen Transformation verändert die Geschäftswelt nachhaltig. Dabei ist die Sicherheitstransformation entscheidend für den Erfolg des digitalen Wandels.

ERINNERN

Technologien wie die Cloud, das Internet of Things (IoT), Machine Learning/Künstliche Intelligenz (ML/KI) und Analytik tragen erheblich zur Verbesserung der Geschäftsergebnisse bei. Wenn die Sicherheit mit dieser Entwicklung nicht mithalten kann, ist der Fortschritt gefährdet.

- **Die Datenexplosion:** Die Analysten von IDC gehen davon aus, dass bis 2025 weltweit 175 Zettabytes (ZB) an Daten anfallen werden. Dies entspricht einer Steigerung um das 25-fache seit 2010. Angreifer stehlen Daten für ihre Zwecke: um sie zu verkaufen, böswillig zu verändern oder Lösegeld zu fordern. Die Netskope Threat Labs haben herausgefunden, dass die Cloud bei Cyberkriminellen immer beliebter wird: 2021 wurden 68 Prozent der Malware über die Cloud verbreitet (im Gegensatz zu weniger als der Hälfte im Jahr 2020). Die explosionsartige Zunahme von Daten, auf die über die Cloud zugegriffen wird, schafft mehr Ziele für Angreifer und größere Herausforderungen für die Sicherheitsverantwortlichen.
- **Die Cloud-Explosion:** Unternehmen nutzen Cloud-basierte Infrastrukturen und Anwendungen, um Geschwindigkeit, Flexibilität und Agilität zu gewinnen. Laut Netskope Threat Labs nutzt ein durchschnittliches Unternehmen mittlerweile mehr als 800 verschiedene Software-as-a-Service (SaaS)-Anwendungen. 97 Prozent davon sind so genannte „Schatten-IT", d. h. sie werden nicht von der internen IT-Abteilung verwaltet und sind in vielen Fällen für diese auch nicht sichtbar. Außerdem sind die Standard-Sicherheitseinstellungen vieler Cloud-Anwendungen sehr offen – ein weiterer Grund, warum die Cloud für Angreifer ein besonders interessantes Ziel ist.
- **Die Geräteexplosion:** Die Schätzungen über die Anzahl der mit dem Internet verbundenen Geräte gehen weit auseinander und reichen von 25 Milliarden im Jahr 2030 bis zu 75 Milliarden im Jahr 2025. Mehr Geräte und mehr Konnektivität schaffen einen größeren Technologiebestand – und eine größere Angriffsfläche. Gleichzeitig führt die Geräteexplosion oft zu beschleunigter Innovation.

ERINNERN

Bei der Sicherheitstransformation geht es darum, einen neuen Weg zu finden, mit all diesen Entwicklungen umzugehen, damit Unternehmen erfolgreich weiter arbeiten können.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Unternehmen, die es versäumen, die Cloud-basierte Sicherheitstransformation umzusetzen, sind einem wachsenden Risiko ausgesetzt. Die derzeitige Sicherheitslandschaft ist zu komplex geworden und kostet die Unternehmen hohe Summen an Kapitalausgaben (CapEx), Betriebsausgaben (OpEx) und Arbeitsstunden, während gleichzeitig die Effizienz sinkt. Sicherheitsanbieter müssen daher Funktionen in Systeme umwandeln, die zusammenarbeiten..

Auf dem Weg zu himmlischer Sicherheit

Um eine ganzheitliche Sicherheitsstrategie umzusetzen, sollten sich Unternehmen von praktischen Ratschlägen und Erfahrungen leiten lassen und nicht bloß Marketingversprechen oder Hypes folgen.

Im Großen und Ganzen läuft dieser Übergang wie folgt ab:

1. **Umgestaltung des Netzwerks.**

   Das Netzwerk muss Daten so effizient wie möglich zwischen allen Punkten einschließlich Cloud-Diensten und Rechenzentrum übertragen, ohne dass Leistung und Benutzerfreundlichkeit gegen Sicherheit eingetauscht werden. Der Datenverkehr wird durch ein Netzwerk geleitet, das für SSE entwickelt wurde und aus weltweit verteilten Points of Presence (PoPs) besteht. Die Mitarbeiter im Büro, zu Hause oder im Café erhalten ein hohes Maß an Sicherheit und Leistung, während die Unternehmensdaten geschützt bleiben.

2. **Konsolidierung der Security.**

   Eine umfassende SSE-Suite eines einzigen Anbieters ersetzt den Flickenteppich älterer Sicherheitsanwendungen. Zusammengeführte Funktionen vereinfachen die Verwaltung und Administration, gewährleisten eine konsistente Durchsetzung der Richtlinien und optimieren die Verarbeitung des Datenverkehrs.

3. **Ausweitung der SSE-Nutzung und Implementierung erweiterter Security Services.**

   Mit SSE können Sicherheitsteams leistungsstarke Funktionen wie Remote Browser Isolation (RBI), Cloud Security Posture Management (CSPM) und SaaS Security Posture Management (SSPM) einführen. Erweiterte Funktionen wie Data Loss Prevention (DLP) und Advanced Threat Protection (ATP) funktionieren besser als in alten Modellen, die durch mangelnde Integration und eingeschränkte Transparenz geprägt sind.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

4. **Schutz der Daten in der Cloud und auf den Geräten.**

   Der SSE-Anbieter sollte auch eine Firewall als Service (FWaaS) bereitstellen, um Cloud-basierte Anwendungen, unternehmenseigene Geräte und Daten-Repositories zu schützen.

5. **Das Rechenzentrum wird zu einem Ziel unter vielen.**

   Das traditionelle Rechenzentrum des Unternehmens, das früher der einzige Punkt war, über den der gesamte Datenverkehr geleitet wurde, wird zu einem weiteren Ziel, zu dem und von dem SSE den Datenverkehr leitet. Die Beseitigung von Hairpinning, also der Leitung des gesamten Traffics über das Rechenzentrum, senkt die Kosten, reduziert die Komplexität und erhöht die Leistung.

6. **Anwendung der Zero-Trust-Prinzipien, um einen Zustand des kontinuierlichen, adaptiven Vertrauens zu erreichen.**

   Da SSE den Datenverkehr nach der Gewährung des Zugriffs ständig überwacht, können Sicherheitsverantwortliche eine gründliche kontextbezogene Analyse der Session durchführen, Entscheidungen auf der Grundlage von Risikoinformationen Dritter treffen, Änderungen im Risikoprofil erkennen und gefährliche Aktionen unterbinden. Zudem können durch entsprechende Benachrichtigungen Mitarbeiter dazu angehalten werden, ihre Sicherheitsgewohnheiten zu verbessern.

7. **Verbessertes Risikomanagement im gesamten Unternehmen durch mehr Transparenz.**

   Die Möglichkeit, die Aktivitäten aller Mitarbeiter des Unternehmens zu sehen, zu steuern und zu kontrollieren, verbessert das Risikobewusstsein und die Risikoerkennung erheblich. Das Sicherheitsteam kann sich auf Hochrisikobereiche konzentrieren und schneller neue Richtlinien im SSE einführen, um Risiken zu reduzieren. Sicherheitsverantwortliche können zur Geschäftsstrategie beitragen und bei Unternehmensentscheidungen eine stärkere Rolle einnehmen..

Die Sicherheitstransformation ist eine große Herausforderung. Kapitel 4 zeigt, wie die Zero-Trust-Prinzipien einen schrittweisen Übergang zur vollständigen Implementierung von Cloud-basierter Sicherheit ermöglichen. Kapitel 5 beleuchtet häufige Fehler sowie Erfolgsfaktoren und beschreibt einen exemplarischen Weg, den viele Unternehmen einschlagen werden, wenn sie SSE, Zero Trust und letztlich SASE auf die richtige Weise angehen.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- Betrachten wir die Geschichte der Firewall
- Erfahren wir, warum uns die Cloud erhalten bleiben wird
- Weisen wir auf die Einschränkungen von Einzelprodukten hin
- Erklären wir, warum Sicherheit integriert sein sollte und den Daten folgen muss
- Zeigen wir, wie SSE die neuen Sicherheitsanforderungen erfüllen kann

Kapitel 2
Wie das herkömmliche Sicherheitsmodell von der Cloud verdrängt wurde

Vor einem Jahrzehnt konnten nur wenige Führungskräfte vorhersehen, wie schnell sich die Cloud in der Unternehmenswelt durchsetzen würde. Laut Netskope Threat Labs abonnieren Unternehmen heute im Durchschnitt mehr als 800 Software-as-a-Service (SaaS)-Anwendungen.

Cloud- und Edge-Computing verdrängen immer mehr geschäftliche Workloads aus dem Rechenzentrum. Die Corona-Pandemie hat „Work-from-anywhere“ - den Trend zum flexiblen und mobilen Arbeiten - erheblich beschleunigt. Immer mehr Menschen, Geräte, Anwendungen, Dienste und Daten verlassen die Grenzen des klassischen Rechenzentrums. Die Cloud ist heute für Produktivität des Unternehmens von entscheidender Bedeutung. Sie bringt aber auch neue Risiken mit sich und erfordert daher einen überarbeiteten Sicherheitsansatz.

Rufen Sie sich kurz all die Dinge ins Gedächtnis, die Eltern zum Schutz ihrer Kinder tun. Sie bringen Kindersicherungen an Treppen, Steckdosen und Schränken an und sichern den Innenbereich durch eine

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Alarmanlage, die ausgelöst wird, sobald ein Kind versucht, Türen oder Fenster zu öffnen. Der Außenbereich wird durch einen Zaun geschützt. Natürlich wollen Eltern ihre Kinder auch später so gut es geht schützen, wenn sie in den Kindergarten, zur Schule und schließlich zur Uni gehen, doch ihre Rolle als Eltern ändert sich in jeder Phase.

So ähnlich verhält es sich mit der Sicherheit in der Cloud. Das Ziel selbst – der Schutz von Daten, Anwendungen und Menschen – ändert sich nicht. Die zu schützenden Daten, Anwendungen und Personen haben jedoch das „Haus" verlassen und die Firewall spielt nun eine weniger wichtige Rolle. Inzwischen befinden sich die am schnellsten wachsenden Bedrohungen in der Cloud, nicht im Rechenzentrum. Das Ergebnis: Die Sicherheitstaktiken müssen sich ändern.

Als die Firewall noch über die Sicherheit herrschte

Früher war die Firewall der wichtigste zentrale Sicherheitskontrollpunkt und wahrscheinlich auch der größte Posten im Sicherheitsbudget der meisten Unternehmen. Bei der Gestaltung von Netzwerk- und Sicherheitsarchitekturen stand das Rechenzentrum im Mittelpunkt und war von einem klar definierten Perimeter umgeben. Sicherheit bedeutete, das Netzwerk zu sichern.

Vor dem Siegeszug der Cloud war dieser Ansatz sinnvoll. Schließlich war das Rechenzentrum der einzige Ort, an dem Unternehmen ihre wertvollen digitalen Ressourcen verwahrten. Das Rechenzentrum war wie ein gut bewachtes Schloss, um das sich ein (meist) undurchdringlicher Schutzwall zog. Der Zugang zu diesem Schloss wurde durch ein mächtiges Tor aus Sicherheitsgeräten eingeschränkt. Wie die Eltern, die Alarmanlagen an Türen und Fenstern anbringen, hatte das Unternehmen vor dem Einzug der Cloud weitreichende Kontrolle über seine Sicherheit.

Mitarbeiter nutzten ein exklusives, privates Netzwerk, das sie mit den Ressourcen verband, die sie für ihre Arbeit benötigten. Wer in einer entfernten Zweigstelle oder remote arbeitete, musste lediglich den Alarmcode eingeben, um Zugriff auf die internen Anwendungen und Daten in diesem privaten Netzwerk zu erhalten, und hatte darüber hinaus Zugang zu allen externen verbundenen Zielorten. Der Datenverkehr von Remote-Mitarbeitern musste allerdings immer mittels Backhauling durch dieses zentrale Rechenzentrum innerhalb des Perimeters geleitet werden. Dies verursachte nicht nur hohe Kosten und Komplexität, sondern beeinträchtigte auch die Leistung.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Die durch Firewalls bereitgestellte Sicherheit der alten Schule bestand einfach darin, einer Person den Zugriff entweder zu erlauben oder zu verweigern. Wurde einer Person erst einmal Zugriff gewährt, ging man davon aus, dass tatsächlich *sie* anwesend war und keine bösen Absichten verfolgte. Als Teil der Perimeter-basierten Sicherheit führten viele Unternehmen Sicherheitssysteme zur Abwehr bestimmter Bedrohungen oder Bedrohungskategorien ein. Sobald eine neue Bedrohung erkannt wurde, kaufte man mehr Ausrüstung. Beim On-Premises-Modell nutzen Unternehmen nicht selten zehn oder mehr über ein Kabel miteinander verbundene Sicherheitsprodukte.

Jedes dieser Produkte führte seine eigenen Prüfungen durch und stellte quasi seine eigenen Fragen. Das kann man sich in etwa so vorstellen: „Hallo, ich will Malware erkennen ... Ich will Signaturen vergleichen und Eindringlinge blockieren ... Ich will E-Mails filtern oder nach sensiblen Daten scannen ... Ich will vor Angriffen mit Namensauflösung schützen ... Ich will Port- und Protokollsperren mit Zugriffskontrolllisten bereitstellen.“ Nachdem eine Funktion ihre jeweilige Aufgabe erledigt hatte, leitete sie Pakete an die nächste Funktion weiter, was zu zusätzlichen Latenzzeiten und einer größeren Komplexität führte.

Die Cloud hat all das verändert.

Wie Unternehmen von der Cloud profitieren

Es gibt kein Zurück mehr: Die meisten Unternehmen wollen auf Cloud Computing nicht mehr verzichten, da dieses Modell eine nahezu grenzenlose Flexibilität und eine Vielzahl geschäftlicher Vorteile bietet. Trends wie “Cloud Repatriation”, also die „Rückführung“ von Daten und Anwendungen in das unternehmenseigene Rechenzentrum, werden sich mit Sicherheit nicht durchsetzen - höchstens in einigen sehr seltenen Szenarien. Die Cloud ist für CEOs, CFOs, CIOs und Unternehmen attraktiv, weil der Großteil der Infrastruktur standardisiert und schlüsselfertig ist. Unternehmen, die die Cloud nutzen, müssen nicht mehr viel Zeit und Geld in ihre eigene Infrastruktur investieren. Sie können einfach einen Cloud-Dienst abonnieren und ihn an ihre individuellen Geschäftsanforderungen anpassen. Für Unternehmen, die ihre Umsatzgenerierung steigern und profitabler werden wollen, ist der Wechsel zur Cloud ein unverzichtbarer Schritt.

Die Cloud ist auch für Mitarbeiter attraktiv. Sie können nun SaaS-Anwendungen nutzen, die moderne und oft sehr attraktive Plattformen für die Zusammenarbeit, Kommunikation, Finanzverwaltung, den

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Verkaufsabschluss und die Verwaltung von Kundenbeziehungen bieten. Diese von Drittanbietern zur Verfügung gestellten Anwendungen in der Cloud sind besser, schneller und effektiver als alles, was die alten, umständlichen Unternehmensanwendungen hinter den starren Grenzen des Rechenzentrums bieten konnten.

Doch genau hier liegt der Haken – und die Gefahr: Die meisten dieser Cloud-Anwendungen werden nicht von der IT-Abteilung des Unternehmens genehmigt und kontrolliert – und sind daher alles andere als sicher. Zwar müssen Sie nach wie vor in der Lage sein, Ihr Unternehmen zu schützen, doch es fehlt Ihnen nun an der dazu erforderlichen Kontrolle. Und hier kommen wir wieder zum Beispiel der Eltern zurück. Die Einführung der Cloud verlangt, dass Sie Ihre „Kinder" an einen anderen Ort schicken – in die Schule oder an die Uni. Dort können Sie sie nicht mehr sehen und wissen nicht, was sie tun.

Im Zeitalter der Cloud ist die Firewall nicht mehr die wichtigste Sicherheitseinrichtung, da sie Ihr Unternehmen nicht umfassend vor Bedrohungen in der Cloud schützen kann. Ohne angemessene Security-Lösungen, die digitale Prozesse, Mitarbeiter, Kunden und Vermögenswerte in dieser neuen, weit offenen Landschaft zuverlässig schützen können, ist es sehr riskant, mit der Umsetzung der digitalen Transformation zu beginnen. Im Zeitalter der Cloud muss Security das Unternehmen dabei unterstützen, den geschäftlichen Nutzen der Cloud zu realisieren und gleichzeitig seine ebenfalls durch die Cloud geschaffene größere Anfälligkeit für Bedrohungen zu verwalten.

Einzelprodukte sind keine Lösung für komplexe Probleme

Immer mehr Arbeitskräfte arbeiten heute außerhalb des Büros und viele Unternehmen haben ihre Daten und Anwendungen in die Cloud verschoben. Im Rechenzentrum werden jedoch weiterhin herkömmliche Sicherheitstools eingesetzt, die blind für die jenseits seines Perimeters stattfindenden Aktivitäten sind. Zur sinnvollen Nutzung von SaaS-Anwendungen werden Daten von *innerhalb* der Unternehmens- „Mauern" benötigt. Die Anwendungen selbst befinden sich jedoch *außerhalb* der Mauern, sodass die zu ihnen migrierten Daten nicht von den Sicherheitseinrichtungen des Unternehmens kontrolliert und geschützt werden können.

So war es unmöglich, die Vorteile Cloud-basierter Anwendungen auf sichere Weise zu nutzen. Der Sicherheitsansatz musste sich ändern. Viele Unternehmen begannen damit, zur Beseitigung ihrer dringendsten Sicherheitsprobleme und Schwachstellen neue, zielgerichtete

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Einzelprodukte für ihre privaten Netzwerke und die Cloud zu nutzen. Zu diesen Tools gehörten:

- **Cloud Access Security Brokers** (CASBs) CASBs helfen bei der Verwaltung und dem Schutz von auf Fremdgeräten gespeicherten Unternehmensdaten.
- **Secure Web Gateways** (SWGs) SWGs schützen Mitarbeiter und Unternehmen, wenn sie sich online befinden und auf öffentliche Websites zugreifen.
- **Zero Trust Network Access** (ZTNA) ZTNA-Produkte schirmen die privaten Anwendungen eines Unternehmens von der Öffentlichkeit ab und machen sie nur für eine Gruppe bekannter Mitarbeiter verfügbar.

Diese Tools sind eine frühe Generation der Cloud-Sicherheit. Aber auch dieser Generation fehlte etwas Entscheidendes: die Integration.

Integrierte Sicherheit ist unverzichtbar

Cloud-Sicherheitsprodukte früherer Generationen stammen oft von unterschiedlichen Anbietern und konnten daher nicht zusammenarbeiten. Jedes Produkt hatte seine eigene Konsole und Richtlinien mussten mehrfach konfiguriert werden, so dass es oft zu Überschneidungen kam (man denke nur an DLP). Jede Lösung benötigte ihren eigenen Agent, was zu Problemen bei der Bereitstellung und der Weiterleitung des Datenverkehrs führte, und für jede waren separate Vertragsverhandlungen und Kaufvereinbarungen erforderlich.

Stellen Sie sich vor, wie es wäre, wenn alle fünf Sinne - Hören, Riechen, Schmecken, Sehen und Tasten - mit unterschiedlichen Gehirnen verbunden wären. Wenn Sie ein Feuer sehen, riechen oder hören, wissen Sie ohne Integration nicht, was Sie tun sollen, da Ihre Gehirne keine Informationen austauschen. Sie können die von Ihren Sinnesorganen aufgenommenen Reize nicht zueinander in Beziehung setzen.

In einer solchen Sicherheitsinfrastruktur gibt es viele unterschiedliche Systeme, und jedes davon hat sein eigenes Gehirn, das auf einen bestimmten Bereich spezialisiert ist. Ein CASB ist demnach ein Gehirn, das sich hauptsächlich mit dem Zugriff auf SaaS-Anwendungen befasst.

ERINNERN

Das Gehirn nimmt Informationen von allen Ihren Sinnesorganen auf, damit Sie die richtigen Entscheidungen treffen können. Ihre Sicherheitsdienste müssen ebenfalls vollständig integriert sein, damit sie durch eine effektive Entscheidungsfindung Ihre Cloud-Strategie unterstützen können. SSE ist das Gehirn, das die unterschiedlichen

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Sicherheitskategorien integriert. Mit SSE arbeiten diese „Sinnesorgane der Sicherheit“ nicht mehr getrennt voneinander, sondern werden gleichzeitig aktiviert. Das Ergebnis: eine schnellere und effizientere Security. Außerdem ist die Anschaffung von SSE viel einfacher, da alle Funktionen (CASB, SWG, ZTNA und zugehörige Tools) in einer einzigen Transaktion erworben werden.

Die Sicherheit muss den Daten folgen

Wie wir in Kapitel 1 gesehen haben, beschreibt der Secure Access Service Edge (SASE) eine Vision, in der der klassische Unternehmensperimeter nicht mehr existiert. Stattdessen wird das gesamte Portfolio an Netzwerk- und Sicherheitsfunktionen in die Cloud verlagert – in die unmittelbare Nähe der Mitarbeiter, der in der Cloud gespeicherten Daten und der SaaS-Anwendungen.

SASE gibt Unternehmen die Möglichkeit, ihren Sicherheitsansatz an eine Cloud-first-Welt mit Work-from-anywhere-Umgebungen anzupassen, in denen es den physischen Perimeter nicht mehr gibt. In dieser neuen Welt muss die Sicherheit weit über die Grenzen des Rechenzentrums hinausgehen. Die Sicherheit muss jetzt dem wichtigsten Vermögenswert eines Unternehmens folgen - seinen Daten. Sie muss den Kontext kennen, damit diese Daten überall und unabhängig davon geschützt werden, wie auf sie zugegriffen wird.

Sicherheitslösungen für die Cloud müssen neue Voraussetzungen erfüllen und neue Fähigkeiten aufweisen. Sicherheit muss:

- den Daten folgen.
- auf einem reichhaltigen Kontext beruhen.
- sich an die spezifischen Merkmale des User-Kontexts anpassen.

Ein weiterer wichtiger Aspekt, für den das SASE-Modell eine Lösung bietet, ist das Gleichgewicht zwischen Sicherheit und Netzwerkleistung. Beide sind gleichermaßen wichtig. Menschen sind am produktivsten, wenn sie ihre Technologie mühelos und reibungslos nutzen können. Wenn Sicherheitstools die Netzwerke verlangsamen, leidet sowohl die Leistung als auch die Produktivität. Schlimmer noch: Mitarbeiter könnten versuchen, Sicherheitskontrollen gänzlich zu umgehen, was enorme Risiken und Gefahren mit sich bringen würde.

Unternehmen können dieses Gleichgewicht erreichen, indem sie ihre wichtigsten Netzwerk- und Sicherheitsfunktionen in die Cloud verlagern und sich von ihren Perimeter-basierten Appliances und allen Legacy-Produkten trennen (nicht jeder wird davon begeistert sein).

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Mit diesem Ansatz können sie Usern einen sicheren und zuverlässigen Zugang zu Webdiensten, Anwendungen und Daten bieten, wobei Zero-Trust-Prinzipien durchgängig angewendet werden, um bei jeder Interaktion einen Zustand des kontinuierlichen, adaptiven Vertrauens zu erreichen.

SSE: Die Sicherheitsanforderungen auf der SASE-Reise

Mit SASE und SSE wird die Sicherheit in die Cloud verlagert - und wird dadurch effektiver als je zuvor.

SASE ist ein umfassendes Programm für den Umzug von Netzwerk- und Sicherheitsfunktionen in die Cloud. SSE ist das Gehirn, das die für SASE erforderlichen Sicherheitsservices integriert, identifiziert und ausführt. Diese integrierten Dienste werden zum Hauptkontrollpunkt, an dem eine konsistente Sicherheitsüberprüfung und -inspektion auf den gesamten Datenverkehr angewendet wird. SSE ersetzt die Firewall zwar nicht, doch sie verdrängt die Position der Firewall als zentrale Sicherheitsfunktion.

CASB, SWG, ZTNA und andere damit verbundene Dienste haben als Point Products zweifellos ihren eigenen Nutzen und die meisten Unternehmen verwenden mindestens zwei dieser Dienste. Die Vorteile der Cloud können jedoch erst dann voll ausgeschöpft werden, wenn diese Dienste integriert werden und zusammenarbeiten.

Netskope ist der Ansicht, dass zu den wesentlichen SSE-Funktionen noch viele weitere hinzukommen können. Dabei handelt es sich um Funktionen, die derzeit in der Unternehmenssicherheit fehlen, doch für die zuverlässige Sicherung digitalen "Eigentums" über die Grenzen des Rechenzentrums hinaus entscheidend sind. Dazu gehören:

- **Klassifizierung:** Identifiziert und kennzeichnet sensible Informationen, idealerweise bei ihrer Erstellung, aber auch durch regelmäßige Scans von Datenspeichern.
- **Data Loss Prevention (DLP):** Überwacht und kontrolliert aktiv die Bewegung sensibler Informationen.
- **Bedrohungserkennung und Neutralisierung (auch bekannt als Advanced Threat Protection oder ATP):** Erkennt Anzeichen dafür, dass eine Umgebung kompromittiert wurde, und führt Maßnahmen durch, um die Wahrscheinlichkeit künftiger Angriffe zu verringern oder zu beseitigen.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

- **Cloud Security Posture Management (CSPM):** Bewertet die Konfiguration von Infrastruktur- und Plattform-Clouds und ergreift Maßnahmen zur Beseitigung von Fehlkonfigurationen, die zu einer Gefährdung führen könnten.
- **SaaS Security Posture Management (SSPM):** Bewertet die Konfiguration von SaaS-Anwendungen und beseitigt Fehlkonfigurationen, die Exfiltration, Identitätsbetrug oder andere Arten von Angriffen ermöglichen könnten.
- **Digital Experience Management (DEM):** Analysiert die zu Sicherheitszwecken erfassten Daten in Kombination mit anderen Signalen, um die Usererfahrung zu messen und Probleme schnell zu beheben.

ERINNERN

Da SSE alle diese Funktionen in einem einzigen, integrierten Sicherheitsprodukt zusammenführt und in der Cloud bereitstellt, wo sie Menschen, Daten und Anwendungen am nächsten sind, wird SSE zum wichtigsten Kontrollpunkt für den Schutz Ihres Unternehmens. (Kapitel 3 wird sich näher mit SSE befassen.)

Wir brauchen Sicherheit für die Zukunft, nicht für die Vergangenheit

Unternehmen müssen Tools bereitstellen, die die Cloud unterstützen, denn letztlich ist die Cloud der ausschlaggebende Faktor für die Schaffung von Geschäftswert und Umsatz. Diese Tools müssen Angreifer abwehren können und dürfen den Geschäftsbetrieb nicht behindern. Stellen Sie sich vor, Sie könnten einen unsichtbaren Bodyguard engagieren, der Ihr Kind in den Kindergarten oder in die Schule begleitet. SSE ist dieser Bodyguard.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- Erfahren wir, warum wir SSE brauchen
- Untersuchen wir die Fähigkeiten und Anforderungen von SSE
- Betrachten wir die Vorteile von SSE

Kapitel 3
Security Service Edge: Die Zukunft der Cloud-basierten Sicherheit

Secure Access Service Edge (SASE) verändert unsere Sichtweise auf die Bereitstellung von Sicherheit in einer Cloud-basierten Welt, in der von überall auf Daten zugegriffen werden kann. Arbeitskräfte arbeiten zunehmend dezentral, viele Anwendungen werden als Software-as-a-Service (SaaS) genutzt und immer mehr Daten wandern in die Cloud. Die Sicherheit muss diesen Usern, Anwendungen und Daten folgen. Durch die Implementierung einer richtig konzipierten SASE-Architektur können Unternehmen dafür sorgen, dass sich die Sicherheit so nah wie möglich an dem Ort befindet, an dem sich die Daten befinden und an dem User auf sie zugreifen. Die Sicherheitsdienste der SASE-Architektur schützen die Interessen des Unternehmens, wenn User aus der Ferne auf Daten zugreifen, ohne die Netzwerkkonnektivität und das Benutzererlebnis zu beeinträchtigen.

Die Realisierung von SASE erfordert die Konsolidierung von Sicherheitstools und -methoden sowie Integration – darin liegt der Kern vom SSE.

Der SSE verlagert kritische Prüf- und Kontrollpunkte in die vom Unternehmen genutzte(n) Cloud(s). Die Sicherheit ist nun dort angesiedelt, wo sich Daten, Anwendungen und User befinden – und wo Gefahren lauern. Mit SSE arbeiten Prüf- und Kontrolldienste für SaaS, Internet

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

und Daten, sowie eine ausgefeilte Bedrohungserkennung und -neutralisierung als ein einziges, zusammenhängendes, interoperables System.

TIPP

Sie haben kein Problem mit Ihrem Netzwerk. Sie haben ein Problem mit Ihrer Cloud-Sicherheit. Netzwerksicherheit kann durch die Einführung einer Architektur gewährleistet werden, die den SSE zum primären Prüfpunkt in der Cloud macht.

Die vom SSE zur Verfügung gestellten Funktionen gehen weit über die Fähigkeiten herkömmlicher Firewalls hinaus. Bei richtiger Implementierung kann der SSE auch den Kontext erkennen – detaillierte Informationen wie User, Standort und Authentifizierungsmethode – und kann so in Echtzeit differenzierte Sicherheitsentscheidungen treffen. Der SSE verbindet alle „Sinnesorgane" der Security in einem einzigen Gehirn, das die Daten interpretiert, das Ausmaß der Risiken versteht und jederzeit und in jedem Szenario die richtige Zugriffsebene bestimmt.

Im nächsten Abschnitt werden wir uns genauer ansehen, wie der SSE funktioniert.

Warum wir SSE brauchen

Bei dem veralteten Ansatz wurden Angreifer, die in das Rechenzentrum eines Unternehmens gelangen wollten, mithilfe Perimeter-zentrierter Sicherheitsmechanismen und Firewalls abgewehrt. Kein Sicherheitssystem ist jedoch unüberwindbar. Angreifer, denen es gelang, den Perimeter zu durchdringen, konnten sich lateral durch das gesamte Netzwerk bewegen und nach Lust und Laune auf ungeschützte Daten und Anwendungen zugreifen.

Zur Authentifizierung von Mitarbeitern stützen sich SASE-Architekturen weiterhin auf der Identitäts- und Zugriffsverwaltung, während sie zum Schutz von Geräten Endpoint Security Plattformen einsetzen. Eine effektive SASE-Lösung implementiert jedoch auch Zero-Trust-Prinzipien zur zur Kontrolle der Zugriffe, die bewerten, wie viel Vertrauen einem User unter bestimmten Bedingungen gewährt werden soll. In der Cloud wird der Kontext des Users zum Perimeter.

Zero Trust ist eine Philosophie, die auf drei Säulen beruht, welche für den SSE und damit auch für SASE von grundlegender Bedeutung sind:

» Das implizite Vertrauen, das mit veralteten Ansätzen einhergeht, entspricht den heutigen Anforderungen nicht mehr. Zero Trust kehrt das herkömmliche Prinzip um und führt einen Ansatz ein, nach dem zuerst geprüft und dann vertraut wird. Die Identität und der Kontext jedes Users werden jedes Mal beim Versuch eines

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Datenzugriffs überprüft, um ein bestimmtes Vertrauensniveau zu erreichen. Dabei werden keine Ausnahmen gemacht.

- Es wird nur minimaler Zugriff gewährt, der dem festgelegten Vertrauensniveau entspricht. Dieses Prinzip wird als „Least Privilege' bezeichnet. Der Zugriff ist auf eine bestimmte Ressource beschränkt und kann nicht auf andere Ressourcen übertragen werden.
- Der Kontext muss auf der Grundlage von Signalen, wie z.B. der Identität des Mitarbeiters, der Geräteidentität, des Sicherheitszustands des Geräts, der Tageszeit, des Standorts, der Geschäftsrolle und der Sensibilität der Daten ständig neu bewertet werden. Jede Signaländerung löst eine neue Bewertung aus. (Netskope bezeichnet dies als *kontinuierliches adaptives Vertrauen*. In Kapitel 4 werden wir näher darauf eingehen.)

SASE bietet einen Rahmen für ein effektives Zero-Trust-Programm zum Schutz von Umgebungen, in denen sich User, Anwendungen und Daten an den unterschiedlichsten Orten befinden können. Wie wir in Kapitel 4 sehen werden, handelt es sich bei Zero Trust jedoch lediglich um eine Reihe von Prinzipien, und nicht um eine technische Architektur zur einheitlichen Implementierung unterschiedlicher Sicherheitsfunktionen.

Diese technische Architektur kann mit dem SSE bereitgestellt werden. Der SSE vereint, integriert und koordiniert viele unterschiedliche Sicherheitsdienste. Durch einen benutzerzentrierten und kontextbezogenen Ansatz können effektivere Sicherheitsfunktionen bereitgestellt werden, während das Unternehmen und seine Mitarbeiter von einer höheren Leistung profitieren. Um die gewünschten Ergebnisse zu erzielen, liefert der SSE:

- detaillierten Kontext durch Informationen über Anwenderhistorie, Gerätetyp, angeforderte Daten, Anwendung, Netzwerk und sogar den Grund des Zugriffs.
- Informationen über die Ressourcen, auf die ein User zugreifen darf (SSE kann diese aus den Autorisierungs- und Berechtigungsdetails ableiten).
- Granularität, um die Sensibilität unterschiedlicher Datenressourcen zu klassifizieren (und Datenverluste zu verhindern).
- Anleitungen und detaillierte Richtlinien, die das gewünschte Sicherheitsergebnis auf der Grundlage unterschiedlicher Kombinationen von personen-, daten-, anwendungs- und anderen kontextbezogenen Informationen beschreiben.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Das Problem besteht darin, dass viele der gewünschten Ergebnisse, wie eine funktionierende Data Loss Prevention und die Erkennung und Neutralisierung von Bedrohungen, das Zusammenwirken mehrerer Sicherheitskomponenten erfordern.

WARNUNG

Würde man jeden Dienst unabhängig implementieren, müssten viele Überprüfungen in den Konsolen mehrerer Tools wiederholt werden. Dies ist ein mühsamer und fehleranfälliger Prozess, wenn ein Auftrag – oder ein Menschenleben – auf dem Spiel steht.

Mit dem SSE gibt es keine solchen Wiederholungen. Bei richtiger Implementierung verbindet der SSE diese Dienste miteinander und ermöglicht die gemeinsame Nutzung von Daten in Verbindung mit Kontext, Berechtigungen, Sicherheitsrichtlinien, Risikoinformationen, Browser-Isolierung, Datenverschlüsselung/-entschlüsselung usw. Dieser Zusammenschluss ermöglicht es den Sicherheitsdiensten, Transaktionen in einem einzigen Durchgang zu verarbeiten und schnell den richtigen Zugriff zu gewähren.

Wie SSE Sicherheitsdienste zusammenbringt

Der SSE basiert auf der Integration vieler Sicherheitsdienste, die durch zahlreiche verbundene Funktionen unterstützt werden. Es gibt eine richtige Herangehensweise an die Realisierung von SSE - und viele falsche.

WARNUNG

Da sich der SSE zunehmender Beliebtheit erfreut, gibt es mittlerweile auch schon einige irreführende Marketing-Tricks. Eine unzulängliche SSE-Lösung lässt sich leicht an ihrer mangelnden Integration erkennen. Bei einigen dieser Ansätze werden lediglich einzelne Prozesse miteinander verbunden oder alte, miteinander verkettete Geräte aktualisiert. Dies deutet darauf hin, dass die Systeme einfach aus einzelnen Bestandteilen zusammengestellt wurden – aus Legacy-Produkten von verschiedenen Anbietern, die vor dem Zeitalter der Cloud hergestellt wurden. Die auf diese Weise zusammengestoppelten Systeme sind mit einer hohen Latenz verbunden. Da sie die umfassenden Vorteile eines SSE nicht bieten können, stellen sie eigentlich keine sinnvolle SASE-Lösung dar.

Bei einem SSE handelt es sich niemals um eine Verkettung von Geräten oder eine Abfolge einzelner Prozesse, bei denen Daten erst eine DLP-Engine, dann einen Access Control List Evaluator, dann ein Web-Gateway und so weiter durchlaufen. Dennoch ist es hilfreich, die Merkmale einer vollständig integrierten SSE-Lösung zu analysieren.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Die saubere Analyse komplexer Daten

Bei einer idealen SSE-Lösung arbeiten alle integrierten Sicherheitsdienste parallel. Alle Überprüfungen erfolgen gleichzeitig und in Echtzeit, unabhängig davon, ob der Datenverkehr aus dem Internet, der Cloud oder dem Rechenzentrum stammt.

Ein einzelner Arbeitsdurchlauf ("single pass") sorgt für eine immer feinere Filterung des Datenverkehrs, um Daten und Anwendungen optimal zu schützen. Stellen Sie es sich zunächst so vor, als wenn der Datenverkehr durch einen Trichter fließt.

Echtes SSE unterscheidet zwischen Unternehmensanwendungen (z. B. Salesforce, Workday), persönlichen Anwendungen (z. B. dem Gmail-Konto einer Person) und Anwendungen/ Diensten von Drittanbietern (z. B. Unternehmensinstanzen von Microsoft Office 365 oder Dropbox) (Instance Awareness). Dieses Wissen wird dann genutzt, um die entsprechenden Verbindungen zu initiieren, die für den Schutz jeder Anwendung oder jedes Dienstes in Übereinstimmung mit der Richtlinie erforderlich sind.

Echtes SSE bewertet den Kontext und passt den Zugang entsprechend an, z. B. je nachdem, ob ein Arzt (siehe Kapitel 4) ein krankenhauseigenes Tablet im Patientenzimmer, sein Telefon im Wi-Fi des Cafés oder den Gaming-Computer im Kinderzimmer verwendet.

Echtes SSE legt Richtlinien fest, die verhindern, dass Daten verloren gehen oder ausgeschleust werden können. Kontrollen können das Herunterladen von Dokumenten, das Anfertigen von Screenshots, die Eingabe von Daten in Webformulare oder das Posten in sozialen Medien verhindern.

Echtes SSE ermöglicht eine kontinuierliche Überwachung des Sicherheitsstatus. Während Mitarbeiter ihren üblichen Tätigkeiten nachgehen, hält SSE Ausschau nach Anomalien. Wenn Datenobjekte klassifiziert werden, kann SSE zwischen sensiblen und nicht sensiblen Inhalten unterscheiden und die Zugriffsberechtigungen und erlaubten Aktivitäten dynamisch ändern. SSE kann einen Alarm auslösen, Empfehlungen geben oder einen Mitarbeiter um weitere Informationen bitten, damit seine Aktivitäten auf sichere Weise gesteuert werden können.

Gemeinsam genutzte Dienste

Alle übergeordneten Sicherheitsfunktionen wie DLP, Threat Awareness, Neutralisierung und Digital Experience Management (DEM) können jeden einzelnen Dienst und jede hier beschriebene Methode nutzen, um die gewünschten Sicherheitsergebnisse zu erzielen:

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

- **Gemeinsamer Kontext:** Alle SSE-Elemente nutzen eine umfangreiche Sammlung von Metadaten zur Identifizierung des Users, Geräts und Standorts. Die angeforderte Ziel-Website, die Zielanwendung oder der Zieldienst werden identifiziert und einer Risikobewertung unterzogen, und ihre Aktivitäten werden untersucht. Dabei werden alle Daten berücksichtigt, die von dem Mitarbeiter und der Anwendung angefordert oder erstellt werden. Umfassender SSE-Kontext beinhaltet die Bewertung des Mitarbeiterverhaltens und stellt zur Analyse aktueller Aktivitäten sogar Bezüge zu früheren Interaktionen her. Diese ständig aktualisierte Kontextlandschaft bildet die Grundlage für die von allen SSE-Elementen ergriffenen Maßnahmen und durchgesetzten Richtlinien (beim SSE-Angebot von Netskope heißt dieser Dienst Cloud XD).
- **Kontinuierliches und adaptives Vertrauen:** Der Zugriff auf Daten und Anwendungen kann heute nicht mehr durch einfache "entweder - oder"-Entscheidungen kontrolliert werden. Er erfordert eine flexible Herangehensweise, bei der sich ändernde Anforderungen und Kontexte berücksichtigt werden. Echtes SSE passt den Grad des Vertrauens an die Bedeutsamkeit der Daten an, die genutzt werden sollen und orientiert sich dabei an zahlreichen kontextbezogenen Signalen und der in den Richtlinien vorgegeben Risikobereitschaft des Unternehmens.
- **Richtlinienbasierte Verwaltung:** Echtes SSE verfügt über einen detaillierten, gemeinsamen Richtlinienrahmen. Damit können Unternehmen die Grenzen ihrer Risikotoleranz festlegen und die erwarteten Sicherheitsergebnisse klar definieren. Dies ist ein weiterer Teil der "Single-Pass"-Security, der die Tausenden mit Firewalls verbundenen Sicherheitsregeln eliminiert. Die einzelnen SSE-Komponenten nutzen den Richtlinienrahmen, um Aktivitäten und Daten über alle Anwendungen, Anwendungskategorien und Webdienste hinweg zu kontrollieren.

SSE: Wesentliche Vorteile

Im vorherigen Abschnitt haben wir erläutert, welche Komponenten einem SSE zugrunde liegen. Nun können wir näher darauf eingehen, welche Funktionen der SSE bereitstellt. Einige davon sind Ihnen sicher bekannt, weil Ihr Unternehmen sie bereits in anderer Form einsetzt. Der SSE wird diese Tools wahrscheinlich im Laufe der Zeit ersetzen.

ERINNERN

SSE soll Menschen und Unternehmen ein möglichst schnelles und sicheres Arbeiten ermöglichen. Da SSE überall funktioniert, ist es nicht mehr nötig, die Sicherheit im Rechenzentrum derart auszuweiten, dass sie Daten, Anwendungen und Usern in die Cloud folgt.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Tabelle 3-1 zeigt die Mindestanforderungen an ein Produkt, das nach Meinung mehrerer Analysten im Jahr 2021 als *Security Service Edge* bezeichnet werden kann.

TABELLE 3-1 Mindestanforderungen an SSE

Funktion	Was führt sie aus?	Wie SSE sie besser macht
SWG	Kontrolliert den Zugriff und schützt nur vor Web-Bedrohungen.	Deckt auch Cloud-basierte Bedrohungen und Datenrisiken für persönliche Instanzen verwalteter Anwendungen, Tausende von Schatten-IT-Anwendungen und Cloud-Dienste ab.
CASB	Ein Policy Enforcement Point, der zwischen Verbrauchern und Anbietern von Cloud-Services eingerichtet wird, um die Sicherheitsrichtlinien des Unternehmens beim Zugriff auf Cloud-basierte Daten oder Anwendungen durchzusetzen. Bewertet das Benutzerverhalten und bietet Transparenz und Kontrolle über SaaS-Anwendungen, um den richtigen Zugang für bestimmte User festzulegen.	Eliminiert die Verwendung mehrerer Richtlinien (zwischen SWG und CASB), vereinfacht die Verwaltung (ein einziger Agent für SWG, CASB und ZTNA) und bietet Transparenz über den gesamten Datenverkehr hinweg.
ZTNA	Setzt das Prinzip durch, dass keiner Instanz implizit vertraut bzw. Zugriff auf Unternehmensressourcen gewährt werden darf, bevor ihre Legitimität überprüft und bestätigt wurde. Unterstützt die Implementierung der Zugriffskontrolle nach dem „Least Privilege"-Prinzip, bei dem Personen oder Personengruppen nur Zugriff auf Ressourcen erhalten, die sie benötigen.	Verbessert ZTNA durch die Möglichkeit des adaptiven Zugriffs. Harmonisiert die Richtlinienverwaltung mit anderen SSE-Komponenten, während die Durchsetzung von Richtlinien beibehalten wird.
Remote Browser Isolation (RBI)	Trennt die Browser-Aktivität von der Endgeräte-Hardware. Alle Browser-Aktivitäten werden in einem entfernten, Cloud-basierten Container gehostet und ausgeführt. Durch dieses Sandboxing werden Daten, Geräte und Netzwerke beim Browsen von Websites vor den unterschiedlichsten Bedrohungen geschützt.	Ermöglicht der RBI, Datenklassifizierung und Rollenkontext zu nutzen. Isolierung kann durch Richtlinien in SWG und CASB durchgesetzt werden.

(Fortsetzung)

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

TABLE 3-1 *(Fortsetzung)*

Funktion	Was führt sie aus?	Wie SSE sie besser macht
Firewall-as-a-Service (FWaaS)	Netzwerksicherheit für alle ausgehenden Ports und Protokolle für einen sicheren, direkten Internetzugang über einen Agent auf verwalteten Geräten oder über GRE und IPsec für Büros. Eine Richtlinien-Engine und eine Sicherheitsplattform, die eine vereinfachte Verwaltung für Mitarbeiter und Zweigstellen über eine einheitliche Konsole ermöglicht.	Gibt Unternehmen die Möglichkeit, den Datenverkehr aus unterschiedlichen Quellen zu bündeln - sei es aus Rechenzentren vor Ort, aus Zweigstellen, von mobilen Mitarbeitern oder der Cloud-Infrastruktur. Sorgt für eine konsistente Durchsetzung von Anwendungs- und Sicherheitsrichtlinien an allen Standorten und bei allen Mitarbeitern und bietet gleichzeitig vollständige Netzwerktransparenz und -kontrolle, ohne dass physische Appliances eingesetzt werden müssen.

Die Möglichkeiten von SSE: bald auch für Ihr Sicherheitsteam!

Mit zunehmender Produktreife und der Verbreitung von Cloud-First-Initiativen wird SSE mit weiteren Funktionen ausgestattet. Die richtige SSE-Architektur umfasst viel mehr als die ursprüngliche Basisdefinition, darunter:

- Verbesserte Klassifizierung zur Unterstützung von DLP
- Security Posture Management für die Cloud und SaaS
- Erkennung und Neutralisierung von Bedrohungen
- Digital Experience Management (Steuerung von User Experience)
- Diese werden wir in den folgenden Abschnitten näher betrachten.

Verbesserte Klassifizierung zur Unterstützung von DLP

DLP ist ein Sammelbegriff für eine Funktion, die den absichtlichen und versehentlichen Datenabfluss verhindern soll. Eine DLP-Lösung erkennt die Bewegung sensibler Daten und verhindert, dass sie an unerwünschte Orte gelangen. Mitarbeiter werden durch Benachrichtigungs-Pop-ups auf Risiken aufmerksam gemacht. DLP nutzt maschinelles Lernen, um die Risikoeinstufungen von Mitarbeitern zu bewerten.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

TIPP

SSE verbessert DLP durch die aktive Identifizierung und Klassifizierung von Daten, damit die Regeln für die Bewegung sensibler Daten genauer verfolgt und durchgesetzt werden können.

Security Posture Management für die Cloud und SaaS

Cloud Security Posture Management (CSPM) und SaaS Security Posture Management (SSPM) werden eingesetzt, um Fehlkonfigurationen in Clouds (die häufigsten Sicherheitsfehler in der Cloud) zu erkennen und zu beheben. CSPM und SSPM nutzen den von SSE bereitgestellten Kontext, API-gestützte Kontrollen und die Echtzeit-Bewertung von Public-Cloud-Deployments, um Risiken zu minimieren. Dabei werden Konfigurationen analysiert und Änderungen vorgeschlagen, durch die die Wahrscheinlichkeit eines potenziellen Angriffs verringert oder ganz beseitigt werden kann, und die Einhaltung von Vorschriften überwacht.

TIPP

CSPM und SSPM in „echten" SSE-Implementierungen erkennen Bedrohungen und ergreifen aktiv Maßnahmen, um den Sicherheitsstatus eines Unternehmens zu verbessern.

Einige CSPM- und SSPM-Implementierungen können beispielsweise Verstöße erkennen, wenn die Richtlinie eines Unternehmens vorschreibt, dass alle Daten in der Cloud standardmäßig verschlüsselt werden sollen. Dies ist eine konsequente Haltung, da bei Zugriffskontrollen die folgenden Vorgaben eingehalten werden müssen: Die Identität einer Person muss sowohl in der Zugriffskontrollliste für ein verschlüsseltes Objekt als auch in der Liste für den zugehörigen Verschlüsselungsschlüssel enthalten sein. CSPM und SSPM müssen erkennen, wenn eine Person unverhältnismäßige Zugriffsrechte hat, und auf Unregelmäßigkeiten aufmerksam machen.

Erkennung und Neutralisierung von Bedrohungen

Tools zur Erkennung und Neutralisierung von Bedrohungen sind in der Lage, frühe Hinweise auf erfolgreiche Angriffe zu erkennen und lösen einen Alarm aus, damit die Gefahr rechtzeitig eingedämmt werden kann. Typische Hinweise sind ungewöhnliche Netzwerkaktivitäten, Konfigurationsänderungen und das Löschen von Protokolldateien. Durch forensische Analysen wird festgestellt, ob eine aktive Bedrohung in der Umgebung vorhanden ist. Die Neutralisierung von Bedrohungen ist ein perfektes Beispiel für einen Dienst, der von den gemeinsam genutzten Fähigkeiten der SSE-Architektur profitiert.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Digital Experience Management (DEM)

Ein neuer und wichtiger Aspekt von SSE ist die Fähigkeit, die Benutzererfahrung von Mitarbeitern und die Anwendungsleistung abzuschätzen. Dies ist vor allem deshalb nützlich, weil sich die Netzwerkgrenze jetzt bis zur Cloud erstreckt. Durch die kontinuierliche Überwachung des gesamten Datenverkehrs profitieren Kunden von einer durchgängigen Transparenz über das Netzwerk- und Anwendungsverhalten. Sie erhalten wertvolle Echtzeit-Einblicke in die Aktivitäten von Usern und können dadurch sicherstellen, dass SSE ohne Leistungseinbußen funktioniert. Wenn es Probleme mit Geräten, dem Netzwerk oder einer Anwendung geben sollte, kann DEM der Ursache schnell auf den Grund gehen, die Lösung beschleunigen und proaktive Schritte unternehmen, damit aus kleinen Problemen keine großen geschäftsschädigenden Ereignisse werden.

Auch Netzwerke müssen sich weiterentwickeln

Bis jetzt haben wir uns vor allem auf Sicherheitsfunktionen und die Möglichkeiten konzentriert, die SSE für eine Cloud-first-Welt bietet. Es bedarf jedoch weiterer wichtiger Veränderungen, die über das hinausgehen, was wir als Security bezeichnen.

ERINNERN

Der Netzwerkzugang muss dezentral möglich sein, damit Mitarbeiter und Unternehmen den vollen Nutzen aus den von SSE geschützten Cloud-basierten Systemen ziehen können, wie in Abbildung 3-1 dargestellt.

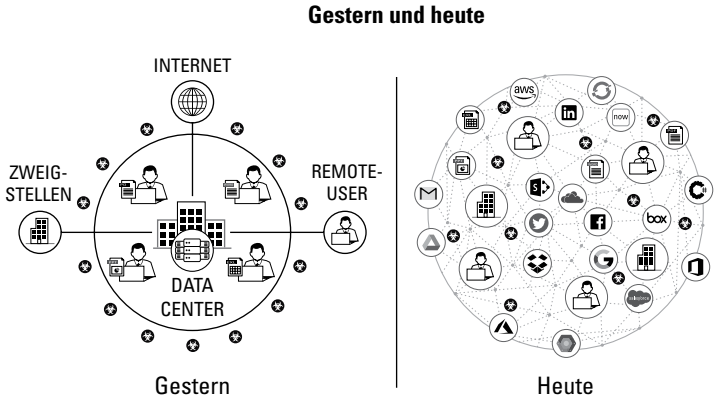

ABBILDUNG 3-1: Im Vergleich zum neuen Zugangsmodell, das einen ortsunabhängigen Zugang ermöglicht, war das alte Modell ineffizient und ineffektiv.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Mitarbeiter waren mit einem Netzwerk verbunden, das durch einen genau definierten Perimeter geschützt war. Zweigstellen mussten teure private Netzwerkverbindungen zum Rechenzentrum unterhalten. Dies wurde zu einem Problem, als das Internet und später die Cloud eine immer größere Rolle für den Geschäftsbetrieb spielten. Damit Mitarbeiter sicher auf Cloud- und Web-Ressourcen zugreifen konnten, musste der Datenverkehr durch den Security-Stack des Rechenzentrums geleitet werden.

Dieser Ansatz war weder effizient noch effektiv. Die Nutzung von Cloud-Ressourcen verbessert zwar die Leistung und Produktivität von Arbeitskräften, doch sie untergräbt auch die Transparenz und Kontrolle des Rechenzentrums. Es ist schwierig und kostspielig, private Netzwerke aufzubauen, zu warten und zu überwachen, um alle Möglichkeiten der Cloud voll ausschöpfen zu können. Außerdem lässt sich ein solches Netzwerk nicht einfach skalieren - ein wichtiger Aspekt in einer Zeit, in der Sicherheit auf jeder Ebene oberste Priorität haben muss.

Die Architektur des neuen Netzwerkmodells ist für die Arbeit an Remote-Standorten konzipiert, damit sich Mitarbeiter von überall aus mit dem Netzwerk verbinden, mit anderen Menschen kommunizieren und auf Informationen zugreifen können, die sich zum größten Teil in der Cloud befinden. Um eine optimale Leistung und Anwendungserfahrung zu gewährleisten, muss das Netzwerk eines SSE-Anbieters:

- über umfangreiche Peerings und Verbindungen zu den wichtigsten Zielen verfügen
- aus einer ausreichenden Anzahl von Points of Presence bestehen, die mit allen Rechenressourcen ausgestattet und strategisch verteilt sind, damit sich Mitarbeiter nie weit von ihnen entfernt sind.

TIPP

Der beste Weg zu schnellen, mühelosen Verbindungen ist die Zusammenarbeit mit einem Anbieter, dessen Netzwerk über zahlreiche Direktverbindungen zu den wichtigsten Zielen verfügt. Je mehr Verbindungen Ihr Anbieter zur Verfügung stellen kann, desto besser sind die Leistung und die Ausfallsicherheit - und umso zufriedener die User.

ERINNERN

Ein gut vernetzter Anbieter sorgt für eine bessere Leistung und Ausfallsicherheit und damit für ein hervorragendes Benutzererlebnis. Die User Experience zählt! Die digitale Transformation ist nur dann erfolgreich, wenn Sicherheit und Vernetzung vom ersten Tag an eine stabile Partnerschaft bilden. Sicherheit darf die Netzwerkleistung nicht beeinträchtigen. Ein Unternehmen sollte nie gezwungen sein, einen gefährlichen Kompromiss zwischen Sicherheit und Produktivität einzugehen.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Wie alle Aspekte von SASE und SSE wird auch die Netzwerktransformation im Laufe der Zeit immer weiter optimiert. Ihr Cloud-Security-Anbieter muss die Kluft zwischen Ihrer derzeitigen Sicherheitsarchitektur und der Security, die Sie sich für die Zukunft wünschen, effektiv überbrücken können. Er muss SSE anbieten, neue On-Ramps für Ihre geografisch verteilten Mitarbeiter bereitstellen und sich nahtlos in die bestehenden Netzwerkinfrastrukturen und -prozesse integrieren.

Vorteile der SSE-Sicherheit

Durch die Einführung einer SASE-Architektur mit Zero-Trust-Prinzipien als Kernstück und die Zusammenarbeit mit einem SSE-Anbieter, der in der Lage ist, kritische, dezentral erreichbare Sicherheitsdienste bereitzustellen, können Unternehmen erhebliche Vorteile erzielen:

- größeres Vertrauen bei der Gewährung des Zugriffs auf Daten und Anwendungen außerhalb des Rechenzentrums
- flexible Sicherheit auf der Grundlage von Erkenntnissen über die Risikolage mit adaptiven Richtlinien und Kontrolle über bestimmte Aktivitäten, die auf die jeweilige Anwendung zugeschnitten sind
- die Möglichkeit, Zero Trust-Prinzipien über private Anwendungen hinaus auf Web- und SaaS-Anwendungen auszuweiten
- Zugriff auf zusätzliche Sicherheitsservices wie RBI und erweiterte DLP auf der Grundlage des bewerteten Risiko- oder Vertrauensniveaus
- kontinuierliche Überwachung von Änderungen in ihrem spezifischen Kontext, die automatisch eine Neubewertung von Vertrauen und Zugriff auslösen
- Verringerung der Angriffsfläche, da Protokolle und Dienste nicht mehr durch das öffentliche Internet gefährdet sind
- korrekt konfigurierte Clouds, um die häufigste Form von Sicherheitsfehlern in der Cloud auszuschließen.

Alle diese Vorteile sind Aspekte der in Kapitel 1 erwähnten sorgenfreien Sicherheit. Kapitel 4 befasst sich mit den geschäftlichen Vorteilen, die „echtes“ SSE bieten kann, sowie den Schritten zu ihrer Realisierung.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

IN DIESEM KAPITEL

- Erfahren wir, wie durch Zero-Trust-Prinzipien ein Zustand des kontinuierlichen, adaptiven Vertrauens erreicht werden kann
- Lernen wir die vier Schritte zur SSE-Einführung kennen
- Betrachten wird die geschäftlichen Vorteile von SSE

Kapitel 4
Wie SASE mit Zero Trust erfolgreich realisiert werden kann

Wie wir in Kapitel 2 gesehen haben, ist die Verlagerung der Sicherheit in die Cloud wichtiger denn je, da Unternehmen immer stärker auf die Cloud angewiesen sind. Die Einführung von Cloud Computing vollzieht sich in einem rasanten Tempo, mit dem selbst vorausschauende Unternehmen bis vor Kurzem nicht rechnen konnten. Unternehmen wechseln in die Cloud, um von kürzeren Entwicklungszyklen, Zugang zu On-Demand-Ressourcen, einer elastischen Skalierung und einem wesentlich geringeren Verwaltungsaufwand zu profitieren. Die Cloud hilft ihnen dabei, in Rekordzeit neue Produkte und Dienstleistungen zu entwickeln und auf den Markt zu bringen.

Angreifer zieht es ebenfalls in die Cloud, weil sie dort immer mehr potenzielle Opfer finden. Deshalb muss sich heute jedes Unternehmen Gedanken über die Sicherheit seiner Daten, Anwendungen und Mitarbeiter in der Cloud machen.

WARNUNG

Wenn es keinen ausreichenden Schutz in der Cloud gibt, ist es unmöglich, ihre Vorteile voll auszuschöpfen.

Sicherheitsverantwortliche müssen den zuständigen Entscheidungsträgern im Unternehmen zunächst klarmachen, wie wichtig die Sicherheit

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

in der Cloud ist. Dann sollten sie ihnen erklären, dass SASE, SSE und ein neues Netzwerkmodell das Risikomanagement erheblich verbessern und Sicherheitsrisiken effektiv verringern können. Aus den Plänen zur Einführung von SSE sollte klar hervorgehen, warum sich diese Änderungen lohnen, welche geschäftlichen Vorteile sie mit sich bringen und wie diese Vorteile gemessen werden können.

Nach unseren Ausführungen über SASE, SSE und die Sicherheitstransformation werden wir in diesem Kapitel nun aufzeigen, wie sich die von uns allen gewünschte sorgenfreie Sicherheit für Daten, Anwendungen und Mitarbeiter in der Cloud erreichen lässt und zur Realisierung eines nachhaltigen geschäftlichen Nutzens beitragen kann. Bei der Gestaltung dieser Sicherheit müssen Zero-Trust-Prinzipien eine zentrale Rolle spielen.

Von Zero Trust zum kontinuierlichen adaptiven Vertrauen

Eine erfolgreiche Implementierung von SASE und SSE erfordert mehr als das Ausmustern von Technologie. Wie wir in Kapitel 3 gesehen haben, ändert Zero Trust einige grundlegende Annahmen darüber, wie Sicherheit funktioniert. Bei einem netzbasierten On-Premises-Modell wird davon ausgegangen, dass das Netz sicher ist und dass die Identität jedes Users vor der Gewährung des Zugriffs überprüft wird. Dabei erhielt der User entweder vollen Zugang oder gar keinen – „erlauben“ und „blockieren“ waren die einzigen Möglichkeiten. Zero Trust ändert dieses Modell grundlegend:

- **Wenn eine Person Zugang anfordert, wird diese Anforderung auf der Grundlage mehrerer Kontextfaktoren bewertet.** Identität ist einer dieser Faktoren. Das System berücksichtigt aber auch den geografischen Standort, die Tageszeit, das Gerät, die Art der Netzverbindung und viele andere Variablen.
- **Die Anwendung, mit der sich die Person verbinden will, ist Teil dieses Kontextes.**
- **Das gewünschte Dienstleistungsniveau ist ein wichtiger Faktor.** Handelt es sich um eine Anwendung, bei der es um Leben und Tod geht, oder um ein Videospiel, das lediglich der Unterhaltung dient?
- **Je nach verwendeter Anwendung kann der Netzwerkpfad auf unterschiedliche Weise geschützt werden.** Wenn ein User auf sein persönliches E-Mail-Konto zugreift, wird eine normale Internetverbindung verwendet, wobei zwischen dem E-Mail-Server und dem E-Mail-Client TLS-Schutz (Transport Layer Security) besteht. Will ein Arzt auf Patientendaten zugreifen, wird ein sicherer, verschlüsselter

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

und authentifizierter Pfad eingerichtet. Die Fähigkeiten des zugrunde liegenden Netzwerks oder der Anwendung spielen dabei keine Rolle.

Auf der Grundlage dieses Kontexts wird für jede Sitzung das Vertrauensniveau der Person bestimmt, d. h. sie kann als wenig oder sehr vertrauenswürdig eingestuft werden. Wenn jemand zu einer ungewöhnlichen Zeit von einem ungewöhnlichen Ort aus Zugriff auf eine hochsensible Anwendung anfordert (ein Beispiel für ein niedriges Vertrauensniveau), wird wahrscheinlich ein mehrstufiger Authentifizierungsprozess angewandt. Der gewährte Zugriff kann auf wenige Daten und Funktionen beschränkt werden, die dann ausschließlich im schreibgeschützten Modus verfügbar sind. Ein Mitarbeiter, der zur üblichen Zeit von einem sicheren Ort aus Zugriff anfordert (ein Beispiel für ein hohes Vertrauensniveau), erhält Zugang zu allen Daten und Anwendungen.

Das folgende Szenario, in dem ein Arzt auf elektronische Krankenakten zugreifen will, soll die Funktion von Zero-Trust-Prinzipien bei der Arbeit mit SSE veranschaulichen.

> Ein Arzt behandelt einen Patienten im Krankenhaus. Er hat ein krankenhauseigenes Tablet bei sich. SSE entscheidet anhand der Identität des Arztes, des Standorts, des Geräts und anderer Faktoren, dass es sicher ist, dem Arzt vollen Zugriff auf die Patientenakten zu gewähren.
>
> Der Arzt geht nun in ein Café gegenüber dem Krankenhaus, um einen Kaffee zu trinken. Er öffnet seinen persönlichen Laptop, verbindet sich mit dem Netzwerk des Cafés und versucht, auf die Patientendaten zuzugreifen. SSE erkennt den Arzt, stellt aber fest, dass der Laptop nicht dem Krankenhaus gehört und sich in einem unbekannten Netzwerk befindet. Der Arzt kann die Akten einsehen und kommentieren, aber er kann die Daten nicht ändern.
>
> Beim Abendessen zu Hause erfährt der Arzt, dass es im Krankenhaus eine Krise gibt. Er loggt sein Kind aus Minecraft aus, um vom PC der Familie aus auf Patientenakten zuzugreifen. SSE erkennt, dass dieser Computer weniger sicher ist als das Tablet des Krankenhauses. Anstatt dem Arzt den Zugriff auf die Akten gänzlich zu verweigern, stellt SSE mehrere Eingabeaufforderungen bereit, damit er seine Identität bestätigen und den Grund für den benötigten Zugriff angeben kann. SSE stellt dem Arzt dann eine Reihe von sicheren Ressourcen zur Verfügung, mit denen er auf den Notfall reagieren kann – zum Beispiel in einer isolierten, von SSE kontrollierten Browsersitzung.

Zero Trust Network Access (ZTNA) ist Ihnen sicher ein Begriff. ZTNA ist ist eine ausgezeichnete Lösung zur Erweiterung Ihres VPN (Virtual Private Network), um mehr Möglichkeiten für den Remote-Zugriff zu schaffen. Mit ZTNA wird Mitarbeitern der Zugriff auf einen Teil des Netzwerks verwehrt, der ihnen Verbindungen zu zahlreichen Diensten

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

ermöglichen könnte. Stattdessen erlaubt ZTNA nur eine Verbindung zu der Anwendung, die der jeweilige Mitarbeiter gerade nutzen möchte. Wie wir in unserem Beispiel mit dem Arzt gesehen haben, wird dem User nur so viel Netzwerkzugriff gewährt, wie er tatsächlich zur Ausführung der jeweiligen Aufgabe benötigt.

Wenn wir uns die Funktionsweise dieses Modells in seiner fortschrittlichsten Form ansehen, treten einige wichtige Konzepte zum Vorschein, an denen wir uns orientieren können:

- **Kontext:** Bevor es das SASE-Sicherheitsmodell gab, definierte das Netzwerk den Perimeter. Wer auf Ressourcen zugreifen wollte, musste diese Grenze überwinden. Heute wird Identität oft als der neue Perimeter des-Zero Trust Modells bezeichnet, weil die Identität zur Zugriffsgewährung überprüft werden muss. Dieses Konzept ist jedoch unzureichend. Ein besserer Ansatz ist die Bewertung des gesamten Kontexts, einschließlich der Identität und vieler anderer Variablen.
- **Least Privilege:** Bei Zero Trust wird immer nur ein Minimum an Zugriffsrechten gewährt. Der User erhält ausschließlich Zugang zu den Ressourcen, die er für die Arbeit benötigt. In seiner fortschrittlichsten Form versucht Zero Trust auch, festzustellen, ob zu viele Privilegien gewährt wurden, und passt das System entsprechend an.
- **Risikoeinstufung:** SSE stellt einen Aktivitätsverlauf bereit, damit Unternehmen sehen können, wie Mitarbeiter mit Anwendungen interagieren. Dieser Aktivitätsverlauf kann analysiert werden, um eine Darstellung der normalen Aktivitäten zu erhalten und verdächtige Aktivitäten in Echtzeit zu erkennen. Bei dieser Analyse werden Risikoeinstufungen für Mitarbeiter, Anwendungen und Websites erstellt. Diese Bewertungen liefern zusätzlichen Kontext, um zu bestimmen, welche Art von Zugriff gewährt werden soll.
- **Ressourcenverschleierung:** Beim Zero-Trust-Netzwerkzugriff (ZTNA) werden keine IP-Adressen offengelegt, die Benutzer und Ressourcen für Angriffe zugänglich machen können. Eine Verbindung ist erst möglich, nachdem der Kontext bewertet wurde. Alles ist standardmäßig verborgen (was die Sicherheit anbelangt, spielt Verschleierung tatsächlich eine Rolle, auch wenn in Informatikkursen manchmal das Gegenteil behauptet wird).
- **Kontinuierliches adaptives Vertrauen (wahrscheinlich das wichtigste Konzept auf dieser Liste):** Kontinuierliches adaptives Vertrauen bedeutet, Verbindungen zu überwachen und Zugriffsberechtigungen auf der Grundlage sich ändernder Kontextinformationen laufend anzupassen. Eine Person, die normalerweise Salesforce verwendet, will auf das Finanzsystem des CFO zugreifen? Red Flag:

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Zugriff und Berechtigung werden reduziert, die Risikoeinstufung erhöht und ein Verantwortlicher erhält eine Warnmeldung, damit die erforderlichen Maßnahmen ergriffen werden können. Jemand versucht, auf eine gefährliche Website zuzugreifen? Ein Fenster mit einer Warnung erscheint, bevor der Zugriff gewährt wird. Das Ziel besteht darin, ständig auf Änderungen im Kontext zu reagieren, damit Daten, Anwendungen und Menschen adäquat geschützt werden.

ERINNERN

Durch die Implementierung von SSE mit Zero-Trust-Prinzipien verkleinert sich die Angriffsfläche. Prozesse sind in hohem Maße datengesteuert, sodass sich der Sicherheitsstatus des Unternehmens bedeutend verbessert. Der Grad des von einer Person, einer Anwendung oder einer Website ausgehenden Risikos wird ständig neu bewertet. Die Sicherheit passt sich in Echtzeit an Veränderungen des Kontexts an.

Mit dieser auf kontinuierliches adaptives Vertrauen gerichteten Denkweise können wir uns der Frage zuwenden, wie SSE richtig implementiert werden sollte.

Vier einfache Schritte auf dem Weg zu SSE

Um SSE erfolgreich zu realisieren, müssen die meisten Unternehmen von einer On-Premises-Sicherheit innerhalb des definierten Netzwerkperimeter zu einer Cloud-basierten Sicherheit überwechseln, bei der der Kontext den Perimeter darstellt. Als Ausgangspunkt nehmen wir dabei die Situation, in der sich die meisten Unternehmen derzeit befinden: eine On-Premises-Firewall, die VPNs für den Remotezugriff umfasst, eine lokale Secure Web Gateway (SWG)-Appliance, die den Webzugriff kontrolliert, und vielleicht ein Abonnement für einen eigenständigen Cloud Access Security Broker (CASB), der die Nutzung von SaaS-Anwendungen schützt.

Schritt 1: Migration mobiler Mitarbeiter, um mehr Transparenz zu erhalten

Zunächst müssen Sie bewerten, was Ihre Mitarbeiter tun, und das aktuelle Risikoniveau zu bemessen. Am einfachsten ist es, mit Ihren mobilen Mitarbeitern zu beginnen, die potenziell das größte Risiko darstellen. Leiten Sie den Web- und SaaS-Verkehr dieser Arbeitskräfte über das SWG und den CASB von SSE. Diese sollten so genau wie möglich nach den bestehenden Richtlinien konfiguriert sein. Beobachten Sie dann, was passiert.

Dadurch erhalten Sie ein vollständigeres Bild von den Aktivitäten Ihrer Mitarbeiter. Unternehmen, die CASB oder SWG noch nicht nutzen, werden eine sehr große (und möglicherweise alarmierende) Anzahl von

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Aktivitäten entdecken, von denen sie bisher nichts wussten. Doch auch Unternehmen, die CASB und SWG bereits verwenden, erhalten viele wertvolle Einblicke.

Sicherlich werden Sie feststellen, dass mobile Mitarbeiter auf Anwendungen und Dienste zugreifen, von denen sie bisher nichts ahnten. Sie erfahren auch, wo genau sie arbeiten und welche Netzwerke sie nutzen.

Zu Schritt eins gehört auch noch, den Zugang zu internen Systemen im Rechenzentrum von VPNs auf den ZTNA von SSE zu migrieren. Dies erhöht nicht nur die Sicherheit, sondern verbessert auch das Nutzererlebnis. Stellen Sie sich das folgende Szenario vor: Sie haben eine undichte Wasserleitung und der Klempner kommt zu Ihnen nach Hause, während Sie in der Arbeit sind. Auf dem Weg zwischen seinem Lastwagen und Ihrem Badezimmer hat er Zugang zu Ihrem gesamten Grundstück. Vielleicht lässt er die ganze Zeit die Haustür offen. Währenddessen haben Sie keine Ahnung, was vor sich geht. Mit ZTNA haben Sie plötzlich einen Teleportations-Button, der Ihnen nahezu magische Fähigkeiten verleiht. Wenn der Klempner auftaucht, können Sie ihn ohne Zwischenstopps von seinem Wagen zum Badezimmer und zurück beamen. Das ist ein Beispiel für Zugangskontrolle, die für das Zeitalter der Cloud perfektioniert wurde.

Schritt 2: Migration aller übrigen Mitarbeiter und unternehmensweite Datenklassifizierung

Der zweite Schritt besteht darin, alle Mitarbeiter, die vor Ort arbeiten, unter den Schutz von SSE zu stellen, damit Sie ihren Zugriff auf Cloud-basierte Anwendungen und Dienste effektiv kontrollieren können. Nun sind alle Mitarbeiter – ob vor Ort oder mobil – durch SSE geschützt. Dieser Schritt führt zur Transformation Ihrer Netzwerkarchitektur. Alle Mitarbeiter passieren nun den nächstgelegenen POP des SSE-Anbieters, der den Datenverkehr optimal an das Ziel weiterleitet – oft mit weniger Zwischenstationen als im öffentlichen Internet. Jetzt haben Sie die Möglichkeit, das Netzwerk zu vereinfachen und teure private Netzwerke, die nicht mehr benötigt werden, endlich in den Ruhestand zu versetzen. Als Teil dieser Netzwerkumstellung kann ein Software-Defined Wide-Area-Networking (SD-WAN) eingeführt werden, damit der Datenverkehr von Zweigstellen selektiv weitergeleitet werden kann.

Das hilft Ihnen dabei, zu verstehen, welche Daten, Anwendungen, Websites oder Dienste für Mitarbeiter von Interesse sind. Da SSE in der Lage ist, Aktivitäten zu erfassen und zu analysieren, nehmen der Umfang und die Tiefe des Kontexts in dieser Phase dramatisch zu. Der Sicherheitsstatus, der bei diesem Schritt durch Ihre SSE-Richtlinien widergespiegelt

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

wird, sollte wahrscheinlich ähnlich wie bei den durch SSE ersetzten Legacy-Produkten sein. Es ist wichtig, zunächst einen bekannten Zustand zu erreichen, bevor neue Funktionen hinzugefügt werden, für die möglicherweise Schulungen und Trainings erforderlich sind.

Mit diesem neuen Kontext können Sie den Grundstein für eine bessere Sicherheit legen und Daten, Anwendungen und Personen auf der Grundlage ihres Verhaltens und des mit ihnen verbundenen Risikos klassifizieren. Wenn diese Klassifizierung abgeschlossen ist, kann das SSE-System mit Hilfe interner und externer Daten in Echtzeit Risikoeinstufungen für Mitarbeiter, Anwendungen und Websites erstellen. Nun kann ein Großteil der alten Sicherheitsinfrastruktur in den Ruhestand versetzt werden und Sie können zur nächsten Phase übergehen, in der SSE ein neues Sicherheitsniveau erreicht.

Schritt 3: Implementierung von kontinuierlichem adaptiven Vertrauen und erweiterten Diensten

Bis zu diesem Punkt hat sich die User Experience bei Ihren Nutzern nicht grundlegend verändert. Dies passiert erst durch Schritt 3. Das Nutzerlebnis verbessert sich erheblich, da sich die Sicherheit kontextabhängig anpasst.

ERINNERN

Kontinuierliches adaptives Vertrauen bewertet den Kontext, um ein Gleichgewicht zwischen Risiko und Vertrauen herzustellen und den richtigen Personen zur richtigen Zeit das richtige Maß an Zugriff auf die richtigen Informationen zu gewähren. Dadurch können viel detaillierter Sicherheitsrichtlinien festgelegt werden. Es werden auch häufiger Warnmeldungen oder Empfehlungen ausgegeben, zum Beispiel, wenn jemand eine riskante Aktivität ausführen will. In diesem Fall werden Mitarbeiter auf genehmigte Aktivitäten hingewiesen.

Mit SSE wissen Sicherheitsexperten, welche Daten sensibel und welche Anwendungen und Websites riskant sind. Wenn dieses Wissen mit Funktionen wie DLP kombiniert wird, kann das Sicherheitspersonal genau kontrollieren, was Mitarbeiter mit sensiblen Daten tun – und zwar auf einer Ebene, die es im Sicherheitsbereich noch nie gegeben hat. Anstelle einer einfachen Entscheidung über Blockieren oder Zulassen entwickelt sich die Gewährung des Zugriffs zu einem "großen Ganzen".

Kontinuierliches adaptives Vertrauen ermöglicht auch das Hinzufügen weiterer Dienste. Nehmen wir zum Beispiel an, ein Arzt möchte eine Website besuchen, die als riskant eingestuft wurde. Er erhält eine Warnmeldung, lässt sich dadurch jedoch nicht von seinem Ziel abhalten. SSE kann den Arzt in diesem Fall in eine RBI-Sitzung (Remote Browser Isolation) umleiten – einen Browser, der auf einer virtuellen Maschine

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

beim SSE-Anbieter läuft, wodurch das Risiko erheblich verringert wird. Je nach Bedarf können weitere fortgeschrittliche Dienste hinzugefügt werden.

Schritt 4: Proaktives Risikomanagement mit dynamischer Analyse und Risikoeinstufung

In Schritt 4 kann das für SSE verantwortliche Team damit beginnen, proaktiv nach Risiken zu suchen und diese aus der Umgebung zu entfernen. Der Fortschritt dieses Prozesses kann durch das Tracking der Risikoeinstufungen von Mitarbeitern, Anwendungen und Websites gemessen werden. Letztendlich soll der Datenverkehr zu risikobehafteten Websites und die Häufigkeit risikobehafteter Handlungen reduziert werden. Eine weitere Methode ist die Reduzierung von Berechtigungen durch die Verfolgung von Nutzungsmustern und die Beseitigung übermäßiger Privilegien.

An diesem Punkt sollte der Fokus auf einigen der übergeordneten Sicherheitskontrollen wie DLP und der Neutralisierung von Bedrohungen liegen, um die Fähigkeiten von CASB, SWG, ZTNA und Firewall-as-a-Service (FWaaS) zu erweitern. Bei SSE funktionieren diese Kontrollen viel besser als bei ihren getrennt eingesetzten On-Premises-Äquivalenten, und sie verfügen außerdem über zusätzliche Fähigkeiten. Dank seiner auf maschinellem Lernen basierenden Erkennungsfunktionen kann DLP zum Beispiel sensible Dokumente in Echtzeit identifizieren und entsprechend reagieren.

TIPP

Das Risikomanagement wird zusätzlich durch Digital Experience Management (DEM), Cloud Security Posture Management (CSPM) und SaaS Security Posture Management (SSPM) verbessert. Ihre fortschrittlichen Methoden sorgen für konsistente Verfügbarkeit und Leistung und tragen dazu bei, Konfigurationsfehler zu finden und zu beheben.

ERINNERN

Wie diese Schritte im Einzelnen aussehen, hängt von Ihrer konkreten Situation ab. Die hier beschriebenen Schritte sollen lediglich den Prozess umreißen, den die meisten Unternehmen bei der vollständigen Implementierung von SSE durchlaufen.

Netzwerktransformation und andere Sicherheitsbereiche

TIPP

Die Implementierung von SSE ist ein wichtiger Schritt nach vorn und ein unverzichtbarer Schritt für SASE. Um eine sorgenfreie Sicherheit zu erreichen, muss sich allerdings auch der Rest der Sicherheitslandschaft weiterentwickeln, damit alle wichtigen Elemente zusammenarbeiten

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

können. Die meisten Unternehmen gehen zu einem Work-from-anywhere-Modell über. Die Vorteile einer Sicherheit, die an jedem Ort und zu jeder Zeit verfügbar ist, liegen dabei klar auf der Hand. Dieser Trend führt zu einer natürlichen Abkehr von VPN und privaten Netzwerkverbindungen, die mit der Einfachheit und den Kostenvorteilen von SSE nicht konkurrieren können.

Ein besonders wichtiger Vorteil ist jedoch, dass die gesamte technologische Infrastruktur durch die Einführung von SSE (und SASE) vereinfacht wird. Bei dem veralteten Modell waren die Sicherheitskontrollen zum Schutz vor unbefugtem Zugriff in das Unternehmensnetzwerk integriert, da dieses Netzwerk der einzige Pfad zu den Daten war. Beim neuen Modell bilden die strategisch positionierten Points of Presence des SSE-Anbieters die Pfade zu den Daten und übernehmen nicht nur die Zugangskontrolle, sondern auch die vollständige Überprüfung des Datenverkehrs. Das zugrundeliegende Netzwerk kann sich dann auf seine eigentliche Aufgabe konzentrieren und die Bits & Bytes so schnell und effizient wie möglich durch die Welt schicken.

Identity and Access Management (IAM)-Systeme übernehmen die wichtige Aufgabe der Authentifizierung von Mitarbeitern. Viele dieser Systeme sind bereits über Application Programming Interfaces (APIs) hochgradig konfigurierbar. Außerdem sind sie so konzipiert, dass sie sich in andere Systeme integrieren lassen – eine notwendige Funktion für jede SSE-Implementierung. Dank einiger Verbesserungen kann IAM-Technologie jetzt noch mehr Kontext, Überwachungs- und erweiterte Authentifizierungsfunktionen zur Verfügung stellen, von denen SASE und SSE profitieren. Einen noch größeren Nutzen zieht SSE aus Endpoint Protection-Plattformen (EPP). Sie erfassen wichtige Signale (und erzeugen dadurch mehr Kontext), führen eine detaillierte Überwachung durch und enthalten Mechanismen zur Verhaltenskontrolle und Sicherheitskonfiguration. Sie können Ihren SSE-Implementierungsplan mit einer entsprechenden EPP-Entwicklung synchronisieren, um den maximalen Nutzen aus Ihren Sicherheitsinvestitionen zu ziehen.

SASE und SSE werden die Rolle des Rechenzentrums zweifellos weiter verändern. Nach dem Siegeszug der Cloud verlor das Rechenzentrum seine Stellung im Mittelpunkt aller sicherheitsrelevanten Aktivitäten. SSE verlagert die Sicherheit aus dem Rechenzentrum in die Cloud.

ERINNERN

Rechenzentren werden in den meisten Unternehmen nach wie vor eine wichtige Rolle spielen. Dafür gibt es einige gute Gründe, darunter Kostendruck, regulatorische Anforderungen, Risikomanagement und dem Nutzen, den bestimmte Arten von Recheninfrastruktur weiterhin haben. Das Rechenzentrum wird nun einer von vielen Standorten sein, an denen sich wichtige Anwendungen befinden und von SSE geschützt werden.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Die Vorteile von SSE für Ihr Geschäft

Cyberrisiken sind eine Priorität für die meisten Führungskräfte. Wie wir jedoch in Kapitel 2 gesehen haben, ist Sicherheit kein Selbstzweck. Security hat die Aufgabe, den Werte zu schützen, der durch die Systeme des Unternehmens geschaffen werden. Viele Unternehmen sind in die Cloud gewandert, weil dies geschäftlich sinnvoll ist. Die Aufgabe einer SASE-Architektur, einschließlich SSE, ist der Schutz von Anwendungen, Daten und Menschen. Dies lässt sich folgendermaßen in geschäftlichen Nutzen umsetzen:

Die Sicherheit steht der Produktivität nicht mehr im Weg. Die geschäftliche Agilität wird gefördert und die Sicherheitsteams müssen nicht mehr die Rolle des Spielverderbers übernehmen, da die vom Unternehmen gewünschten Schritte nun richtig abgesichert werden können. Sicherheitsbedingte Spannungen werden erheblich reduziert. Produktentwicklungs- und Wartungsprozesse werden gestrafft, da die Sicherheit leichter integriert werden kann. Cloud-basierter SSE eignet sich perfekt für den Schutz einer Multi-Cloud-Umgebung.

Führungskräfte können sich darauf verlassen, dass die für die sichere Nutzung von Cloud-Ressourcen erforderlichen Kontrollen richtig ausgeführt, geprüft und verwaltet werden. Der Prozess zur Verwaltung der mit Menschen, Daten und Anwendungen verbundenen Risiken wird wesentlich ausgefeilter. Dasselbe gilt für die zur Risikominderung eingesetzten Mechanismen. Mit SSE können Risiken proaktiv erkannt und systematisch eliminiert werden. Da die Sicherheit den Daten folgt, können sich Führungskräfte in dem guten Gefühl wiegen, dass die wichtigsten Vermögenswerte des Unternehmens zuverlässig geschützt sind.

Das Sicherheitsteam arbeitet viel einheitlicher und geschäftsorientierter. Statt einem SWG-Verantwortlichen, einem CASB-Spezialisten und einem Firewall-Experten haben Sie ein Team, das sich auf das Gesamtbild konzentriert und mehr Einblicke hat, um proaktiv handeln zu können.

ERINNERN

Wenn SSE erfolgreich realisiert wird, lässt sich eine bessere Welt der Sicherheit schaffen: eine sorgenfreie Sicherheit, von der jeder im Unternehmen profitieren wird.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Kapitel 5
Ungefähr 10 do's & don'ts, die wir Ihnen auf dem Weg zu SSE mitgeben möchten

Eine wichtige Erkenntnis auf dem Weg zu einer sicheren und flexiblen Cloud ist die, dass Ihre derzeitige IT-Organisation nicht für dieses Ziel konzipiert wurde. Es ist völlig normal, dass die IT-Organisation die vorhandene Technologiearchitektur widerspiegelt. In Ihrem Unternehmen sind möglicherweise unterschiedliche Personen oder Teams für Cloud Access Security Broker (CASBs), Secure Web Gateways (SWGs), Virtual Private Networks (VPNs) und Firewalls verantwortlich. Diese Mitarbeiter können einem Security Operations Center (SOC)-Team oder einem Network Operations Center (NOC)-Team angehören bzw. mit diesen Teams zusammenarbeiten. Der Vorschlag, eine neue integrierte Architektur für Secure Access Service Edge (SASE) und Security Service Edge (SSE) zu implementieren, in der Sicherheit und Netzwerke zu einer stabilen Partnerschaft zusammenwachsen, könnte daher bei manchen Beteiligten auf Ablehnung stoßen. Es liegt in der Natur des Menschen, sich Veränderungen zu widersetzen, nicht zuletzt aus Angst, die Kontrolle über einen Bereich zu verlieren, in den man viel Arbeit investiert hat.

SASE und SSE bieten zahlreiche taktische Vorteile, die die Qualität der Sicherheitsinfrastruktur verbessern und die Reichweite von Sicherheitsprozessen vergrößern. Gleichzeitig bringen sie strategische Vorteile mit sich, da sie geschäftliche Abläufe beschleunigen können. Die folgenden Abschnitte enthalten einige Empfehlungen für die erfolgreiche

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Einführung von SASE und SSE. Zunächst stellen wir Ihnen vier Prinzipien vor, die Ihnen auf dem Weg zu SASE uns SSE helfen sollen. Dann weisen wir auf vier Fehler hin, die Sie unbedingt vermeiden sollten.

Stellen Sie die Daten in den Mittelpunkt

Bei SSE folgt die Sicherheit den Daten, unabhängig davon, wo sich diese Daten befinden. Es spielt also keine Rolle, ob Sie Daten in Google Workspace und Microsoft 365, in einer Software-as-a-Service (SaaS)-Anwendung oder auf einem Cloud-Objektspeicher erstellen. SSE ist immer da und schützt diese Daten.

Da SSE zum primären Prüfpunkt wird, der auch die Klassifizierung von Daten ermöglicht, ist es besonders wichtig, den Zweck und den Speicherort aller Daten zu bestimmen. Dieses Wissen kann Ihnen dabei helfen, sensible Daten ortsunabhängig zu priorisieren.

Nutzen Sie die Vorteile der Integration

In jeder Phase des Incident-Response-Prozesses müssen Automatisierungs- und Integrationsfähigkeiten aufgebaut werden, so dass alle Sicherheitskomponenten eine fein abgestimmte Maschine bilden. Bei diesem Prozess werden Informationen aus unterschiedlichen Systemen extrahiert und integriert, damit Vorgänge analysiert werden können. Es ist auch wichtig, ein gutes Team zusammenzustellen und wo immer möglich, automatisierte Abläufe einzuführen.

SSE integriert alle Sicherheitsdienste, die für die Cloud-Sicherheit wichtig sind. Gleichzeitig ist SSE aber auch Teil eines größeren Ökosystems wichtiger Sicherheitsdienste. Identity and Access Management (IAM)-Systeme, Endpoint Protection P

lattformen (EPP) und Security Information and Event Management (SIEM)-Tools sind einige der Schlüsselkomponenten, die mit SSE-spezifischen Funktionen zusammenarbeiten, um eine umfassende Sicherheit zur Verfügung zu stellen und die schnelle Diagnose und Lösung von Problemen zu unterstützen.

Denken Sie daran, dass auch Angreifer in die Cloud wandern

Was die Reichweite und die Qualität der Sicherheit anbelangt, stellen SSE und SASE einen großen Entwicklungssprung dar. Natürlich ist man erst einmal zufrieden, wenn die Grundkonfiguration eingerichtet ist. Man sollte jedoch nie vergessen, dass auch Angreifer die Cloud zu ihrem Vorteil nutzen. Laut dem Cloud and Threat Report von Netskope (`www.netskope.com/blog/july-2021-netskope-cloud-and-threat-report`) stieg der Anteil von Malware, die über Cloud-Anwendungen

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

verbreitet wird, von 50 Prozent im zweiten Quartal 2020 auf ein Allzeithoch von 68 Prozent im zweiten Quartal 2021 an. Mit SSE können Sie solchen Angreifern einen Schritt voraus sein, vorausgesetzt, sie lernen ständig weiter und passen sich an neue Gegebenheiten an.

Machen Sie Sicherheit zu einem wichtigen Teil der Unternehmensstrategie

Der Security muss von Anfang an eine zentrale Rolle in der Unternehmensstrategie zukommen. Die besten Anwendungen und die Cloud nutzen Ihnen wenig, wenn diese Anwendungen und ihre User nicht adäquat geschützt werden können. Zum Glück kann SSE Ihren Sicherheitsteams dabei helfen, Business Enabler zu werden. Je besser das Sicherheitsteam die Geschäftsziele und die damit verbundenen Auswirkungen für die Sicherheit versteht, desto häufiger kann es positive Entscheidungen zum Schutz des Unternehmens treffen.

TIPP

Damit eine SASE- und SSE-Implementierung erfolgreich ist, müssen die Befürworter des Programms erklären können, warum die Vorteile der Cloud-Sicherheit für die Gesamtstrategie wichtig sind. Die Botschaft sollte lauten: Wir haben in die Cloud investiert, um unser Unternehmen umzugestalten und bessere Ergebnisse zu erzielen. Jetzt müssen wir diese Investition schützen. Der Wunsch, dieses Ziel zu erreichen, ist wohl die beste Motivation für eine enthusiastische Einführung von SASE und SSE.

Vermeiden Sie Silodenken

SASE und SSE lösen die heiklen Probleme, die häufig mit Cloud-Projekten einhergehen. Versuchen Sie nicht, CASB, SWG und Zero Trust Network Access (ZTNA) als unabhängige Projekte zu implementieren. Dies führt lediglich dazu, dass Sie mit mehreren Nischenanbietern verhandeln müssen, die Ihnen viel versprechen, doch letztendlich vom eigentlichen Ziel ablenken. Das Ziel lautet, die Cloud durch eine kontextbezogene Plattform zu schützen. Seien Sie nicht überrascht, wenn der mit SASE und SSE einhergehende Wandel von einigen Seiten auf Widerstand stößt.

WARNUNG

Der Prozess vollzieht sich langsamer, wenn man das Problem mit der für herkömmliche IT-Silos typischen Einstellung angeht. Diese „Cylinders of Excellence“ bewahren alte Denkweisen in einer neuen Welt. Sicherheit darf nicht als reines Netzwerkproblem betrachtet werden. Führen Sie keine Netzwerkgespräche über ein Sicherheitsproblem. Im Rahmen einer voll funktionsfähigen SASE-Architektur stellt SSE jetzt die entscheidenden Sicherheitsdienste zur Verfügung, die vor Bedrohungen schützen und gleichzeitig Transparenz und Kontrolle bieten.

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

Übernehmen Sie keine alten Regeln

Manche IT-Kräfte haben richtiggehend Angst vor ihren Firewalls, weil sich dort Regelwerke angesammelt haben, die in längst vergangenen Zeiten erstellt wurden. Das Gleiche gilt für andere Sicherheitstechnologien, die komplexe Regeln und Konfigurationseinstellungen erfordern, um die gewünschten Ergebnisse zu erzielen. Bei SSE ist das anders. Es gibt zwar weiterhin Regeln und Konfigurationen, aber ein Großteil wird durch die Festlegung von Richtlinien erledigt, die die gewünschten Ergebnisse beschreiben. Bei effektiver Implementierung verwaltet SSE die Einzelheiten Ihrer Regelinteraktionen selbstständig. Sie müssen sich also nicht um die Konfiguration Ihrer alten Technologie kümmern, sondern können sich stattdessen auf die Sicherheitziele konzentrieren, die Sie mit SSE erreichen wollen.

Die meisten SSE-Produkte bieten auch Cloud Security Posture Management und SaaS Security Posture Management an, die Ihnen weitere wichtige Funktionen zur Verfügung stellen können.

Unterschätzen Sie das Rechenzentrum nicht

Wer die Vorteile von SASE und SSE erkannt hat, kann leicht zu dem Schluss kommen, dass das klassische Rechenzentrum nicht mehr wichtig ist. Rechenzentren wird es jedoch in irgendeiner Form immer geben; schließlich ist die Cloud nichts anderes als eine Ansammlung von Rechenzentren mit Zugriff über Application Programming Interfaces (APIs). In seiner neuen Rolle ist das Rechenzentrum ein Ort, an dem wichtige Computing-Workloads und Anwendungen ausgeführt werden. In der Sicherheitsinfrastruktur spielt es zwar nicht mehr die Hauptrolle, die es früher innehatte, doch es übernimmt jetzt eine wichtige Nebenrolle.

Haben Sie keine Angst vor Veränderungen

Lassen Sie sich nicht von der Angst vor SASE und SSE bremsen. Ja, es wird eine veränderte Architektur und neue Produkte geben, die es zu beherrschen gilt. Das ist nicht immer eine leichte Aufgabe, da sich alle Mitarbeitern des Unternehmens mit diesen Produkten auseinandersetzen müssen. Durch eine SSE-Implementierung werden Sie mehr über Ihre Mitarbeiter, Daten, Anwendungen, Websites und die Anwendungen von Drittanbietern erfahren. Dieses Wissen öffnet Ihnen dann die Tür zu weiteren Automatisierungsmöglichkeiten, die Sie dabei unterstützen können, Fehler schneller zu finden und effektive Maßnahmen zu ergreifen. Im Vergleich zu Ihrem derzeitigen Sicherheitsstatus werden Sie mit SSE ein völlig neues Sicherheitsniveau erreichen: sorgenfreie Sicherheit!

Urheberrechtlich geschütztes Material © 2022 John Wiley & Sons, Inc. Jede Verbreitung, Weitergabe oder unbefugte Nutzung ist strengstens untersagt.

SSE bezeichnet eine Reihe von Sicherheitsdiensten, die eine erfolgreiche SASE-Architektur ermöglichen. Dieses Buch zeigt Ihnen, wie Sie SSE erfolgreich realisieren können.

Auf der SASE-Reise brauchen Unternehmen einen verlässlichen Partner, der integrierte Plattformfunktionen bieten kann. Was sie nicht brauchen, sind Anbieter, die mit vollmundigen Marketingsprüchen behaupten, irgendeine Form von „SASE"- oder „SSE"-Angebot im Portfolio zu haben. Dieses Buch ist Ihr praktischer Leitfaden zu SSE und SASE, einschließlich der Frage, warum beide Konzepte so entscheidend für den Aufbau von Cloud-zentrierten Sicherheits- und Netzwerkarchitekturen der Zukunft sind und warum man heute in Security Service Edge (SSE) investierten sollte.

Im Buch ...

- Definition von SASE und SSE
- Die entscheidende Rolle von Zero Trust
- Schutz kritischer Unternehmensdaten in der Cloud
- Sicherheit für dezentrale Mitarbeiter
- Fehlervermeidung bei der Implementierung von SSE und SASE

netskope

Netskope leaders **Jason Clark** (CSO and CMO) and **Steve Riley** (Field CTO) are widely acknowledged authorities in cloud computing technology, cybersecurity, and networking, with decades of experience from global organizations including Gartner, Optiv, Riverbed, and Websense.

Besuchen Sie Dummies.com®
um sich Videos und schrittweise Bildanleitungen anzusehen oder Produkte zu kaufen!

ISBN: 978-1-119-89723-1
Nicht für den Wiederverkauf

9 781119 897231

für dummies®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.