netskope

5 Kritische SASE-Anwendungsfälle für hybride Arbeitsumgebungen

5 Kritische SASE-Anwendungsfälle für hybride Arbeitsumgebungen

Die Pandemie hat die Einführung von hybriden Arbeitsmodellen beschleunigt, die sich auf Cloud-basierte Netzwerke, Rechenzentren und Anwendungen stützen. Und obwohl 63 % der wachstumsstarken Unternehmen hybrides Arbeiten einsetzen, kann dieser Ansatz eine Herausforderung für unzureichend vorbereitete Netzwerk- und Sicherheitsteams darstellen. Unzuverlässige Heimnetzwerke mit hohen Latenzzeiten können die Produktivität der Benutzer beeinträchtigen und es können Sicherheitslücken durch mangelndes Cloud-Bewusstsein entstehen. Gleichzeitig stellen teure und komplexe alte Netzwerk- und Sicherheitssysteme ein weiteres Hindernis für die Einführung dar. Aus diesen und anderen Gründen ist die Nutzung von Security Service Edge (SSE)-Funktionen als Teil einer Secure Access Service Edge (SASE)-Architektur jetzt entscheidend für erfolgreiche hybride Implementierungen.

netskope

[1] Quelle: Accenture https://www.accenture.com/us-en/blogs/business-functions-blog/hybrid-workforce

5 Critical SASE Use Cases for Hybrid Work Environments

Anwendungsfall #1 | Sicherstellung von robuster Netzwerkleistung, Benutzerfreundlichkeit und Sicherheit

Anwendungsfall #2 | Sichtbarkeit und Kontrolle in der Cloud beibehalten

Anwendungsfall #3 | Erzielung von Kosteneinsparungen und betrieblicher Effizienz

Anwendungsfall #4 | Schutz vor Cloud-basierten Saas- und Web-Bedrohungen

Anwendungsfall #5 | Vermeidung von Datenverlusten, Diebstahl und Insider-Risiken

netskope

Sicherstellung von robuster Netzwerkleistung, Benutzerfreundlichkeit und Sicherheit

Bei der hybriden Arbeitsweise müssen Sicherheitsteams ein Gleichgewicht zwischen Sicherheit auf der einen Seite und Netzwerkleistung/Benutzererfahrung auf der anderen Seite finden. Denn jede Auswirkung auf die Benutzer birgt das Risiko, dass diese nach Möglichkeiten suchen, die Sicherheitskontrollen zu umgehen. Veraltete Sicherheitslösungen wirken sich negativ auf die Benutzerfreundlichkeit aus, da sie entweder isoliert sind, was die Latenz im Netzwerk erhöht, oder zentralisiert sind, was bedeutet, dass der Datenverkehr durch den Perimeter-Sicherheits-Stack geleitet werden muss und auf langsame, veraltete Technologien wie MPLS und VPN angewiesen ist.

Achten Sie auf die folgenden SASE-Funktionen zur Verwaltung dieses Anwendungsfalls

Eine **allgegenwärtige Cloud-native Architektur** mit globalen Rechenzentren macht es überflüssig, dass der Datenverkehr aus der Ferne zur Sicherheitsüberprüfung durch das zentrale Netzwerk geleitet werden muss. Vielmehr ermöglicht eine Cloud-native Architektur die Einbettung der Sicherheitsinspektion in schlanke, direkt ins Internet führende Datenverkehrsmuster, die die Latenzzeit verringern. Darüber hinaus ermöglicht eine konvergierte SSE-Plattform, die den für SASE erforderlichen Sicherheitsstapel bildet, einen "Single-Pass "-Ansatz, bei dem die gesamte Sicherheitsprüfung an einer Stelle durchgeführt wird, so dass die Sicherheit für den Benutzer als effizienter "Bump in the Wire" mit geringer Latenz transparent wird.

Zero-Trust Network Access (ZTNA) bietet eine weitere Möglichkeit, um sicherzustellen, dass der Datenverkehr nicht zurück zum Unternehmensnetzwerk geleitet werden muss. Durch den Einsatz von ZTNA können Sicherheits- und Netzwerkteams einen effizienten und sicheren Zugriff auf private Anwendungen ermöglichen, unabhängig davon, ob sie sich im Unternehmensnetzwerk oder in der Cloud befinden.

Edge-Sicherheitsfunktionen tragen auch dazu bei, die Latenzzeit des Netzwerks zu verringern und gleichzeitig die allgemeine Zuverlässigkeit des Netzwerks zu erhöhen. Achten Sie auf Cloud-native Plattformen, die an jedem Servicepunkt volle Rechenleistung für Echtzeit-Inline-Verarbeitung in großem Umfang ermöglichen und über direkte Peering-Partnerschaften mit Cloud-, Content-Delivery-Netzwerken und SaaS-Anbietern verfügen, um zusätzliche Leistungssteigerungen zu erzielen.

Die **enge Integration mit SD-WAN-Lösungen (Software-defined Wide Area Network)** bedeutet, dass Sie langsame und kostspielige MPLS-Verbindungen vermeiden können, die den gesamten Datenverkehr von Zweigstellen zurück in das Unternehmensnetzwerk zwingen. Stattdessen können Ihre Benutzer von einer schnellen, erschwinglichen "Direct-to-Internet"-Breitbandverbindung zu Web- und Cloud-Anwendungen profitieren und so ihre Produktivität steigern.

Tools für **das Digital Experience Management (DEM)** bieten Unternehmen eine detaillierte End-to-End-Transparenz der Benutzeraktivitäten und verwertbare Einblicke in die Netzwerk- und Anwendungsleistung, was die Fehlerbehebung und Optimierung der Benutzererfahrung erleichtert. Mit den DEM-Funktionen können Sie sicher sein, dass Ihre Cloud-Sicherheit den Schutz bietet, den Sie brauchen, ohne dabei Leistung zu kompromittieren.

Sichtbarkeit und Kontrolle in der Cloud bewahren

Herkömmliche Sicherheitsarchitekturen haben Schwierigkeiten, die Sicherheitstransparenz und -kontrolle aufrechtzuerhalten, wenn Anwendungen und Daten in die Cloud verlagert werden. Beim hybriden Arbeiten müssen Unternehmen das zusätzliche Sicherheitsrisiko minimieren, das entsteht, wenn nicht verwaltete Geräte und private/öffentliche Netzwerke auf Unternehmensressourcen zugreifen können. Netzwerkteams können nicht zulassen, dass Sicherheitskontrollen die Netzwerkleistung beeinträchtigen. Infolgedessen entscheiden sich einige dafür, Sicherheitskontrollen zu umgehen und das Unternehmen einem Risiko auszusetzen.

Achten Sie auf die folgenden SSE-Funktionen, um diesen Anwendungsfall in einer SASE-Architektur zu verwalten:

Eingebettete Datenschutztechnologien, die überall dort greifen, wo Daten gespeichert sind und die den Zugriff auf sensible Daten und das Hochladen von Daten durch externe Mitarbeiter auf nicht verwaltete Cloud-Anwendungen oder Websites überwachen und verhindern.

Technologien zum Schutz vor Bedrohungen, einschließlich Sandboxing und Remote-Browser-Isolierung, die selbst die fortgeschrittensten Angriffe erkennen und verhindern. Suchen Sie nach Tools, die in der Lage sind, Malware von Cloud-basierten Bedrohungen in der gesamten hybriden Arbeitsumgebung und in Echtzeit zu erkennen und zu stoppen. Der richtige Ansatz hilft dabei, Datenexfiltration und Insider-Bedrohungen zu bekämpfen, bei Kontokompromittierung zu warnen und anormales Benutzerverhalten aufzuzeigen.

Risikomanagement-Technologien, die die Cloud-Sicherheitslage von Unternehmen automatisch bewerten und verbessern. Diese Tools sollten in der Lage sein, die gesamte Bandbreite der Cloud-Apps und -Dienste des Unternehmens zu scannen, um Inhalt und Kontext zu verstehen, z. B. Unternehmens- und persönliche Instanzen, App-Risiko und Datensensibilität, und so adaptive Kontrollen zu ermöglichen, die genau den Bedürfnissen des Unternehmens entsprechen.

Erweiterte Verhaltensanalysen mit KI/ML-Modellen haben das Potenzial, unbekannte Bedrohungen und anomale Verhaltensmuster zu erkennen, die in Netzwerkdaten verborgen sind. Das macht sie zu einem unverzichtbaren Bestandteil jeder umfassenden Cyber-Sicherheitslösung für hybrides Arbeiten. Der Schlüssel zum Erfolg liegt darin, eine Lösung zu finden, die in der Lage ist, das gesamte Spektrum der Benutzeraktivitäten über SaaS-Anwendungen, die Cloud-Infrastruktur und die von den Benutzern besuchten Websites zu erfassen.

Reverse-Proxy-Funktionen, die es nicht verwalteten Geräten ermöglichen, auf Unternehmensressourcen zuzugreifen, ohne die Unternehmenssicherheit zu gefährden. Diese Funktion bietet eine Pufferzone zwischen externen Geräten und internen Systemen, so dass Remote-Mitarbeiter nicht direkt auf das Netzwerk zugreifen können, ohne zuvor vom Reverse-Proxy überprüft worden zu sein.

Zero-Trust Network Access (ZTNA) bietet einen hochgradig granularen Zugriff auf Anwendungen und Ressourcen und reduziert das Risiko von Seitwärtsbewegungen, das mit der Gewährung von netzwerkweitem Zugriff für VPN-Benutzer verbunden ist. Anders als bei VPNs bietet ZTNA einen kontextabhängigen, risikooptimierten Anwendungszugang und keinen uneingeschränkten Netzwerkzugang. Mit einer “Inside-Out”-Konnektivitätsarchitektur minimiert ZTNA die gesamte Angriffsfläche, da Protokolle und Dienste nicht mehr dem öffentlichen Internet ausgesetzt sind.

Schutz vor Cloud-basierten SaaS- und Web-Bedrohungen

Da hybrides Arbeiten Anwendungen, Daten und Benutzer außerhalb der Netzwerkgrenzen einbindet, wird die Cloud zur neuen Angriffsfläche für Unternehmen. Cyberkriminelle haben sich die Cloud zu eigen gemacht und nutzen sie, um erfolgreich Bedrohungen zu verbreiten. Durch die Nutzung vertrauenswürdiger Domänen, gültiger Zertifikate und Instanzen der gleichen verwalteten Anwendungen, die Unternehmen selbst verwenden, können diese Bedrohungen leicht unbemerkt bleiben. Alle Stufen der Cyber-Kill-Chain sind jetzt Cloud-fähig, von der Aufklärung bis zur Datenexfiltration und Persistenz.

Achten Sie auf die folgenden SSE-Funktionen zur Verwaltung dieses Anwendungsfalls:

Der **erweiterte Schutz vor Bedrohungen** bietet mehrere Abwehrmechanismen zur Erkennung, nachdem alle möglichen Präventionsprüfungen abgeschlossen sind. Dazu gehören die Entschleierung und das rekursive Entpacken von Dateien, die Analyse vor der Ausführung und Heuristiken, Bare-Metal-Sandboxing, Machine-Learning-Analysen sowie Verhaltensanalysen zur Erkennung von Insider-Bedrohungen, Account-Kompromittierung und Datenexfiltration.

Zugangsdaten in Form von Formularen — da Identität, Anwendungen und Daten die neuen Sicherheitsebenen sind, überrascht es nicht, dass sich Cyberangriffe auf den Diebstahl von Zugangsdaten und Brute-Force-Angriffe konzentrieren. Verwenden Sie Cloud DLP, um festzustellen, ob Anmeldedaten in unerwünschten Webformularen veröffentlicht werden, die von Cyberkriminellen erstellt wurden und sich als vertrauenswürdige verwaltete Anwendungen und Instanzen ausgeben. Diese Art von Cloud-Phishing lässt sich leicht durch herkömmliche Endpunkt-, E-Mail- und Web-Abwehrsysteme umgehen.

Der **Austausch von Bedrohungsdaten** ist ein weiterer Vorteil der technologischen Konvergenz in der Cloud (siehe oben). Die verschiedenen Elemente einer SSE-Lösung können Informationen austauschen, wodurch die Wahrscheinlichkeit steigt, dass cloudbasierte Bedrohungen entdeckt werden. Außerdem können Investitionen in Bedrohungsdaten automatisiert werden, um sie mit Tools wie Cloud Threat Exchange (CTE) zu teilen, und Unternehmen können vermeiden, dass ihre Webfilterkonfiguration überlastet wird.

Die **Erforschung von Cloud-Bedrohungen** konzentriert sich auf Cloud-fähige Bedrohungen und erfordert die Sichtbarkeit von Daten und Kontext innerhalb von Apps und Cloud-Diensten für den Benutzerverkehr. Wenn Ihre alte Sicherheitslösung die Daten in der Cloud-Anwendung nicht sehen kann, ist es unwahrscheinlich, dass die Bedrohung aufgedeckt wird.

Vermeidung von Datenverlusten, Diebstahl und Insider-Risiken

Angesichts der Tatsache, dass hybride Arbeitsumgebungen die Migration von Daten in die Cloud erfordern, ist der Datenkontext ein Kernprinzip der SSE innerhalb einer SASE-Architektur. Herkömmliche Abwehrsysteme sind nicht in der Lage, Datenflüsse zwischen verwalteten und nicht verwalteten Anwendungen zu erkennen und Cloud-Dienste sind für diesen Anwendungsfall ungeeignet. Außerdem ist es ohne das Wissen um die mit Cloud-Anwendungen verbundenen Risiken unmöglich, den Zugriff oder die Benutzeraktivitäten für die Cloud-Anwendungen einzuschränken, bei denen ein Risiko der Kompromittierung von Daten besteht.

Achten Sie auf die folgenden SASE-Funktionen zur Verwaltung dieses Anwendungsfalls

Die **Single-Pass-Architektur** bietet die Möglichkeit, den Datenschutz für Web, verwaltete Anwendungen, nicht verwaltete Anwendungen, IaaS Public Cloud-Benutzerdatenverkehr und benutzerdefinierte Anwendungen an einem einzigen Ort und in einem Durchgang anzuwenden. Dazu gehören kontextbezogene Richtlinien, Compliance-Vorlagen, exakte Datenübereinstimmung, Fingerabdrücke mit einem Ähnlichkeitsgrad und mehr als 3.000 Datenkennungen für mehr als 1.400 Dateitypen.

Datenschutzkontrollen verringern die Angriffsfläche für DLP, indem sie bösartige und riskante Websites blockieren, Anwendungen mit hohem Risiko blockieren, Uploads auf nicht verwaltete Anwendungen und Instanzen blockieren und Freigabeaktivitäten auf genehmigte Domänen beschränken.

Advanced Cloud DLP bietet die Möglichkeit, Cloud DLP auf bewegte Daten für verwaltete Geräte über Forward Proxy, bewegte Daten für nicht verwaltete Geräte über Reverse Proxy und über API auf ruhende Daten in verwalteten Anwendungen anzuwenden. Suchen Sie nach einem DLP-Tool, das ein umfassendes Verständnis von Inhalt, Kontext, Instanz, Kategorie und der Risikostufe der genutzten Cloud-Anwendungen bietet. Diese Variablen, die in herkömmlichen Web-Verteidigungssystemen nicht zu finden sind, können verwendet werden, um effektive Datenschutzrichtlinien direkt in der Cloud zu erstellen.

Erzielung von Kosteneinsparungen und betrieblicher Effizienz

Da hybrides Arbeiten zur Norm wird, drohen die Kosten und die Komplexität der Sicherheit außer Kontrolle zu geraten. Ein durchschnittliches Unternehmen verwaltet 76 verschiedene Sicherheitstools, und jedes Mal, wenn eine neue Bedrohung oder eine IT-Änderung auftaucht, muss ein neues Tool in Betracht gezogen werden. Zu den zusätzlichen Kosten für die Lösung kommt noch hinzu, dass mehr Mitarbeiter und Zeit für die Verwaltung der Sicherheit über verschiedene Tools, Richtlinien und Berichte benötigt werden. Inzwischen wollen Unternehmen von kostspieligen MPLS- und VPN-Technologien auf SD-WAN umsteigen, tun sich dabei aber schwer, weil es an integrierter Sicherheit mangelt.

[2] Quelle: https://www.infosecurity-magazine.com/news/organizations-76-security-tools/

05

Erzielung von Kosteneinsparungen und betrieblicher Effizienz

Achten Sie auf die folgenden SASE-Funktionen zur Verwaltung dieses Anwendungsfalls:

Die Technologiekonvergenz in der Cloud — insbesondere die Konvergenz von Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), ZTNA und Firewall-as-a-Service (FWaaS) — vereinfacht den Kauf- und Installationsprozess für Unternehmen dramatisch und optimiert gleichzeitig die laufende Verwaltung der Lösung durch einen gemeinsamen Agenten und eine gemeinsame Verwaltungskonsole. Gleichzeitig vereinfacht die durch diese Konvergenz ermöglichte einheitliche Richtlinienverwaltung den Verwaltungsprozess erheblich.

Durch die **SD-WAN-Integration** können Unternehmen enorme Kosteneinsparungen erzielen, indem sie langsame, ineffiziente und kostspielige MPLS-Zweigstellenverbindungen durch schnelle, erschwingliche Breitbandverbindungen ersetzen und gleichzeitig die Kosten für umfangreiche WAN-Konnektivität in der Zentrale senken. Die Integration von SWG-Technologien in das SD-WAN gewährleistet, dass Sie Ihren Web-, Cloud- und SaaS-Datenverkehr sichern und schützen können, während Sie auf das kostengünstigere Netzwerkmodell umsteigen.

Zero-Trust Network Access (ZTNA) macht den Einsatz von VPN-Clients für hybride Mitarbeiter überflüssig und senkt die Kosten für Bandbreite und VPN-Infrastruktur in der Zentrale weiter. Darüber hinaus vereinfacht ZTNA mit der Anwendungserkennung und der API für die Automatisierung die Abläufe rund um die Verwaltung privater Anwendungen, die Bereitstellung von Benutzerzugängen und die laufende Wartung.

Zusammenfassung

Die Anwendung von SASE-Funktionen bedeutet, dass die Sicherheit in Cloud-first, hybrid arbeitenden Unternehmen nicht auf Kosten der Leistung oder Produktivität gehen muss.

Von nun an wird ein erheblicher Teil der Belegschaft außerhalb des Büros arbeiten und erwarten, dass sie von jedem Gerät und jedem Ort aus arbeiten und auf Informationen zugreifen können. Man schätzt, dass langfristig 50% der amerikanischen Arbeitnehmer von zu Hause aus arbeiten werden, da die Arbeitgeber die Flexibilität und die Bequemlichkeit des hybriden Arbeitens schätzen. Während sich dieser Wandel vollzieht, müssen Unternehmen die richtige technologische Grundlage schaffen. Durch die Nutzung von SSE-Funktionen als Teil einer SASE-Strategie können Unternehmen ihre Zweigstellen mit einer Cloud-Architektur umgestalten, die Sicherheit nahtlos mit einem effizienten und kostengünstigen SD-WAN verbindet und sich perfekt in die Cloud-first-Architekturen moderner Unternehmen einfügt.

Über die Zweigstelle hinaus können SASE-Funktionen auch dazu beitragen, Mitarbeiter an entfernten Standorten und zu Hause zu schützen und zu befähigen, indem sie eine allgegenwärtige Cloud-Struktur schaffen, die einen schnellen, einfachen und sicheren Zugriff auf Web-, Cloud- und private Anwendungen von jedem Gerät oder Standort aus ermöglicht. So können Unternehmen ihr Geschäft flexibler gestalten, Sicherheitsrisiken besser abfedern und den Betrieb vereinfachen, um die Gesamtbetriebskosten zu senken.

[3] Quelle: https://www.inc.com/bill-murphy-jr/a-stanford-economist-who-studiesremote-work-says-half-of-allworkers-will-make-thisbig-change-in2022.html

Für mehr Informationen

Netskope, ein weltweit führendes Unternehmen im Bereich Cybersicherheit, definiert Cloud-, Daten- und Netzwerksicherheit neu, um Unternehmen bei der Anwendung von Zero Trust-Prinzipien zum Schutz von Daten zu unterstützen. Die Netskope Intelligent Security Service Edge (SSE)-Plattform ist schnell, einfach zu bedienen und sichert Menschen, Geräte und Daten überall.

Finden Sie heraus, warum Tausende von Unternehmen Netskope im Bereich Cloud-Sicherheit und SASE-bereite Netzwerke vertrauen - besuchen Sie netskope.com/de.