netskope

White Paper

Bisherige und neue Rolle von Firewalls und Proxy-Gateways

INHALT

EINFÜHRUNG

Wer sollte dieses Whitepaper lesen?

Network und Security VPs, Architects, Directors und Manager.

Wann sollte dieses Whitepaper gelesen werden?

Wenn zukünftige Inline-Kontrollpunkte für den Bedrohungs- und Datenschutz geplant werden.

Warum sollten Sie dieses Whitepaper lesen?

Die Rolle von Firewalls und Proxy-Gateways verändert sich, weil Inhalte und Kontexte für den adaptiven Zugriff, Zero-Trust-Prinzipien und Remote- und Hybrid-Arbeit mit SSE-Lösungen (Security Service Edge) erforderlich werden.

KURZFASSUNG

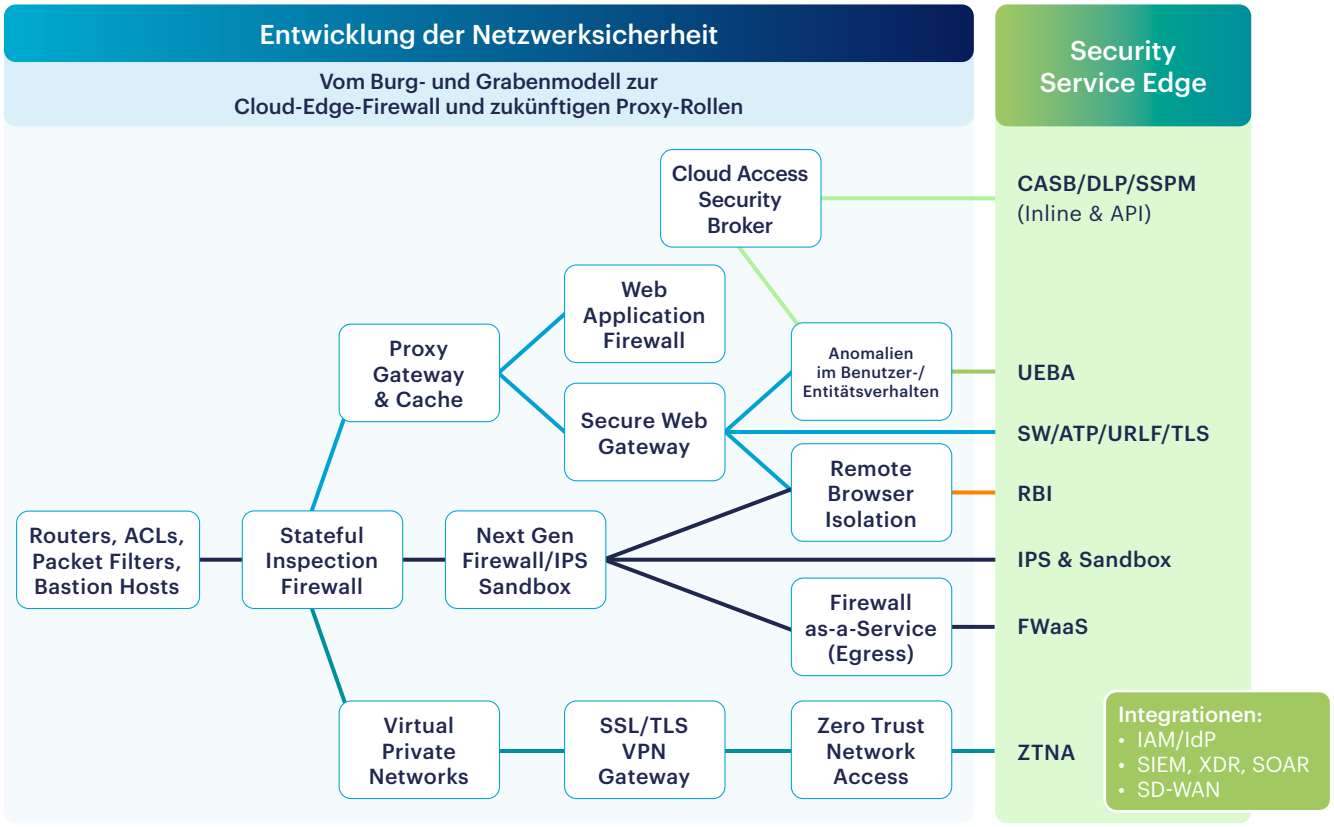
Der Mensch an sich mag keine Veränderung. Wer aber glaubt, dass mit den ewig selben Handlungen ein besseres Ergebnis erzielt werden kann, ist auf dem Holzweg. Im Hightech-Bereich, in dem sich innerhalb von fünf bis sieben Jahren zwangsläufig massive Änderungen ergeben, prallen daher Welten aufeinander: Auf der einen Seite steht die voranschreitende Technologie, auf der anderen der Mensch, der sich dagegenstemmt. Die ewige Debatte darüber, ob Firewalls oder Proxy-Gateways besser für die Inline-Netzwerksicherheit geeignet sind, hat mittlerweile zur Entwicklung einer neuen Generation geführt. Die Perspektive hat sich verschoben, weil man die bisherigen Unterschiede heute besser versteht und sich nach der Pandemie Rollenveränderungen ergeben haben.

> Was den Generationenwechsel bei Firewalls und Proxy-Gateways deutlich beschleunigt hat, sind künstliche Intelligenz und maschinelles Lernen, die Inhalte und Kontext für Echtzeitanalysen benötigen, was viele veraltete Inline-Sicherheitseinrichtungen nicht vorweisen können.

Infolge der zunehmenden Hybrid-Arbeit hat sich die Rolle des Remote-Zugriffs ebenfalls geändert. Gleichzeitig zwingen uns Zero-Trust-Prinzipien dazu, unsere lang gehegten Ansichten zum Thema Sicherheit zu überdenken. Vor Jahren wurde die Rolle von Gateway-Proxys so aufgeteilt, dass Secure Web Gateways (SWGs) den Egress-Datenverkehr und Web Application Firewalls (WAFs) den Ingress-Datenverkehr prüfen.

Eine ähnliche Entwicklung können wir heute bei Next-Generation Firewalls (NGFWs) für Egress-Datenverkehr feststellen, wobei eine in der Cloud gehostete Firewall-as-a-Service (FWaaS) für Hybrid- und Remote-Arbeit innerhalb von SSE-Plattformen (Security Service Edge) zum Einsatz kommt. Gleichzeitig sorgt eine Ingress-/Egress-Firewall für eingehenden/ausgehenden Datenverkehr weiterhin für den Schutz von Rechenzentren, der Infrastruktur und der Mitarbeiter vor Ort. Auch die ZTNA-Technologie (Zero Trust Network Access) ersetzt Virtual Private Networks (VPNs), die öffentlich zugängliche, ausnutzbare Services und bekannte Probleme mit lateralen Bewegungen aufweisen, durch eine besser abgesicherte Inside-Out-Direktverbindung zu den gewünschten Anwendungen und Ressourcen.

Noch gravierender sind die Auswirkungen auf den Inline-Bedrohungs- und Datenschutz, dessen jahrzehntealtes Modell mit Datei-Hash-Signaturen für schädliche Dateien oder vertrauliche Daten sich nicht skalieren lässt. Da hilft auch kein häufiger Austausch von Threat Intelligence bezüglich Indicators of Compromise (IOCs) in der Community. Die Zahl der unbekannten und Zero-Day-Bedrohungen nimmt weiter zu, und Umgebungen mit dynamischen, unstrukturierten Daten (wie Quellcode) verändern sich zu schnell, als dass eine DLP-Datenklassifizierung und -registrierung noch Wirkung zeigen könnte. Für diese immer häufiger werdenden Anwendungsfälle schließen KI und ML die Lücke in Echtzeit und bieten ein leistungsstarkes Benutzererlebnis. Wir haben einen Generationenwechsel vollzogen und unsere Entwicklung dorthin und die Bedeutung der neuen Rollen sind wichtige Wegweiser für die Netzwerk- und Sicherheitsarchitektur. Unsere Fähigkeit, Inhalte und Kontext in Echtzeit zu analysieren und Veränderungen anzunehmen, wird zukünftig für unseren Erfolg ausschlaggebend sein.



ANFÄNGE UND AUFTEILUNG

Router, ACLs, Paketfilter und Bastion-Hosts

Die meisten erinnern sich noch: Als das Internet Mitte der 1990er Jahre eingeführt wurde, mussten wir uns noch per Modem einwählen, und die Inhalte waren hauptsächlich Texte und statische Bilder. Das sieht heute völlig anders aus. Der ein- und ausgehende Zugriff auf Router wurde mit Zugriffskontrolllisten (ACLs) festgelegt und eine kleine Gruppe Leute tauschte sich auf greatcircle.com über frühe Designs von Firewalls aus, zu denen Dual-Bastion-Hosts und das Firewall Toolkit (FWTK). zählten. Das Internet richtete sich an die Außenwelt und einige behaupteten sogar, dass es der CB-Funk der 90er Jahre sei und der Trend bald wieder einschlafen würde. Von Anfang an wurde für ACLs, Router und Paketfilter zwischen Egress- und Ingress-Datenverkehr unterschieden und frühe Firewalldesigns waren sowohl proxy- als auch netzwerkbasiert.

Leistung von Stateful Inspection Firewalls überzeugt

Sobald sich das Internet als Ort herausstellte, an dem man online Informationen austauschen, Gleichgesinnte einfacher finden und neue Dinge lernen konnte, war sein Höhenflug nicht mehr aufzuhalten. Aufgrund seiner Beliebtheit sollen Politiker sogar behauptet haben, sie hätten das Internet entwickelt. Die Geschwindigkeit spielte eine wichtige Rolle und die Leistung von netzwerkbasierten Stateful Inspection Firewalls übertraf die von Designs mit Proxys und Dual-Bastion-Hosts um das 8- bis 10-Fache. Egress-Ports wurden für genehmigte Richtlinienanforderungen geöffnet und nach Abschluss der Sitzung wieder geschlossen. Oder man konnte sie für Ingress-Datenverkehr erneut nutzen, was eine Verbesserung gegenüber statischer ACLs war, die Ports offen ließen. Der Datenverkehr wurde für spezifische Quell- und Ziel-IP-Adressen/Ports und Protokolle definiert, die als 5-Tupel-Zugriffskontrollpunkte von Firewalls bekannt sind. Die Firewall wurde zur Hauptverteidigungslinie für Netzwerksicherheitsteams, mit der das Innen und Außen sowie DMZs für gehostete Services wie Web- und File-Sharing-Server definiert wurden.

Virtual Private Networks und Next-Generation Firewalls

Der Remote-Zugriff entwickelte sich schnell zum wichtigsten Anwendungsfall und Virtual Private Networks (VPNs) wurden ein wichtiger Bestandteil von netzwerkbasierten Firewalls, die schließlich zum SSL-Browser-basierten Remote-Zugriff führten. Dank VPNs erhielten Mitarbeiter Zugang zu bestimmten Netzwerkzonen und Umgebungen von Auftragnehmern, Partnern und Dritten, wo sie auf interne Anwendungen und Daten zugriffen, was eine gewisse laterale Bewegung mit sich brachte. Der Funktionsumfang von Websites nahm weiter zu, Webfilterung und URL-Kategorien wurden immer ausgereifter und die guten, schlechten und unschönen Seiten des Internets zeichneten sich ab. Beliebte Websites und Domains wurden Anwendungen immer ähnlicher und die Next-Generation Firewall (NGFW) kam und mit ihr die Zugriffskontrolle per App-ID, Content-ID und User-ID, die Vorteile gegenüber den 5-Tupel-Zugriffskontrollpunkten von Firewalls hatte.

Aufteilung von Proxys in Secure Web Gateways und Web Application Firewalls

Die Überprüfung durch einen Proxy war einigermaßen erfolgreich, wobei einige Befürworter dessen sichereres Design als Argument anführten, das die Rekonstruktion von Inhalten zur Durchführung von Sicherheitsscans vorsah. Bei NGFWs hingegen kommt ein Stream-basiertes Antivirus-Programm zur Anwendung. Die Überprüfung durch einen Proxy bot außerdem Protokoll-Compliance, Header-basierte Kontrollen und granulare Richtlinien sowie die Fähigkeit, Webobjekte zu filtern, zu zerlegen oder zu ersetzen. Leistungsprobleme bremsten Proxys jedoch aus, während die Stateful Inspection und NGFWs einfachere Richtlinienkontrollen und somit eine bessere Performance vorweisen konnten. Das Caching wurde bei Proxys ein wichtiger Anwendungsfall für Inhalte, auf die häufig zugegriffen wurde, weil sich dadurch der Weg zum Ursprungsserver verkürzte und das Benutzererlebnis verbesserte. Auf dem Höhepunkt konnten Benutzer deutlich über 30 % der Webinhalte durch Caching aufrufen. Dieser Prozentsatz wurde jedoch geringer, als Websites dynamischer und personalisierter wurden. Caching brachte ein neues Design für Proxyserver mit sich, das auf optimierten Betriebssystemen basierte. Es wurde nicht für Dateien und ausführbare Dateien konzipiert, sondern für Webobjekte, die eine schnellere Leistung ermöglichten.

> Die Egress- und Ingress-Rollen wurden für Proxyserver aufgeteilt, wobei Egress-Datenverkehr von Secure Web Gateways (SWGs) und Ingress-Datenverkehr durch Web Application Firewalls (WAFs) festgelegt wurde. Diese Aufteilung wird in mehreren Jahrzehnten und nach der Pandemie auch für die NGFWs Anwendung finden.

VOR DEM TLS-SIEGESZUG UND ANFÄNGE DER HARDWARESKALIERBARKEIT

HTTP-Überprüfung im Klartext

NGFWs skalierten die Leistung ebenso gut wie Proxy-Gateways (oder SWGs), da beide lediglich den HTTP-Datenverkehr im Klartext prüfen mussten und nur einen kleinen Anteil an verschlüsseltem SSL-Datenverkehr, der später in TLS umbenannt werden sollte. Bevor sich dieser blinde Fleck voll ausbilden konnte, war es für NGFWs, Intrusion-Protection-Systeme (IPS) und SWGs kein Problem, Inhalte in Klartext für die Webfilterung, Antivirus-Dateiprüfungen und die Zugriffskontrolle zu überprüfen. Ein Kernproblem kam auf, weil bösartige interne Benutzer ihre Identität mit release- und renew-Befehlen verbergen konnten. Sie verschafften sich dadurch neue IP-Adressleases, die ihre Identität verschleierten. HR-Teams konnten sich nicht sicher sein, dass sie den richtigen Mitarbeiter für Richtlinienverstöße zur Rechenschaft zogen. Noch schlimmer kam es, als lokale und regionale Behörden bei ihnen anklopften, um jemand Bestimmten zu suchen. Infolgedessen stieg das Interesse an SWGs, die eine integrierte sitzungsspezifische Authentifizierung und Autorisierung bieten. Denn die Benutzeridentität ist vor Gericht zulässig – unabhängig davon, wie oft IP-Adressleases geändert wurden. Ein weiteres Kernproblem war die Weiterentwicklung von Bedrohungen, die es erforderlich machte, Dateidownloads anzuhalten und deren Bandbreite zu limitieren, damit Anti-Malware-Lösungen mehr Zeit für die Erkennung hatten. Heute bezeichnen wir dies als Patient-Zero-Schutz.

Das Aufkommen von verschlüsseltem Datenverkehr

Die Datenverkehrverschlüsselung mit SSL und anschließend TLS wurde immer beliebter und erzeugte einen blinden Fleck für Netzwerksicherheitseinrichtungen.

Wenn die Überprüfung des SSL/TLS-Datenverkehrs aktiviert wurde, konnte dies zur Überlastung der NGFW-Appliance führen, die für die Überprüfung des HTTP-Datenverkehrs im Klartext genutzt wurde. Aus diesem Grund wurde sie häufig vermieden. Für die SSL/TLS-Überprüfung wurden dedizierte SWGs immer beliebter. Dies lag an ihrer Fähigkeit, ein beliebiges Webobjekt zu filtern, zu zerlegen oder zu ersetzen und die Bandbreite für Dateidownloads zu limitieren, damit Anti-Malware-Lösungen mehr Zeit für die Erkennung hatten. Die Filterung statischer URLs entwickelte sich durch maschinelles Lernen zudem zum dynamischen URL Rating weiter, bei dem hohe Confidence Level in Echtzeit ausgegeben wurden. Dazu kommen noch weitere geringfügige Vorteile wie das Caching von Inhalten und Stream-Splitting-Medien, die SWGs zum Egress-Punkt für Webdatenverkehr auf den Ports 80 und 443 machten, während NGFW alle Ports und Protokolle überwachten und VPN-Zugriff aus der Ferne bereitstellten. Zu jener Zeit nahm die SSL/TLS-Verschlüsselung des Datenverkehrs innerhalb weniger Jahre von 15 % auf 75 % zu, als unzureichend bereitgestellte SWGs mit der Bearbeitung von verschlüsseltem Datenverkehr ohnehin überlastet waren. Diese Entwicklung führte zu SSL-Beschleunigungskarten und Geräten für die SSL-Auslagerung, die in einem mehrschichtigen Abwehrlösungsstapel einen erweiterten Bedrohungsschutz bieten sollten.

Unterschiede zwischen Enterprise- und Mid-Market-Lösungen

Ein wesentlicher Unterschied bei Lösungen für die Inline-Netzwerksicherheit in großen und mittelständischen Unternehmen liegt darin, dass sie mit Skripten verwaltet werden konnten. Große Unternehmen investieren in Automatisierung und Skripte, um Sicherheitslösungen zu verwalten. Sie haben kein Interesse an einer Benutzeroberfläche (GUI) für die Webadministration. Bei Mid-Market-Lösungen ist das Gegenteil der Fall, denn dort verfügt die Benutzeroberfläche für die Webadministration über einen schrittweisen Richtlinienprozess, der als Anleitung dient. Bei den heutigen Lösungen liegen die Kernfunktionen auf einer API-Schicht, die von einer GUI-Schicht überlagert wird, welche die Funktionen repliziert. Alle Vorgänge in der GUI werden über die API-Schicht gesteuert und können daher auch geskriptet werden. Benutzergruppen, Communitys und Fachleute tauschen häufig lieber Skripte aus, als eine GUI-Demo mit schrittweisen Anleitungen anzusehen. Das ist etwas, was sie von Enterprise-Administratoren unterscheidet.

ROLLEN VOR COVID

Definierte Rollen für SWGs und NGFWs im Verlauf eines Jahrzehnts

Die Rollen von Secure Web Gateways und Next-Generation Firewalls blieben mehr als ein Jahrzehnt lang unverändert, weil beinahe jedes Unternehmen eine NGFW bereitstellte. Das lag jedoch daran, dass nur die ressourcenstarken Unternehmen sich SWGs leisten konnten. Der Wandel kam in Form des zunehmend mit SSL/TLS verschlüsselten Datenverkehrs, der für Appliances mit Firewall-Hardware nur schwer zu entschlüsseln war. NGFWs überprüften weiterhin Paket-Header, filterten Domains und analysierten sichtbare Inhalte. SWGs wurden hingegen speziell für die Überprüfung von verschlüsseltem Datenverkehr, für Inhaltsanalysen und eine strengere Benutzeridentifizierung konzipiert. Außerdem verfügten sie über die Fähigkeit, Webobjekte zu filtern, zu zerlegen oder zu ersetzen.

Für die Protokollierung von Ereignissen konzentrierten sich NGFWs hauptsächlich auf Warnungen, während SWGs detaillierte Webtranskationsereignisse mit hohen Volumen aufzeichneten, was Reporting-Lösungen häufig überforderte. Ein SWG, das zunächst für die Überprüfung von verschlüsseltem Datenverkehr bereitgestellt wurde, lief mit einer Kapazität von weniger als 10 % und erreichte gegen Ende seiner fünfjährigen Lebensdauer eine Kapazitätsausnutzung von bis zu 75 %. Wenn alles gut lief, konnte die Lösung dann ausgetauscht werden. Allerdings konnten nicht alle Bereitstellungen die starke Zunahme des verschlüsselten Datenverkehrs und die Cloud-Einführung von Office 365 handhaben, was bei Kunden Frust hervorrief und zu Budgetproblemen führte.

> Die Nachfrage nach Administratoren, die sich mit Web-Proxy-Gateways auskannten, war zu jener Zeit hoch, als Personal und Budgets im Bereich IT-Sicherheit knapp waren.

Infolgedessen wurden NGFWs vermehrt eingesetzt, um die Perimeter festzulegen. Einige wenige, die über die notwendigen Ressourcen verfügten, nutzten SWGs für die Entschlüsselung und Überprüfung des Webdatenverkehrs oder zur Analyse von Inhalten in Echtzeit.

Neue Sicherheitseinrichtungen gegen unbekannte Bedrohungen

Das bisher gültige Sicherheits-Mantra, dass Systeme regelmäßig gepatcht und Signaturen aktualisiert werden sollen, hat mit dem Aufkommen neuer URLs, neuer Inhalte und Zero-Day-Bedrohungen an Bedeutung verloren. Für diese nicht bewerteten, unbekannten Inhalte gab es zwei Optionen: Sie konnten entweder inline analysiert werden, während der Benutzer auf das Ergebnis wartete, oder sie wurden an Sicherheitseinrichtungen im Hintergrund gesendet, um sie zu analysieren und anschließend die Signaturen zu aktualisieren. SWGs hatten den Vorteil, dass sie verschlüsselten Datenverkehr überprüften und so Einblicke in Inhalte gewähren konnten, die eine Kategorisierung in Echtzeit ermöglichten (ohne Einsatz von menschlichen Bewertern im Hintergrund). Außerdem konnten sie Dateidownloads anhalten und deren Bandbreite limitieren, bis Dateien nach Feststellung ihrer Unbedenklichkeit zum Download freigegeben wurden. NGFWs und SWGs nutzten auch das Sandboxing von ausführbaren Dateien, um schädliche Bedrohungen zu erkennen und anschließend Signaturen zu aktualisieren.

> Damals galt die folgende Theorie: Je größer die Anzahl der Community-Mitglieder, desto größer das Risiko für neue Bedrohungen durch Patient-Zero-Infektionen. Deshalb sollten neue Signaturen schneller entwickelt und über einen Anbieter von Sicherheitslösungen geteilt werden.

Als Ergänzung von SWGs stellte die Remote Browser Isolation (RBI) eine pixelgenerierte Ansicht von Websites und unbekannten und möglicherweise schädlichen Inhalten bereit, um Benutzer und ihre Geräte vor Angriffen zu schützen.

Threat-Protection-Strategie für Endpunkte und Gateways

Bis zum Jahr 2017 und der Zunahme von dateilosen Bedrohungen war der Endpunkt der beste Ort, um ausführbare Dateien zu analysieren, weil er Zugriff auf Dateisysteme, Laufzeiten und Verzeichnisse ermöglichte. Dateilose Angriffe, die im Arbeitsspeicher ausgeführt werden, umgehen das Dateisystem mit Runtime-Skripten und stellen so eine neue Herausforderung dar. Darüber hinaus gab es inhaltsbasierte Phishing-Angriffe, bei denen es keine ausführbaren Dateien zu analysieren gab, sowie andere Betrüge und Tricks, um Benutzer zu täuschen. SWGs wurden aufgrund ihrer Fähigkeit, Inhalte zwischen Ursprungsservern und Benutzern als MITM-Prüfpunkt (Man-in-the-Middle) analysieren zu können, zum wichtigen Instrument für den Bedrohungsschutz auf Endpunkten.

> Eine skalierbare und leistungsfähige Überprüfung von verschlüsseltem Datenverkehr wurde noch wichtiger, um Benutzer und Ressourcen vor dateibasierte, dateilosen und Phishing-Angriffen zu schützen.

Breite Verwendung von VPNs für den Remote-Zugriff

Für die ersten Virtual Private Networks (VPNs) wurde ein verwalteter Client benötigt, was zu jener Zeit wenig Begeisterung hervorrief, weil Desktopmanagementteams die verschiedenen Konflikte zwischen mehreren Endpunkt-Agenten lösen mussten. Die Neuentwicklung von SSL/TLS-basierten VPNs, die Webbrowser nutzen, beschleunigte die VPN-Einführung als bevorzugte Lösung für den Remote-Zugriff. Zu diesem Zeitpunkt arbeitete weniger als 20 % der Unternehmensbelegschaft an einem Remote-Standort, was die Einführung von VPN-Technologien erforderlich machte. Die meisten Mitarbeiter und Auftragnehmer betraten den Hauptsitz oder die Zweigstelle eines Unternehmens, um ihre Arbeit zu erledigen. Dies taten sie auf einem verwalteten Gerät und in einem vom Unternehmen verwalteten Netzwerk hinter einer NGFW – und in vielen Fällen auch einem SWG.

> Diese Ausrichtung auf den Unternehmensstandort wird zu Beginn der Pandemie ein großes Problem.

Anfänge der SaaS/IaaS-Einführung

NGFWs und SWGs boten sorgfältig definierte Rollen, Aktualisierungszyklen und Konsistenz, doch für SaaS-Anwendungen und IaaS-Cloud-Services ergaben sich völlig neue Möglichkeiten.

> Die meisten Administratoren für NGFWs und SWGs dachten, dass die neuen Lösungen nicht in ihren Zuständigkeitsbereich fielen, und beachteten SaaS und IaaS vor der Pandemie kaum.

CASB-Lösungen (Cloud Access Security Broker) konzentrierten sich auf verwaltete SaaS und IaaS. Dafür nutzten sie die API-Überprüfung und Webhooks für neue Ereignisse oder zeitbasierte Analysen. Das Hauptaugenmerk lag dabei auf dem Datenschutz und der DLP, da die meisten beliebten SaaS-Anwendungen Daten enthielten, die Compliance-Richtlinien unterlagen. Zur gleichen Zeit führten Benutzer auch private SaaS-Anwendungen für E-Mail, soziale Medien, Sofortnachrichten, Chats, private Kommunikation und Cloud-Dateispeicher ein. Während der Pandemie werden sich die Unternehmens- und privaten SaaS-Umgebungen bald überschneiden.

In vielen Regionen der Welt wurde für Betriebssysteme und Webbrowser HTTPS zur Verschlüsselung von Webdatenverkehr verwendet (zu über 90 %), was das Pandemiechaos perfekt machte. Für Inline-Sicherheitseinrichtungen, die keinen HTTPS-Datenverkehr entschlüsseln oder prüfen, wurde der blinde Fleck immer größer. Man musste sich verstärkt auf die Community verlassen, um Threat Intelligence zu erhalten und unbekannte Bedrohungen abzuwehren; und mit zunehmender Einführung von SaaS/IaaS-Lösungen fehlten Einblicke in Datenbewegungen. Falls Sie verschlüsselten Datenverkehr und Ressourcen verwaltet haben, werden Sie Folgendes festgestellt haben: Nämlich, dass sich die für die Handhabung der zunehmenden HTTPS-Nutzung und des Web- und SaaS/IaaS-Datenverkehrs erforderliche Kapazität alle paar Jahre nahezu verdoppelt hat.

Das Ende des Burg- und Grabenmodells

Anfang 2020 markierte das Ende des Burg-und-Grabenmodells für Sicherheit. Sicherheits- und Netzwerkadministratoren, die es gewohnt waren, dass Benutzer sich in Büros innerhalb ihres Netzwerks aufhielten und mit verwalteten Geräten, Anwendungen und Daten von ihren Rechenzentren arbeiteten, sollten bald auf die Probe gestellt werden. Auf einem T-Shirt, das sich unter IT-Administratoren jener Zeit an Beliebtheit erfreute, war der schnippische Spruch „Ich habe deine E-Mail zuerst gelesen“ zu sehen. Netzwerk-TAPs (Test Access Points) konnten beliebigen Datenverkehr in Paketerfassungen aufzeichnen, um sie später wiederzugeben und zu analysieren. Dafür wurde deren Sichtbarkeit vorausgesetzt.

ROLLEN NACH COVID

Aufkommen der Hybrid- und Remote-Arbeit fördert den digitalen Wandel

Wer hätte es geahnt! Im März 2020 werden Angestellte aufgrund der Pandemie vom Arbeiten im Büro abgehalten, was in der Geschichte der IT zum Lackmustest für ihre Resilienz wurde.

> Die Pandemie schlägt voll zu: Die VPN-Kapazität ist eingeschränkt, Sicherheitseinrichtungen sind rechenzentrumsbasiert, es gibt blinde Flecken bei der Überprüfung von verschlüsseltem Datenverkehr und die Nutzung von SaaS/IaaS-Lösungen nimmt zu.

Während der Pandemie wurde die Cloud-Nutzung für Benutzer, Anwendungen und Daten beschleunigt und so der Weg für den digitalen Wandel und geschäftliche Agilität bereitet. Die Transformation, die andernfalls mehrere Jahre gedauert hätte, ging so schnell vonstatten, dass die Rollen der veralteten Sicherheitseinrichtungen neu definiert werden mussten. Unternehmen standen vor der Wahl, den digitalen Wandel entweder selbst zu vollziehen oder den Anschluss zu verlieren. Je nachdem, wie die Entscheidung ausfiel, mussten sie dringend benötigte IT-Fachleute und Kenntnisse erwerben, oder darauf verzichten.

VPNs beim Backhauling des Datenverkehrs überfordert

Praktisch sofort wurden VPNs einem Härtetest unterzogen, als sie Remote-Mitarbeitern Zugriff auf Unternehmensressourcen gewähren sollten. Es kam in vielen Fällen zu Überlastungen, bis mehr Kapazitäten bereitgestellt wurden. Die höheren Kosten und zunehmende Komplexität öffneten weiteren Sicherheitsrisiken Tür und Tor. VPNs nutzen einen öffentlichen Serviceport, der für Exploits, Kompromittierungen des Zugriffs durch schwache Passwörter und offene laterale Bewegungen anfällig ist, weil der Zugang die Angriffsfläche zusätzlich erweitert. Beim Backhauling von VPN-Datenverkehr zu den Rechenzentren über veraltete Sicherheitseinrichtungen litt das Benutzererlebnis. Demzufolge mieden Benutzer diesen Weg oder ihnen wurde direkter Zugriff auf SaaS/IaaS-Lösungen gewährt, um die Produktivität zu steigern. In beiden Fällen ging die bisher gewohnte Sichtbarkeit verloren.

Beschleunigte SaaS-Einführung durch Cloud-First-Strategie

Jahr für Jahr wurden über 18 % mehr verwaltete SaaS-Anwendungen zur Verbesserung der Produktivität in Büros, für die Pflege von Kundenbeziehungen, das Marketing und die Personalabteilung eingeführt, die als wichtige Wachstumsbereiche ausgemacht wurden. Gleichzeitig erwiesen sich privat genutzte SaaS-Anwendungen schnell als gute Ausweichlösung für Remote-Mitarbeiter, um Dateien auszutauschen, Daten zu verschieben und ohne große Umstände Aufgaben zu erledigen.

> Verwaltete SaaS-Lösungen konnten zwar die API-Überprüfung nutzen, aber nicht verwaltete SaaS-Lösungen und private Instanzen von beliebten SaaS-Anwendungen erzeugten nach der Pandemie einen blinden Fleck.

Netzwerk- und Sicherheitsteams verfügten über mehr als zehn Jahre Erfahrung in der Verwaltung von NGFWs und SWGs, aber die CASB-Inline-Prüfung des Datenverkehrs für unternehmenseigene und private SaaS- und IaaS-Anwendungen war für sie Neuland. Unternehmen, die eine Cloud-First-Strategie einführten, verloren den Überblick. Sie konnten nicht erkennen, ob Daten unerkannt oder ungenehmigt verschoben oder exfiltriert wurden.

Aufteilung von NGFWs in FWaaS für Remote Egress und ZTNA für Remote Access

Für Hybrid- und Remote-Mitarbeiter ist das Backhauling von geschäftlichen Transaktionen über rechenzentrumsbasierte Sicherheitseinrichtungen wenig sinnvoll und dem Benutzererlebnis keineswegs zuträglich. Die Rolle, die eine NGFW für diese Benutzer spielt, ändert sich angesichts der Tatsache, dass ausgehender Datenverkehr von einer Firewall-as-a-Service (FWaaS) geschützt wird. Diese ist Bestandteil einer SSE-Sicherheitsplattform mit einem kombinierten Proxy für die Überprüfung des Web- und SaaS/IaaS-Datenverkehrs, die außerdem SWG- und CASB-Inline-Funktionen bietet. Der Remote-Zugriff über VPNs entwickelte sich zum Zero Trust Network Access (ZTNA) weiter, der auf Zero-Trust-Prinzipien basiert und eine besser abgesicherte Inside-Out-Verbindung nutzt. Die NGFW erfüllt ihre bisherige Rolle weiterhin für Rechenzentren und den dort eingehenden und ausgehenden Datenverkehr, bis das Unternehmen zu 100 % auf die Cloud umstellt und seine Rechenzentren ausmustert. Wie SWG-Appliances auch wird NGFW-Appliance allmählich verschwinden, da sich Anwendungsfälle ändern und die Skalierungs- und Leistungsfähigkeit der Cloud für Benutzer, Geräte und Standorte attraktiver ist.

Rasante Konsolidierung im Security Service Edge

Vor der Pandemie sagten einige wenige Analysten voraus, dass Sicherheitseinrichtungen zu Cloud-Edge-Plattformen konsolidiert werden würden. Nach der Pandemie stellten sie sehr schnell fest, wie recht sie damit hatten. Die Technologie Secure Access Service Edge (SASE) wurde mit der Kombination aus Security Service Edge (SSE) und SD-WAN weiter optimiert. Diese Entwicklung überraschte Anbieter von NGFW- und SWG-Lösungen, und ein CEO eines SWG-Anbieters wunderte sich, wie ein CASB-Anbieter Marktführer für SSE-Lösungen werden konnte. Der unternehmensinterne und private SaaS/IaaS-Datenverkehr überstieg den Webdatenverkehr nun volumenmäßig. Deshalb wurde sowohl eine TLS-Entschlüsselung als auch eine Decodierung von SaaS/IaaS-Anwendung en erforderlich, damit transparente Einblicke in Inhalte gewonnen werden konnten. CASB-Lösungen wurden zu jener Zeit hauptsächlich als Instrument für API-Überprüfungen von verwalteten SaaS-Lösungen betrachtet, die für DLP- und Compliance-Zwecke durchgeführt wurden.

Dann kam eine neue Lösung auf, die eine CASB-Inline-Prüfung des Datenverkehrs von dienstlichen und privaten SaaS-, IaaS- und Weblösungen bietet und sich auf dem Markt für SSE-Lösungen zum Platzhirsch entwickelt. Diese nach der Pandemie gewonnenen neuen transparenten Einblicke bestätigten schnell, dass über die Hälfte der Bedrohungen aus der Cloud, und nicht aus dem Internet stammen. Datenexfiltration und -diebstähle sind im letzten Arbeitsmonat ausscheidender Mitarbeiter auf 300 % gestiegen.

> Bei den typischen Anwendungsfällen für NGFWs und SWGs wurde die zunehmende Einführung von SaaS- und IaaS-Lösungen für dienstliche und private Zwecke außer Acht gelassen. Und es wurde nicht bemerkt, dass diese Entwicklung durch die Pandemie beschleunigt wurde.

Das Blockieren dieser Domains bringt nur Frust für Benutzer und könnte auch die Ausweichlösungen behindern, wenn es bei den wichtigsten Anwendungen zu Ausfällen kommt. Mit SSE, Cloud-First-Strategien und dem digitalen Wandel wurden die Anforderungen der Benutzer erstmals ernst genommen und Anwendungen und Datenbewegungen in den Fokus gerückt. Die Rollen von NGFWs und SWGs veränderten sich und sollten noch vor eine weitere Herausforderung gestellt werden.

WANDEL IN RICHTUNG ZERO TRUST

Zero-Trust-Prinzipien und unzureichendes Marketing

Mit Zero-Trust-Prinzipien sollen der implizite Zugriff entfernt, der Zugriff mit den geringsten Berechtigungen verfeinert und eine kontinuierliche Überwachung ermöglicht werden. Diese grundlegenden Konzepte werden beim Marketing von Zero-Trust-Lösungen jedoch kaum berücksichtigt. Die meisten Marketingbotschaften heben den sicheren Zugriff beim Zero-Trust-Modell hervor, vergessen darüber aber, dass Daten mit allen Zero-Trust-Komponenten (Benutzer, Anwendungen, Geräte und Netzwerke) Berührpunkte haben.

> Zero-Trust-Prinzipien funktionieren nicht, wenn blinde Flecken durch veraltete Sicherheitseinrichtungen vorliegen.

Das Konzept des Zugriffs mit den geringsten Berechtigungen funktioniert je nach Geschäftstransaktion und deren Inhalt und Kontext nur, wenn Sie transparente Einblicke haben. Und wenn Sie eine kontinuierliche Überwachung wünschen, um diese Zugriffsart zu verfeinern, müssen Sie alle Benutzer, Daten, Anwendungen, Geräte und Netzwerke überblicken können. Sie benötigen SSE-Lösungen, die CASB- und SWG-Funktionen kombinieren und zu einem Inline-Proxy mit FWaaS und ZTNA konsolidieren, um die bisherigen Rollen von NGFWs und VPNs neu definieren und das Zero-Trust-Modell unterstützen zu können. Als Cloud-Security-Edge-Plattform verfügt SSE über die nötige Skalierfähigkeit und Leistung für alle Benutzer, Geräte oder Standorte, um ein großartiges Benutzererlebnis bereitzustellen. Die Lösung bietet transparente Einblicke in Inhalte, ganz ohne Kompromisse hinsichtlich Leistung und Sicherheit.

Ransomware bei Cyberkriminalität auf dem Vormarsch

> Mit Ransomware wird kompromittierter Remote-Zugriff zu Geld gemacht, deshalb müssen Zero-Trust-Prinzipien dringend umgesetzt werden.

Unternehmen, die sich weiterhin auf veraltete Sicherheitseinrichtungen wie VPNs, Lösungen zur Unterstützung des Remote-Zugriffs und herkömmliche Firewalls verließen und unberechtigte Zugriffe auf Konten, Benutzer und Geräte nicht erkannten, wurden zur Zielscheibe. Wenn Ihre erste Verteidigungslinie darauf ausgelegt ist, Ransomware zu erkennen, die Daten verschlüsselt und die Verschlüsselungsschlüssel verwaltet, dann wurden die Daten in einer früheren Kill-Chain-Phase bereits exfiltriert und Sie werden bald von den Erpressern hören. Kompromittierte Remote-Zugriffe und Phishing sind die führenden Eintrittspunkte für Ransomware und fördern eine branchenübergreifende Schattenwirtschaft, bei der Zugriffsrechte auf gewünschte Ziele verkauft werden.

Behördliche Vorschriften verlangten nicht nur eine Multi-Faktor- oder starke Authentifizierung, sondern empfahlen schließlich auch, VPN-Lösungen zu ersetzen, die für Kompromittierungen und Zero-Day-Bedrohungen anfällig waren. ZTNA mit seiner Inside-Out-Verbindung zu einer bestimmten Anwendung oder Ressource ist sicherer und nutzt dedizierte Egress-IP-Adressen für verwaltete SaaS-Anwendungen auf SSE-Plattformen. Zur Abwehr von Phishing-Angriffen ist die Echtzeit-Inhaltsanalyse von Web-, E-Mail-, SaaS- und IaaS-Datenverkehr erforderlich, da gefälschte Anmeldemasken häufig in beliebten SaaS- und IaaS-Cloud-Services gehostet werden. Insgesamt betrachtet, und abgesehen von der über ausführbare Dateien eingeschleusten Malware, wird Ransomware weiterhin die Triebfeder für den Austausch von veralteten Sicherheitseinrichtungen bleiben.

Unerkannte und nicht genehmigte Datenexfiltration, Diebstahl und Insider

Zu Beginn der Pandemie nahmen Mitarbeiter verwaltete Geräte mit nach Hause, um auf diverse Inhalte zuzugreifen, die nichts mit der Arbeit zu tun hatten. Viele Laptops wurden auch für schulische oder private Zwecke und den Zugriff auf soziale Medien genutzt. Der Zugriff auf nicht jugendfreie Inhalte stieg zunächst auf über 600 %, ging dann aber zurück. Das war nicht überraschend. Als in Linienflugzeugen zum ersten Mal WLAN-Zugriff angeboten wurde, passierte dasselbe. Die Fluglinien schalteten die Funktion wieder ab, bis es die Webfilterung gab. Auch im Berufsleben gab es Veränderungen, weil einige Mitarbeiter sich an die Remote-Arbeit gewöhnt hatten und diese beibehalten wollten. Einige clevere IT-Unternehmen veröffentlichten sogar Werbung, die unbegrenzte Remote-Arbeit anpries, um für sie nützliche Mitarbeiter von anderen Unternehmen wegzulocken, die sie wieder in die Büros zitieren wollten.

Mitarbeiter nutzen ihre Laptops im Büro, wo ihnen andere über die Schulter sehen können, völlig anders als am Remote-Standort. Da sie auf mehr Inhalte zugreifen können, die nichts mit ihrer Arbeit zu tun haben, ist die Verlockung groß – aber auch das Risiko.

> Mitarbeiter, Auftragnehmer und Partner glauben auch, dass sie dazu berechtigt sind, auf Daten zuzugreifen, die für zukünftige berufliche Rollen nützlich sein könnten.

Diese Annahme wurde bestätigt, als die Datenexfiltration und -diebstähle im letzten Arbeitsmonat ausscheidender Mitarbeiter auf 300 % stiegen. Dabei wurden 74 % dieser Daten auf privaten Cloud-Speichern abgelegt. Unerkannte und nicht genehmigte Datenexfiltration, Diebstahl und Risiken durch Insider nahmen mit der Hybrid/Remote-Arbeit zu, weil veraltete Sicherheitseinrichtungen keine Kontrolle über die unternehmensinterne oder private Nutzung von SaaS- und IaaS-Lösungen hatten. Dass weniger als 3 % der SaaS-Anwendungen von der IT verwaltet und die anderen 97 % im Zuge des digitalen Wandels von den Geschäftseinheiten und Benutzern eingeführt wurden, überraschte Anbieter von NGFW- und SWG-Lösungen.

Inhalte und Kontext sind die Zukunft der adaptiven Zugriffskontrolle

Die Inline-Überprüfung von SaaS- und IaaS-Inhalten und -Kontext in Echtzeit wird zukünftiger Bestandteil von SSE-Lösungen für die Zugriffskontrolle sein. Firewalls perfektionierten die Überprüfung des Netzwerkdatenverkehrs und SWGs taten dasselbe für den Webdatenverkehr. Moderne SSE-Lösungen kombinieren nun beide Kontrollen mit der CASB-Inline-Prüfung von Inhalten und Kontext. Die adaptive Zugriffskontrolle, die sich nach dem Anwendungsrisiko, dem Risikoverhalten, dem Gerätestatus, den Aktivitäten, der Vertraulichkeit von Daten oder anderen Variablen richtet, wird zur Überprüfung von Inhalten und Kontext auf jede geschäftliche Transaktion angewendet. Wenn ein Benutzer 100 Dateien mit vertraulichen Unternehmensdaten löschen möchte, kann die adaptive Zugriffskontrolle eine Step-up-Authentifizierung oder eine Begründung vom Benutzer verlangen.

> Wir befinden uns in einer neuen Grauzone, in der die Klassifizierungen „bekannt gut“ und „bekannt schlecht“ verschwimmen. Deshalb braucht es eine adaptive Zugriffskontrolle und Anleitung, um Benutzer und Daten zu schützen.

Wenn ein anderer Benutzer auf eine nicht verwaltete, riskante Cloud-Speicher-Anwendung zugreifen möchte, um Dateien zu verschieben, kann die adaptive Zugriffskontrolle ein Warnung ausgeben und ihm vom Unternehmen genehmigte Cloud-Speicher-Optionen zur Verfügung stellen. Das Konzept des Echtzeit-Coaching ähnelt der Navigation nach Satellit (oder GPS) beim Autofahren und ist auch auf Benutzer anwendbar.

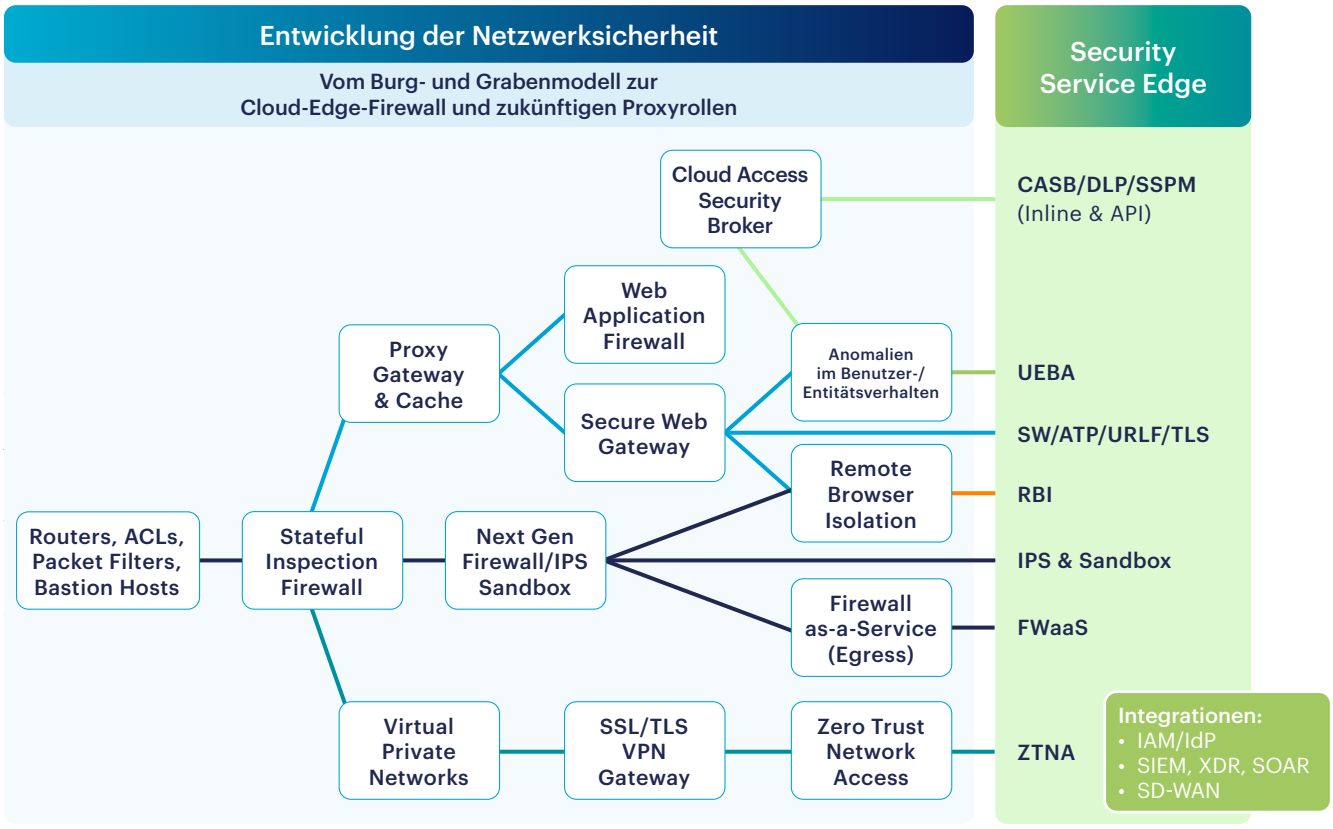
Rolle von KI und ML für den Bedrohungs- und Datenschutz

Künstliche Intelligenz (KI) und maschinelles Lernen (ML) werden schon seit Jahren im Hintergrund eingesetzt, beispielsweise für Bedrohungsabwehr-Engines, zur Datenklassifizierung, für dynamisches URL Rating und zur Planung von IT-Abläufen. Heute werden KI- und Ml-basierte Sicherheitseinrichtungen inline eingesetzt, um unbekannte Zero-Day-Bedrohungen und vertrauliche Daten in Dokumenten und Bildern in Echtzeit zu erkennen. Der KI-Boom an sich bringt positive Impulse für die schnelle Entwicklung von neuem Code, für die Erstellung von Inhalten und für das Lernen. Er hat aber auch schlechte Seiten, weil vertrauliche Daten eher offengelegt werden können. ChatGPT wurde schnell zur KI-Anwendung mit den meisten Zugriffen, der vor allem Quellcode bereitgestellt wurde. Veraltete Sicherheitseinrichtungen waren nicht in der Lage, unternehmenseigene KI-Instanzen zuzulassen oder öffentliche und private Instanzen von Benutzern zu kontrollieren. Sie konnten auch keine Inhalte wie Quellcode identifizieren, mit denen KI-Anwendungen gefüttert wurden. KI/ML-basierte-Inline-Sicherheitseinrichtungen erkennen mittlerweile schädliche ausführbare Dateien und Phishing-Angriffe und klassifizieren Dutzende Dokumente und Bilder sowie Quellcode.

> Inline-KI/ML-Sicherheitseinrichtungen, die Echtzeit-Schutz (T+0) bieten, funktionieren nur mit transparenten Einblicken in Inhalte. Und diese zeichnen eine moderne SSE-Plattform aus.

Moderne Rollen für NGFW, SWG, CASB, VPN und ZTNA für Zero Trust

Dem Web-Gateway wurden schnell verschiedene Rollen für ausgehenden SWG- und eingehenden WAF-Webdatenverkehr zugewiesen. Während die NGFW weiterhin sowohl für ausgehenden als eingehenden Netzwerkdatenverkehr zuständig ist, fließt nach der Pandemie ausgehender Datenverkehr für Hybrid- und Remote-Mitarbeiter in FWaaS. VPN-Funktionen werden durch ZTNA ersetzt, der Bestandteil von SSE-Plattformen ist. CASB wurde schon früh als Instrument für API-Überprüfungen von verwalteten SaaS- und IaaS-Lösungen betrachtet, das auch DLP für ruhende Daten bot. Die häufig übersehene Fähigkeit von CASB, Tausende von verwalteten und unverwalteten Anwendungen und Cloud-Services (einschließlich unternehmenseigener und privater Instanzen Hunderter Anwendungen) schnell und inline zu analysieren, wurde schnell als äußerst nützlich betrachtet. Das Interesse an Zero-Trust-Prinzipien nimmt zu, sie setzen jedoch transparente Einblicke in Inhalte und Kontext voraus, damit Zugriff mit den geringsten Berechtigungen gewährt und jede geschäftliche Transaktion kontinuierlich überwacht werden kann. Und genau diese Inhalte und Kontexte werden für die Weiterentwicklung von KI/ML-basierten Echtzeit-Sicherheitseinrichtungen auf SEE-Plattformen sorgen.



ZUSAMMENFASSUNG

Investitionen in Sicherheitseinrichtungen für Infrastrukturen, die nicht mehr existieren oder bald hinfällig werden, sind fehlgeleitet und kostspielig, da Unternehmen verstärkt auf Hybrid-Arbeit setzen und den digitalen Wandel vollziehen. Die Verlängerung von NGFW-, SWG- und VPN-Lösungen sollte sorgfältig und unter dem Gesichtspunkt analysiert werden, dass vermehrt SaaS- und IaaS-Inline-Überprüfungen stattfinden, Inhalte und Kontext für KI/ML-Sicherheitseinrichtungen sichtbar sein müssen und Benutzern adaptiver Zugriff mit Echtzeit-Coaching bereitgestellt werden muss.

Wir alle sollten wissen, wie wir an diesem Punkt angelangt sind und was die Veränderungen für ausgehenden und eingehenden Netzwerk-, Web- und SaaS/IaaS-Datenverkehr herbeigeführt hat.

Pioniere und frühzeitige Anwender passen sich schnell an, sobald sie Anzeichen für Veränderungen erkennen, und fördern Innovationen, erstellen Roadmaps und bewerten Vorhersagen von Analysten. Bei den meisten wird über Erfolg und Misserfolg entscheiden, wie schnell sie nach der Pandemie Änderungen erkennen, sich anpassen, IT-Mitarbeiter anwerben oder halten und sich auf die nächste Phase vorbereiten können. Denn der Widerstand des Menschen gegen die unbeirrt fortschreitende Technologieentwicklung ist in allen Lebensbereichen spürbar.

GRÜNDE FÜR NETSKOPE

Netskope Intelligent SSE bietet eine einzigartige Überprüfung des Web-, SaaS- und IaaS-Datenverkehrs für Tausende Anwendungen und Cloud-Services, sodass Inhalte und Kontexte besser nachvollzogen werden können. Die Kernarchitektur umfasst ZTNA für den Zugriff auf private Anwendungen und die vollständige Integration von SWG- und CASB-Lösungen für eine Single-Pass-Überprüfung des Inline-Datenverkehrs von Benutzern oder Systemen. Dank dieser umfassenden Einblicke kann die Zero Trust Engine von Netskope adaptive Zugriffskontrolle, Echtzeit-Coaching und einen besseren Überblick über unternehmenseigene und private Instanzen für Hunderte Anwendungen liefern und so die Erkennung von unbekannten Datenbewegungen ermöglichen. Es wird Zugriff mit den geringsten Berechtigungen gewährt, wobei Benutzer die Möglichkeit erhalten, Begründungen für Aktionen anzugeben, damit sie mit geschäftlichen Transaktionen fortfahren können. Richtlinien lassen sich durch die kontinuierliche Überwachung gemäß Zero-Trust-Prinzipien weiter verfeinern.

Für weitere Informationen lesen Sie bitte unser E-Book **Neue Erkenntnisse für Bedrohungs- und Datenschutz – Was Legacy-Anbieter verbergen möchten**, oder sehen sich die Infografik und unser On-Demand-Webinar an.

Netskope, ein weltweit führender Anbieter von SASE-Lösungen, definiert Cloud-, Daten- und Netzwerksicherheit neu, um Unternehmen durch Anwendung von Zero-Trust-Prinzipien beim Schutz ihrer Daten zu helfen. Die schnelle und benutzerfreundliche Netskope-Plattform bietet optimierten Zugriff und Echtzeit-Sicherheit für Benutzer, Geräte und Daten, wo immer sie sich befinden. Netskope hilft Kunden, Risiken zu reduzieren, die Leistung zu steigern und einen einzigartigen Einblick in alle Cloud-, Web- und privaten Anwendungsaktivitäten zu erhalten. Tausende Kunden, darunter mehr als 25 der Fortune 100-Unternehmen, vertrauen Netskope und seinem leistungsstarken NewEdge-Netzwerk im Umgang mit neuen Bedrohungen und Risiken, dem Technologiewandel, betrieblichen und netzwerktechnischen Änderungen und neuen gesetzlichen Vorschriften.

Unter dem folgenden Link erfahren Sie, wie Netskope Kunden hilft, sich bei der Umstellung auf SASE für alle Eventualitäten zu wappnen: netskope.com.

1/24 RA-709-1