KURZVORSTELLUNG

Skyhigh Security
Security Service Edge (SSE)

Der SSE-Sicherheitsdienst für die Cloud-Transformation

Unsere SSE-Lösungen bilden die Sicherheitsstruktur zwischen den Mitarbeitern und ihren Ressourcen. Sie erlaubt den schnellen Direktzugriff auf das Internet, weil die Daten nicht mehr aus Sicherheitsgründen über das Rechenzentrum laufen müssen. Die Analysen für Daten- und Bedrohungsschutz erfolgen an jedem Kontrollpunkt in einem Durchlauf, um Sicherheitskosten zu senken und die Verwaltung zu erleichtern.

Ist Ihre digitale Transformation schnell und sicher genug?

Wir stecken mitten im digitalen Wandel. Dieser bietet enorme Vorteile, stellt uns aber auch vor große Herausforderungen.

- Immer mehr Menschen arbeiten standortunabhängig. Für Benutzer in Niederlassungen, die über herkömmliche VPNs und MPLS angebunden sind, bedeutet dies jedoch, dass die Daten beim Zugriff auf kritische Internet- und Cloud-Ressourcen den Umweg über die alte Netzwerkinfrastruktur nehmen müssen. Diese verstopft dadurch zunehmend und wird immer langsamer.
- Durch die Freigabe des Zugriffs auf Unternehmensressourcen über nicht verwaltete mobile Geräte werden Daten auf neuen Wegen übertragen, die von der Peripheriesicherheit nicht kontrolliert werden.
- Herkömmliche Sicherheits-Tools können mit der Zunahme der hochentwickelten Cloud- und Web-basierten Bedrohungen um 630 % nicht mehr Schritt halten.[1]

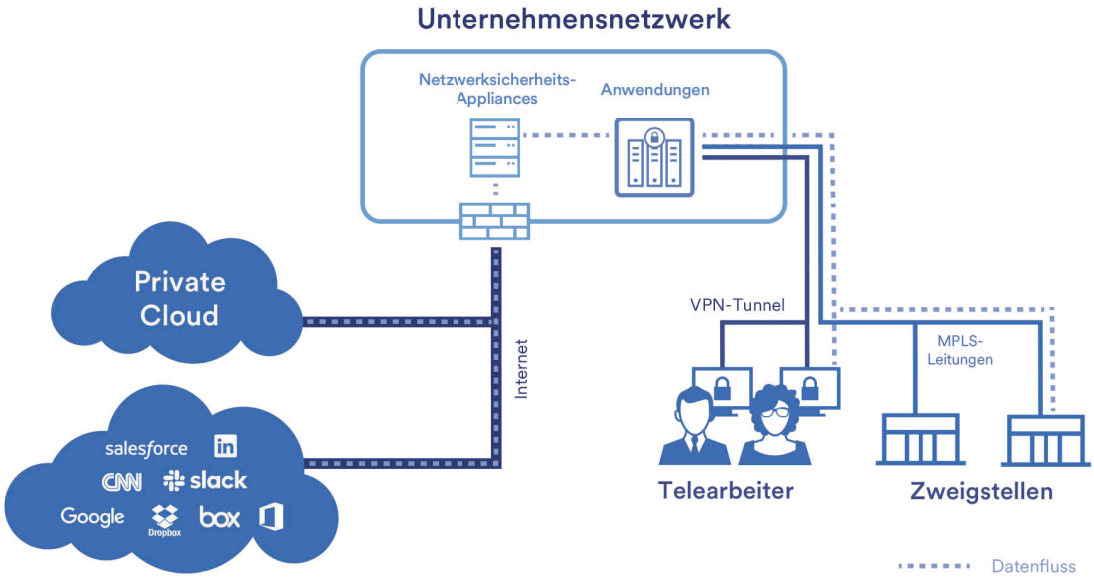

Abbildung 1. Traditionelle Netzwerkarchitektur

1. Quelle: Skyhigh Security: „Cloud Adoption and Risk Report: Work From Home Edition" (Bericht zu Cloud-Nutzung und Risiken: Ausgabe zu Arbeiten von zu Hause).

SSE

Security Service Edge (SSE) bezeichnet – laut Definition von Gartner[2] – mehrere integrierte, Cloud-zentrierte Sicherheitsfunktionen, die den sicheren Zugriff auf Websites, Cloud und Anwendungen ermöglichen. Das SSE-Framework vereint alle Sicherheitsdienste, einschließlich sichere Web-Gateways, Cloud Access Security Broker und Zero-Trust-Netzwerkzugriff, zu einem einzigen, Cloud-nativen Framework. Dieser integrierte Ansatz unterstützt die digitale Unternehmenstransformation und die Mitarbeitermobilität und minimiert gleichzeitig die Auswirkungen auf Sicherheit, Leistung, Komplexität und Kosten.

Beschleunigen Sie die SSE-Implementierung mit unserer integrierten Security Service Edge-Lösung

Die Lösung Skyhigh SSE ist eine SSE-Sicherheitsstruktur, die Daten- und Bedrohungsschutzfunktionen standortunabhängig bereitstellt und damit Ihren Mitarbeiter schnellen und sicheren Direktzugriff auf das Internet ermöglicht.

Durch die digitale Transformation gehen immer mehr Unternehmen zu einem standortunabhängigen Arbeitsmodell über, sodass dem schnellen und sicheren Zugriff der Telearbeiter auf interne Apps und Daten große Bedeutung zukommt. Der Zugriff von einer sicheren Service-Edge aus eröffnet ganz neue Möglichkeiten für den Schutz Ihrer Benutzer und Daten: von komplett transparentem Datenverkehr Ihrer Telearbeiter, über die Kontrolle nicht verwalteter Geräte bis hin zur Cloud-nativen Aktivitätenüberwachung.

Ermöglichen Sie direkten Internet-Zugriff, indem Sie den Datenverkehr Ihrer Bürostandorte und mobilen Benutzer mithilfe der Cloud-nativen extrem skalierbaren Service-Edge von Skyhigh Security nahtlos und direkt in die Cloud leiten. Sie übernimmt die weltweite Kontrolle über unbefugte Zugriffe, Datenrisiken und Bedrohungen, sodass der Umweg der Daten über Ihr Rechenzentrum entfällt.

- Durch den Wechsel zu einer in der Cloud bereitgestellten SSE, die Konnektivität und Sicherheit miteinander verbindet, können Unternehmen die Kosten und Komplexität verringern und gleichzeitig die Geschwindigkeit und Agilität ihrer Mitarbeiter steigern.
- Eine SSE-Architektur bietet an jedem Richtlinien-Entscheidungspunkt komplette Datentransparenz und -kontrolle – am Endgerät, über das Internet oder in der Cloud.
- Bedrohungsschutz-Kontrollen, die sich an veränderliche Risiken und Kontexte anpassen, ermöglichen den Schutz selbst vor extrem hochentwickelten Cyber-Angriffen und Datenverlusten.

Abbildung 2.
Security Service Edge

Bereitstellung von SSE mit Skyhigh SSE

SD-WAN kann Ihr Netzwerk so transformieren, dass es unkomplizierter und kosteneffektiver wird und die Benutzer produktiver arbeiten, weil es die Verbindungen zwischen den Benutzern und Cloud-Ressourcen vereinfacht und beschleunigt. Ohne Kopplung nicht mit einer universellen Cloud-Sicherheitsplattform muss der Datenverkehr jedoch weiterhin zurück zu Ihrem Rechenzentrum geführt werden. Dies beeinträchtigt die Produktivität und strapaziert ein ohnehin veraltetes Architekturmodell noch mehr.

Die extrem skalierbare Service-Edge von Skyhigh Security ist die Cloud-native Sicherheitsstruktur zwischen Ihren Mitarbeitern, der WAN-Infrastruktur, den Cloud-Diensten und dem Internet. Weitere Funktionen unserer Service-Edge:

- Peering-Abkommen für über 60 Zugangspunkte (PoPs) mit Content-Anbietern an IXPs (Internet Exchange Points) in aller Welt
- Bereitstellung des schnellstmöglichen Zugriffs auf Cloud-Anwendungen, oft schneller als direkter Cloud-Zugriff
- Vereinfachte Architektur, mit der Sie das Zugriffsverhalten Ihrer Mitarbeiter optimieren können – für alle Standorte, Anwendungen und Geräte
- 99,999 % Verfügbarkeit, damit die Mitarbeiter ununterbrochen arbeiten können

Führen Sie SD-WAN und ZTNA mit unserer in der Cloud bereitgestellten Service-Edge zusammen, um Ihren Technologiebestand und damit den Verwaltungsaufwand zu reduzieren. Profitieren Sie von geringer Latenz und unbegrenzter Skalierbarkeit mit weltweiter Cloud-Nutzung und Cloud-nativer Architektur. Durch die Einbindung von Skyhigh Security SSE in eine nahtlos integrierte SSE-Lösung können Unternehmen die Kosten und Komplexität reduzieren und gleichzeitig ein rasend schnelles Benutzererlebnis bieten.

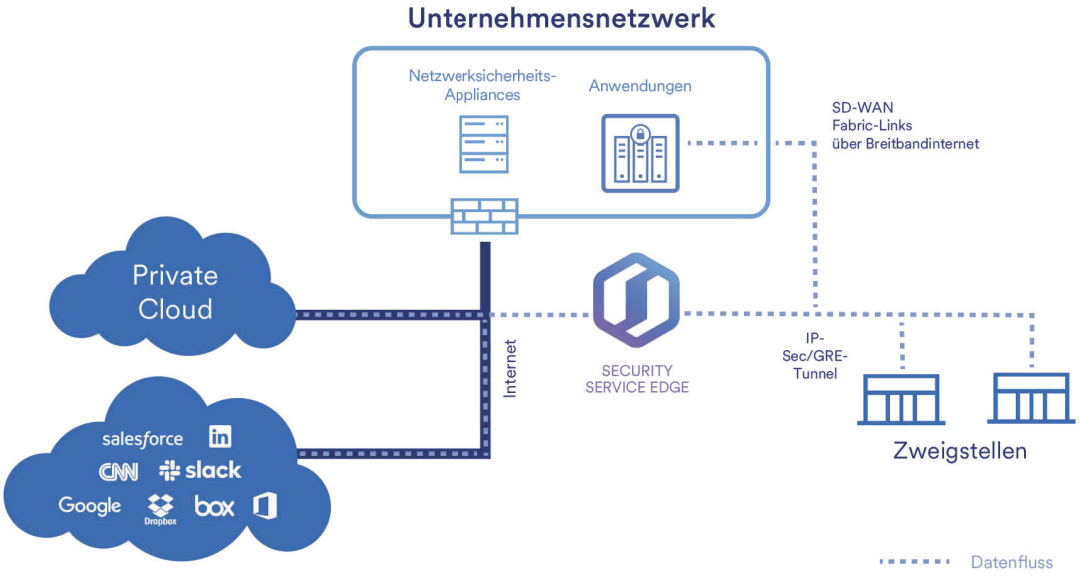

Abbildung 3.
Direct-to-Cloud-Transformation mit SSE

Mehrstufiger Datenschutz: Data Awareness an jedem Zugriffspunkt

Mit der Cloud-Transformation verlassen immer mehr Unternehmensdaten die Netzwerkperipherie, und auch die Zugriffe erfolgen außerhalb des Netzwerks, sodass sie von den herkömmlichen Datensicherheitskontrollen nicht mehr erreicht werden. Die Cloud-basierte Zusammenarbeit mit Dritten und zwischen Cloud-Diensten sowie der Zugriff durch nicht verwaltete Dienste und Geräte zuhause, die mit Peripherie-Elementen verbunden sind, lassen neue blinde Flecken entstehen, die in der Regel mehrere fragmentierte Datenschutzlösungen erfordern.

Der mehrstufige Datenschutz von Skyhigh Security bietet vollen Datenschutz für Ihre Mitarbeiter und schließt Datentransparenzlücken. Dabei fungiert jeder Kontrollpunkt als Teil einer Gesamtlösung.

- Datenklassifikationen können einmal definiert und richtlinienübergreifend angewendet werden, um Endgerät, Netzwerk, Internet und Cloud zu schützen.
- An jedem Kontrollpunkt werden gemeinsame Datenschutzrichtlinien durchgesetzt, sodass Sie einfach entscheiden können, wer Ihre Daten anzeigen und was er damit machen kann.
- Einheitliches Zwischenfall-Management zwischen Kontrollpunkten ist ohne erhöhten operativen Overhead möglich.

Skyhigh SSE lädt die Ereignisinformationen zu Zwischenfällen von allen Kontrollpunkten in eine Verwaltungskonsole, um eine zentrale Ansicht Ihrer Datenschutzumgebung zu erstellen. Die einheitliche Datenklassifikations- und Verwaltungsansicht liefert konsistente Erkennungsergebnisse und verhindert Sicherheitslücken im Datenkompromittierungsschutz (DLP), die durch die Verwendung mehrerer Tools mit unkoordinierten Richtlinien und Berichtsfunktionen entstehen. Unsere Lösung ermöglicht die Korrelation von Datenzwischenfällen aller Vektoren, sodass Administratoren Anzeichen für potenziell schwerwiegende Angriffe identifizieren können.

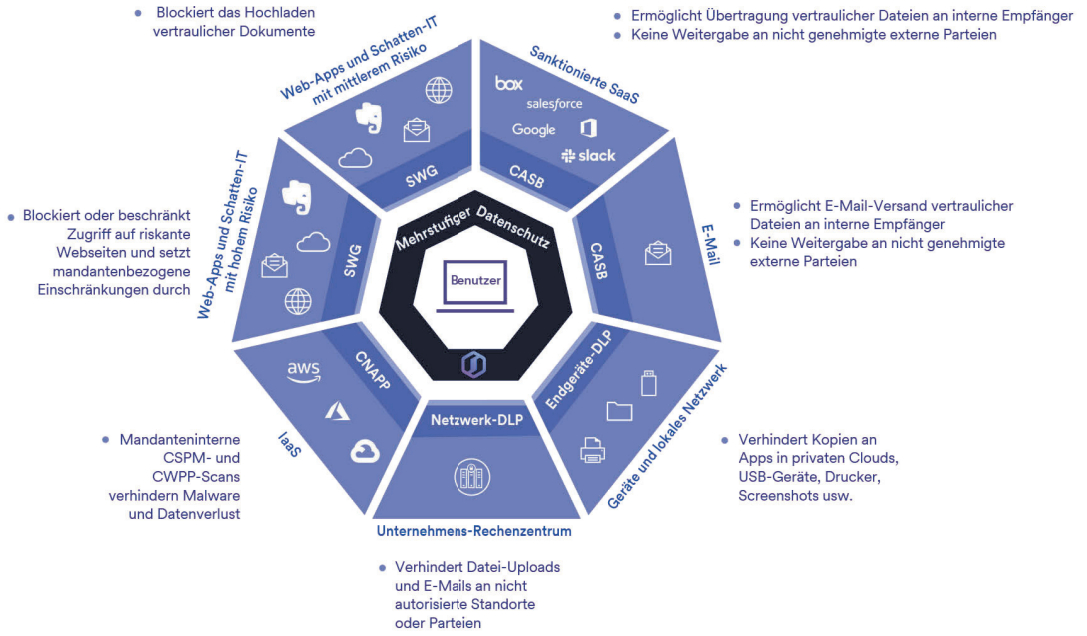

Abbildung 4.
Anwendungsbeispiele für den mehrstufigen Datenschutz mit Skyhigh Security SSE

Abwehr Cloud-nativer Bedrohungen und hochentwickelter Malware

Mit den wertvollen Ressourcen haben sich auch die Bedrohungsakteure in Richtung Cloud orientiert. Wir verzeichnen neue Angriffsmethoden, die die Funktionen der Cloud-Anbieter nutzen, um unter dem Radar bleiben und so Informationen suchen und stehlen zu können. Darüber hinaus bleiben hochentwickelte Malware und böswilliger Code in dateilosen Angriffen eine zunehmende Gefahr. Die Erkennung und Blockierung dieser Bedrohungen ohne Beeinträchtigung der Endbenutzerproduktivität erfordert neue Schutzmethoden. Die integrierte SSE-Lösung von Skyhigh Security wehrt Cloud-native Bedrohungen, hochentwickelte Malware und dateilose Angriffe mit einem Arsenal von traditionellen und modernen Bedrohungsschutzfunktionen ab. Die Abwehrmechanismen reduzieren die Gefahr eines Angriffs und Datenverlusts, während Ihr Unternehmen seine Netzwerk- und Produktivitäts-Tools in Cloud-basierte Dienste umwandelt.

Die Verhaltensanalyse von Benutzern und Entitäten (UEBA) findet Bedrohungen, die von herkömmlichen Technologien übersehen werden, weil sie die Cloud-Aktivitäten aller Cloud-Dienste überwacht und Millionen von Ereignissen seziert, um Anomalien und Bedrohungen in Ihrer Umgebung zu identifizieren. Diese Anomalien werden mit DLP-Zwischenfällen, Cloud-Konfigurationen und App-Schwachstellen korreliert, um eine vorgefertigte Ansicht Cloud-nativer Angriffe mithilfe des MITRE ATT&CK-Frameworks zu erstellen.

Jede Malware, die versucht, auf Ihren Endgeräten zu landen, trifft auf einen rigorosen, maschinenschnellen Inspektionspfad, der die akkurateste Echtzeit-Emulations-Sandbox der Branche beinhaltet. Bei Angriffen, die statt Malware auf Zero-Day Exploits setzen, oder dateilosen Angriffen mit Betriebssystembefehlen oder Website-Code, wechseln Benutzer automatisch in eine Remote-Browser-Isolierungssitzung, in der sie das ganze Internet ohne Infektionsrisiko nutzen können.

Alle Ereignisse können zusätzlich mit SIEM-Drittlösungen genutzt werden, um Sicherheitsteams zu unterstützen.

Abbildung 5. Security Service Edge-Bedrohungsschutz mit Remote-Browser-Isolierung

Skyhigh Private Access – Branchenweit erste ZTNA-Lösung, die vertrauliche Daten erkennt

Benutzer müssen auf interne, private Anwendungen zugreifen können, die häufig sensible Informationen enthalten. Bisher wurden dafür virtuelle private Netzwerke (VPNs) genutzt. Diese leiden jedoch unter Leistungs- und Skalierbarkeitsproblemen und erschweren die Durchsetzung strikter Sicherheitskontrollen. Traditionelle Lösungen für den Zero-Trust-Netzwerkzugriff (ZTNA) ermöglichen über detaillierte dynamische Zugriffsrichtlinien zwar einen schnellen, direkten Zugriff auf private Ressourcen, allerdings fehlen ihnen strenge Datenschutzkontrollen, um die vertraulichen Daten in diesen Ressourcen zu sichern.

Skyhigh Private Access sichert den Zugriff auf private Anwendungen von jedem Standort und Gerät aus und kontrolliert die Datenfreigabe mit dem integrierten Schutz vor Datenkompromittierungen (DLP). Private Access bewertet kontinuierlich die Risiken der angeschlossenen Geräte, indem es erweiterte Informationen zur Sicherheitslage extrahiert und über eine Cloud-native, extrem skalierbare Service-Edge blitzschnellen „Least Privileged"-Zugriff auf private Anwendungen bietet.

Cloud Firewall – Gesamten Nicht-Web-Verkehr für Telearbeiter und Remote-Standorte sichern

Bedingt durch die räumliche Verteilung von Remote-Standorten und Telearbeitern müssen die Sicherheitsverantwortlichen auch den Nicht-Web- und Nicht-Cloud-Verkehr sichern. Wenn alle Verbindungen für die Sicherheitsprüfung zurück zu zentralisierten Rechenzentren geführt werden müssen (Backhauling), steigt die Netzwerklatenz und die Benutzerleistung sinkt.

Über ein Cloud-basiertes Dienstmodell, das alle Ports und Protokolle lokaler Internet-Anschlüsse absichert, dehnt Cloud Firewall die Funktionen von Firewalls der nächsten Generation (NGFW) auf Telearbeiter aus. Die Lösung beinhaltet ein hochentwickeltes Richtlinienmodul, das Kontextsensibilität und ein Eindringungsschutzsystem (IPS) der nächsten Generation mit höchster IPS-Effizienz bietet, und ermöglicht gleichzeitig die End-to-End-Transparenz im Datenverkehr, um Netzwerkprobleme zu beheben und zu optimieren.

Skyhigh Private Access und Cloud Firewall verbinden sich mit unserer Security Service Edge-Lösung, um Unternehmen eine allumfassende, Cloud-basierte Lösung zu bieten, die ihre Transformation beschleunigt.

Informationen zu Skyhigh Security

Da Ihre vertraulichen Daten im Web, in Cloud-Anwendungen und verschiedenen Infrastrukturen verteilt sind, benötigen Sie einen neuen Sicherheitsansatz. Stellen Sie sich eine integrierte Security Service Edge-Lösung vor, die unabhängig von der Quelle kontrollieren kann, wie Daten verarbeitet, weitergegeben und erstellt werden. Mit Skyhigh Security können Unternehmen Daten sicher und zuverlässig mit jedem Gerät an beliebige Parteien in der Cloud weitergeben. Lernen Sie Skyhigh Security kennen, die branchenführende, datensensitive Cloud-Sicherheitsplattform.

Weitere Informationen

Weitere Informationen erhalten Sie unter skyhighsecurity.com.

Skyhigh Security

3099 North First Street
San Jose, CA 95134, USA
+1 888.847.8766
skyhighsecurity.com

Skyhigh Security ist eine eingetragene Marke der Musarubra US LLC. Alle anderen Namen und Marken sind Eigentum dieser Unternehmen oder der jeweiligen Besitzer. Copyright © 2022. März 2022