Cisco Secure Access

Schützen Sie Ihre hybride Belegschaft mit agiler Cloud-Security

Juli 2023

Inhalt

Hybride Arbeit und Security Service Edge

Die neue Ära der hybriden Arbeit erfordert einen überarbeiteten Sicherheitsansatz. SSE (Security Service Edge) spielt dabei eine entscheidende Rolle in Bezug auf die Strategie für hybride Arbeit eines jeden Unternehmens. SSE kombiniert mehrere Sicherheitsfunktionen in der Cloud, um MitarbeiterInnen, Auftragnehmer oder Partner, die von einem beliebigen Standort aus arbeiten, sowie erfolgskritische Ressourcen zu schützen. Unabhängig davon, ob Sitzungen Anwendungen in privaten Rechenzentren, an SaaS-Standorten, Peer-to-Peer, IaaS oder auf Websites umfassen – SSE fungiert als „Sicherheitsvermittler", um verschiedene Arten von schädlichen Aktivitäten zu identifizieren und abzuwehren. EndbenutzerInnen wird bei ihrer Arbeit ein sicheres, transparentes Benutzererlebnis garantiert, und das unabhängig von ihrem Standort – im Büro, zu Hause oder unterwegs. SSE-Lösungen müssen drei Hauptanforderungen erfüllen: die Bereitstellung eines herausragenden Benutzererlebnisses, die Reduzierung der IT-Komplexität und die verbesserte Wirksamkeit der Sicherheit.

Produktübersicht

Cisco Secure Access ist eine auf Zero Trust basierende konvergente Cloud-Security-SSE-Lösung, die nahtlosen, transparenten und sicheren Zugriff von überall ermöglicht. Diese Lösung nutzt einen umfassenden Satz von Kernmodulen, darunter ZTNA, SWG, CASB und FWaaS. Die Plattform geht zudem über diese Funktionen hinaus und fügt Multimode-DLP, DNS-Sicherheit, eine Remote-Browser-Isolierung (Remote Browser Isolation; RBI), Sandboxing und Threat-Intelligence von Talos hinzu. Durch die Nutzung dieser Funktionen, die sich alle auf einer in der Cloud bereitgestellten Plattform befinden, können Unternehmen eine Vielzahl von Sicherheitsherausforderungen bewältigen. BenutzerInnen können jetzt sicher und mühelos auf alle benötigten Ressourcen und Apps zugreifen – unabhängig von Protokoll, Port oder Anpassungsniveau.

Cisco Secure Access wurde mit bekannten administrativen Kontrollen, Datenstrukturen und Richtlinienmanagement entwickelt, wodurch die Interoperabilität mit anderen synergistischen Komponenten vereinfacht wird. Diese Lösung lässt sich beispielsweise gut mit anderen Cisco Angeboten wie Cisco SD-WAN, XDR und Digital Experience Monitoring sowie Technologien von Drittanbietern kombinieren, um die Ergebnisse für Kunden zu verbessern.

Secure Access sorgt für modernste Cybersicherheit und reduziert gleichzeitig Risiken von Grund auf. Dabei vereinfacht es die IT-Betriebskomplexität erheblich und minimiert den Aufwand für EndbenutzerInnen.

Besser für BenutzerInnen

Cisco Secure Access verbessert das Benutzererlebnis erheblich, um Reibungspunkte zu beseitigen, verhindert eine potenzielle Umgehung erforderlicher Sicherheitsmaßnahmen und steigert die Produktivität. Die Lösung nutzt einen einheitlichen Client, über den sich BenutzerInnen einfacher verbinden können. So gelangen sie nach der Authentifizierung direkt zur gewünschten Anwendung. Eine solche „All-Access"-Funktion verbindet sie automatisch mit Least-Privilege-Konzepten, vorkonfigurierten Sicherheitsrichtlinien und anpassbaren Durchsetzungsmaßnahmen, die durch den/die AdministratorIn kontrolliert werden.

Unabhängig davon, ob Sitzungen ZTNA oder VPNaaS für bestimmte nicht standardmäßige Apps nutzen, müssen BenutzerInnen keine zusätzlichen Maßnahmen ergreifen. So wird verhindert, dass mühsame Verifizierungsaufgaben immer wieder wiederholt werden müssen. Mögliche Unsicherheiten von BenutzerInnen hinsichtlich der erforderlichen Zugriffsmethode für verschiedene Ressourcen oder Fragen, ob ein separater Client gestartet oder ein anderer Anmeldeprozess festgelegt werden muss, entfallen. Der zentralisierte Zugriff auf alle Anwendungen vereinfacht den Verbindungsprozess für BenutzerInnen erheblich, ermöglicht maximale Sicherheit inklusive Validierung des Benutzer- und Gerätestatus und verbessert die Produktivität.

Einfacher für die IT

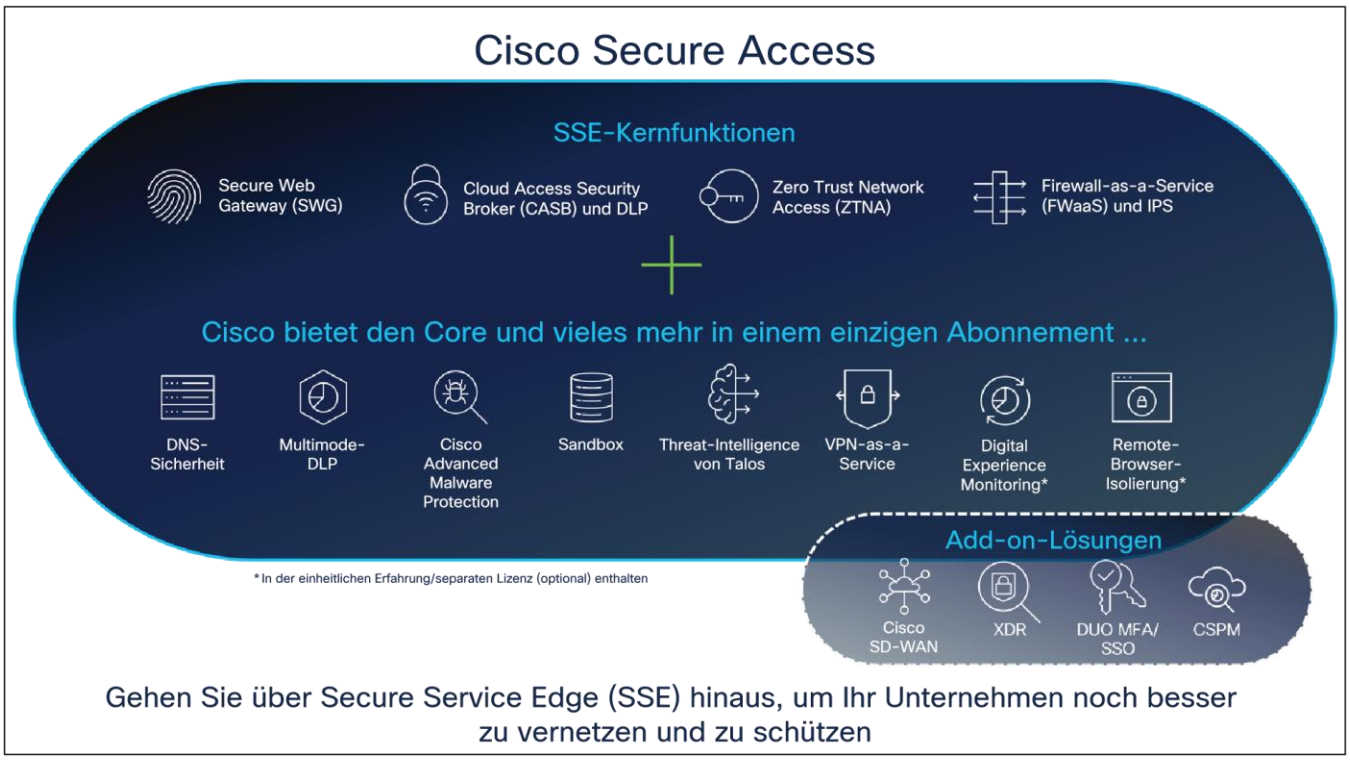
IT-Teams von heute müssen eine Vielzahl von Sicherheitstools integrieren, benötigen mehrere Managementkonsolen sowie Richtlinien-Engines und müssen für jedes Endbenutzergerät mehrere Software-Agenten bereitstellen und verwalten. Diese Herausforderungen werden durch die separaten Berichte, Warnungen und Vorfälle verstärkt, die von jedem einzelnen Sicherheitsprodukt ausgehen.

Cisco Secure Access vereinfacht und automatisiert den Betrieb für Sicherheits- und IT-Teams über eine zentrale, in der Cloud verwaltete Konsole, einen einheitlichen Client, einen zentralisierten Richtlinienerstellungsprozess und aggregierte Berichte. Anstatt verschiedene Produkte bereitzustellen, muss die IT nur noch ein Tool verwalten. Dies führt zu messbaren Effizienzsteigerungen, Kostensenkungen und einer flexibleren IT-Umgebung, die eine höhere geschäftliche Flexibilität ermöglicht. Die IT kann Bedrohungen jetzt schneller erkennen und blockieren, Untersuchungen beschleunigen und Korrekturmaßnahmen minimieren. Gleichzeitig verbessert sie die Transparenz der Endbenutzeraktivitäten mit weniger manuellen Aggregationsaufgaben.

Mehr Sicherheit für alle

Cisco Secure Access bietet branchenführende Wirksamkeit der Sicherheit für EndbenutzerInnen und lokale Ressourcen. Die erweiterten Funktionen des Architekturansatzes für eine tiefgreifende Verteidigung schützen vor einer Vielzahl von Cybersicherheitsbedrohungen. EndbenutzerInnen werden vor Risiken wie infizierten Dateien, schädlichen Websites sowie Phishing- und Ransomware-Angriffen geschützt. IT- und Sicherheitsteams können die Angriffsfläche reduzieren, Kontrollen nach dem Least-Privilege-Prinzip durchsetzen, die Statusvalidierung aktivieren und Sicherheitslücken in verteilten Umgebungen effektiv schließen.

Zudem erhalten Sicherheitsteams Einblicke in Betriebsabläufe nicht autorisierter Schatten-IT sowie die Nutzung nicht genehmigter Anwendungen und können solche Aktivitäten blockieren. Durch das Cloaking interner Ressourcen und das Verhindern, dass Hacker ihre Anwesenheit erkennen, profitiert die IT von einer zusätzlichen Sicherheitsebene. All diese Funktionen werden durch Threat-Intelligence von Cisco Talos mit unübertroffener Telemetrie, umfassender Forschung und fortschrittlicher KI unterstützt, um Bedrohungen zu identifizieren und zu stoppen und Korrekturmaßnahmen zu beschleunigen. Durch die Risikominimierung stellen Unternehmen ihre Business Continuity sicher und vermeiden die potenziell rufschädigenden und finanziellen Auswirkungen einer Sicherheitsverletzung.



Funktionen und Vorteile

Tabelle 1. Funktionen und Vorteile

Funktion	Vorteil
Zero Trust Network Access (ZTNA)	Bereitstellung von granularem, anwendungsspezifischem Zugriff auf private Anwendungen in lokalen Rechenzentren und in Cloud-/IaaS-Umgebungen. Basierend auf definierten Zugriffskontrollrichtlinien nutzt es die Berechtigungen nach dem Least-Privilege-Prinzip sowie kontextbezogene Einblicke, um den Zugriff standardmäßig granular zu verweigern, und vermittelt standort-unabhängigen Benutzerzugriff auf Anwendungen nur dann, wenn dieser ausdrücklich gewährt wird. • Zwei Zugriffsmethoden: Client-basierter und Client-loser browserbasierter Zugriff, granulare Benutzer- und anwendungsbasierte Zugriffsrichtlinie, SAML-Authentifizierung,integrierter Identitätsanbieter (IdP) und kontextbezogene Zugriffskontrolle • Client-basierter Zugriff nutzt den einheitlichen Cisco Secure Client • Richtet sicheren Zugriff ein, nachdem eine Gerätestatusprüfung durchgeführt wurde • Authentifiziert BenutzerInnen durch einen sicheren, verschlüsselten Tunnel, sodass BenutzerInnen nur Anwendungen und Services sehen können, auf die sie Zugriff haben • Der Anwendungsproxy bietet transparenten, sicheren Remote-Zugriff, ohne dass die Anwendungen dem Internet zugänglich gemacht werden – er verbirgt sogar die Netzwerkdetails privater Apps vor den Clients, die auf diese Anwendungen zugreifen; dadurch wird verhindert, dass Angreifer etwas über die IP-Reconnaissance erfahren, selbst wenn sie ein Client-Gerät kompromittiert haben • Verhindert laterale Bewegungen von Angreifern • Implementiert standort- und gerätespezifische Richtlinien für die Zugriffskontrolle, um zu verhindern, dass möglicherweise kompromittierte Geräte eine Verbindung zu den zugehörigen Services herstellen • AdministratorInnen weisen Zugriffsrechte für Auftragnehmer und MitarbeiterInnen nur auf für sie erforderliche Ressourcen zu, ohne dabei laterale Bewegungen zu ermöglichen

Funktion	Vorteil
	• AdministratorInnen können Statusprofile für Betriebssystemtyp und -version eines Endgeräts, Browsertyp und -version sowie Standortdaten konfigurieren, die bei der Zugriffsentscheidung verwendet werden sollen • Stellt BenutzerInnen hilfreiche Informationen zur Erklärung der Ursache für den verweigerten Zugriff bereit
VPNaaS	Nicht alle privaten Apps können von ZTNA abgedeckt werden. Die Cloud-basierte Option VPNaaS für sicheren Remote-Zugriff und sicheren Internetzugriff für nicht-webbasierten Internetdatenverkehr ist im Lieferumfang enthalten. • Funktionsbeispiele: Anwendungsfallunterstützung (Unterstützung von Split-Tunneling und Tunnel-All, Peer-to-Peer-Kommunikation, Trusted Network Detection, BYO-Zertifikat, Split-DNS, Dynamischer-Split-DNS); mehrere Authentifizierungsverfahren (SAML, Zertifikat, Radius, LDAP); Benutzerfreundlichkeit (kontinuierlich aktiver VPN, Start vor der Anmeldung); Vereinfachung des IT-Betriebs (lokaler IP-Pool, mehrere VPN-Profile) • Ermöglicht Remote-BenutzerInnen den Zugriff auf private Anwendungen über die Security Access-Fabric mit Cisco Secure Client • Die identitätsbasierte Zugriffskontrolle ist über die SAML-Authentifizierung über den IdP des Kunden verfügbar • Der Endpunktstatus wird ebenfalls bewertet; dies ermöglicht eine granulare Zugriffskontrolle für private Ressourcen

Funktion	Vorteil
Secure Web Gateway (vollständiger Proxy)	Protokollierung und Überprüfung des gesamten Webdatenverkehrs über die Ports 80/443 für mehr Transparenz, Kontrolle und Schutz. IPsec-Tunnel, PAC-Dateien und Proxyverkettungen werden genutzt, um den Datenverkehr weiterzuleiten und so vollständige Transparenz, Kontrollen auf URL- und Anwendungsebene und intelligenten Schutz vor Bedrohungen bereitzustellen. • Inhaltsfilterung nach Kategorie oder bestimmten URLs, um Ziele zu blockieren, die gegen Richtlinien oder Compliance-Vorschriften verstoßen • Scannen aller heruntergeladenen Dateien auf Malware und andere Bedrohungen • Sandboxing mit Cisco Secure Malware Analytics analysiert unbekannte Dateien (siehe den entsprechenden Abschnitt zu Cisco Secure Malware Analytics) • Dateityp-Blockierung (blockiert z. B. das Herunterladen von .exe-Dateien) • Vollständige oder selektive SSL-Entschlüsselung zum Schutz vor versteckten Angriffen und zeitaufwendigen Infektionen • Granulare App-Kontrollen, um bestimmte Benutzeraktivitäten in ausgewählten Apps zu blockieren (z. B. Datei-Uploads auf Dropbox, Anhänge bei Gmail und Beiträge oder geteilte Beiträge auf Facebook) • Detaillierte Berichterstellung mit vollständigen URL-Adressen, Netzwerkidentität, Bestätigungs- oder Abwehraktionen und der externen IP-Adresse
Cloud Access Security Broker (CASB)	Aufdeckung von Schatten-ID durch Erkennung und Berichterstattung zu verwendeten Cloud-Anwendungen Verwaltung der Cloud-Annahme, geringere Risiken und Blockierung der Verwendung anstößiger, unproduktiver, riskanter oder unangemessener Cloud-Anwendungen • Schutz vor Datenverlust (Data Loss Prevention, DLP), um zu verhindern, dass vertrauliche Daten durch Exfiltration das Unternehmen und die Cloud verlassen (siehe separaten Abschnitt zu DLP) • Berichte mit Informationen zu Anbieterkategorie, Anwendungsname und Aktivitätsvolumen für jede erkannte App • App-Details und Risikoinformationen, wie z. B. die Webreputationsbewertung, die finanzielle Tragfähigkeit und relevante Compliance-Zertifizierungen • Malware-Erkennung in der Cloud zur Erfassung und Entfernung von Malware aus Cloud-basierten Datei-Speicheranwendungen und Sicherstellung, dass diese Daten in den Anwendungen frei von Malware bleiben • Möglichkeit, bestimmte Cloud-Anwendungen zu blockieren oder zuzulassen • Tenant-Einschränkungen zur Kontrolle der Instanz(en) von SaaS-Anwendungen, auf die alle BenutzerInnen oder bestimmte Gruppen/Einzelpersonen zugreifen können
Schutz vor Datenverlust (Data Loss Prevention, DLP)	Multimode-Schutz vor Datenverlust. Direkte Analyse vertraulicher Daten für Transparenz und Kontrolle über vertrauliche Daten, die Ihr Unternehmen verlassen. API-basierte DLP-Funktionen für die Out-of-Band-Analyse ruhender Daten in der Cloud. Enthält einheitliche Richtlinien und Berichte. • Über 190 integrierte Inhaltsklassifizierungen, darunter DSGVO, PCI-DSS, HIPAA, PII und PHI • Anpassbare integrierte Inhaltsklassifizierungen mit Grenzwert und Nähe zur Optimierung und Reduzierung von falsch-positiven Meldungen • Benutzerdefinierte Wörterbücher mit benutzerdefinierten Phrasen (z. B. Codenamen für Projekte) • Erkennung und Berichterstellung zur Nutzung vertraulicher Daten und Drilldown-Berichte zur Identifizierung von missbräuchlicher Nutzung • Prüfung der Inhalte von Cloud-Apps und Webdatenverkehr sowie Durchsetzung von Datenrichtlinien

Funktion	Vorteil
Firewall-as-a-Service (FWaaS)	Bietet Transparenz und Kontrolle für nicht-webbasierten Datenverkehr, der von Anfragen an das Internet stammt, über alle Ports und Protokolle hinweg. Umfasst mobile Apps, Peer-to-Peer-Dateifreigaben, Collaboration (z. B. Webex oder ZOOM), O365 oder sonstigen nicht-webbasierten oder Nicht-DNS-Datenverkehr. • Bereitstellung, Management und Berichterstellung über das zentrale, einheitliche Security Access-Dashboard • Anpassbare Richtlinien (IP-, Port-, Protokoll-, Anwendungs- und IPS-Richtlinien) • Layer-3-/4-Firewall zur Protokollierung aller Aktivitäten und Blockierung von unerwünschtem Datenverkehr mithilfe von IP-, Port- und Protokollregeln • Skalierbare Cloud-Computing-Ressourcen beseitigen Bedenken hinsichtlich der Appliance-Kapazität • Layer-7-Anwendungstransparenz und -kontrolle zum Identifizieren einer wachsenden Anzahl von über 2.800 nicht-webbasierten Anwendungen, die wahlweise blockiert oder zugelassen werden können • Entschlüsselung des Datenverkehrs vor der Prüfung
Intrusion-Prevention-Systeme (IPS)	IPS überprüft Netzwerkverkehrsströme und beugt der Ausnutzung von Sicherheitslücken mit einer zusätzlichen Ebene der Bedrohungsabwehr vor, die auf der SNORT 3-Technologie und signaturbasierter Erkennung basiert. • Verwendung eines einheitlichen Dashboards, Erstellung von Richtlinien zur Prüfung des Datenverkehrs und Ergreifen automatisierter Maßnahmen, damit gefährliche Pakete erkannt und gelöscht werden, noch bevor sie das Netzwerk erreichen • Bietet IPS-Schutz für Internetverkehr und privaten Datenverkehr • Konfiguration von Zugriffsrichtlinien und Optionen für verschiedene benutzerdefinierte Profile abhängig vom Datenverkehrsziel • Nutzung einer umfangreichen und wachsenden Basis von über 40.000 Signaturen von Cisco Talos • Signaturen sind in vordefinierten anpassbaren Vorlagen verfügbar • Erkennung und Blockierung der Ausnutzung von Schwachstellen
Cisco Secure Malware Analytics	Vereint erweitertes Sandboxing und Threat-Intelligence in einer umfassenden Lösung, um Unternehmen vor Malware zu schützen. Bietet Zugriff auf die vollständige Cisco Secure Malware Analytics-Konsole, die die Ausführung schädlicher Dateien in einer Glovebox ermöglicht, die Ausführung von Aktionen verfolgt und von der Datei generierte Netzwerkaktivitäten erfasst. In Kombination mit Investigate können SicherheitsanalystInnen weiter gehen und schädliche Domänen, IPs, und den Aktionen einer Datei zugeordnete ASNs aufdecken, um einen vollständigen Überblick über die Infrastruktur, Taktiken und Techniken eines Angreifers zu erhalten. • Fähigkeit, versteckte Angriffsmethoden zu erkennen und schädliche Dateien zu melden • Zentrale, korrelierte Informationsquelle für eine schnellere Nachverfolgung von Bedrohungen und Incident Response • APIs zur Integration in XDR und häufig verwendete SIEMs zur Anreicherung von Sicherheitsdaten • Retrospektive Benachrichtigung bei Änderung der Dateidisposition (ursprünglich gut/später als schädlich eingestuft)

Funktion	Vorteil
Remote-Browser-Isolierung (RBI)	RBI schützt BenutzerInnen und Organisationen vor browserbasierten Bedrohungen. Es verlagert die Ausführung von Browseraktivitäten von BenutzerInnen zum Schutz vor Internetbedrohungen auf eine Cloud-basierte, virtualisierte Remote-Browserinstanz. Der Website-Code wird separat ausgeführt, und für den/die BenutzerIn wird nur ein sicherer visueller Stream bereitgestellt. Dies ist für den/die EndbenutzerIn völlig transparent. Sie müssen sich keine Gedanken über Malware machen, die noch nicht erkannt wurde. • Isolierung des Webdatenverkehrs zwischen Benutzergeräten und browserbasierten Bedrohungen • Schutz vor Zero-Day-Bedrohungen • Präzise Kontrollen für verschiedene Risikoprofile • Schnelle Bereitstellung ohne Änderung der bestehenden Browserkonfiguration • On-Demand-Skalierung zum einfachen Schutz zusätzlicher BenutzerInnen • Schutz von MitarbeiterInnen, die möglicherweise auf bekannte risikobehaftete Websites zugreifen müssen – die Produktivität wird nicht durch Blockierungen beeinträchtigt und die BenutzerInnen bleiben geschützt
Sicherheit auf DNS-Ebene	Erzwingt eine Filterung auf DNS-Ebene, um Anfragen an schädliche und unerwünschte Ziele zu blockieren, bevor eine Verbindung hergestellt wird. Blockiert Bedrohungen an jedem Port oder Protokoll, bevor sie in das Netzwerk oder die Endpunkte eindringen können. • Schützt den Internetzugriff über alle Netzwerkgeräte, Standorte und alle Roaming-BenutzerInnen hinweg • Bietet detaillierte Berichte zu DNS-Aktivitäten nach Art der Sicherheitsbedrohung oder Webinhalte und der ergriffenen Maßnahmen • Speichert Protokolle aller Aktivitäten • Beschleunigte Einführung für Tausende von Standorten und BenutzerInnen für sofortigen Schutz
Threat-Intelligence von Talos	Als einer der weltweit führenden Anbieter von innovativer Sicherheitsforschung analysiert Talos täglich hunderte Milliarden von DNS-Anfragen und andere Telemetriedaten. Es führt kontinuierlich KI-, statistische und Machine-Learning-Modelle in dieser riesigen Datenbank aus, um Einblicke in Cyberbedrohungen zu erhalten und die Incident-Response-Raten zu verbessern. • Erkennung von schädlichen Domänen, IPs, Malware und URLs, bevor diese bei Angriffen verwendet werden • Priorisierung bei der Untersuchung von Vorfällen • Schnellere Untersuchung von und Reaktion auf Vorfälle • Vorhersagen des Ursprungs zukünftiger Angriffe, indem die Infrastrukturen der Angreifer identifiziert und skizziert werden

Funktion	Vorteil
Malware-Erkennung in der Cloud	Erkennt und entfernt Malware aus Cloud-basierten Dateispeicheranwendungen. Erweitert den Sicherheitsschutz, indem schädliche Dateien erkannt und korrigiert werden, bevor sie einen Endpunkt erreichen. • Erhöht die Effektivität und Effizienz von Sicherheitsadministratoren: Nach der Aktivierung werden alle Dateien in Cloud-basierten Services automatisch gehasht und zum Malware-Scan gesendet; jede Datei, die Malware enthält, wird gekennzeichnet, damit ein Sicherheitsadministrator diese beheben kann – dies beinhaltet Quarantäne und/oder Löschung • Unterstützt Box, Dropbox, Webex und Microsoft 365
Zentrale Konsole für Management und Berichterstattung	Vereinheitlichte Erstellung von Sicherheitsrichtlinien, einschließlich Intent-Based Rules, und Management für den Zugriff auf das Internet, öffentliche SaaS-Apps und private Apps. Bietet umfassende Protokollierung und die Möglichkeit, Protokolle in Enterprise-SOC usw. zu exportieren. • Zentraler Ort zum Definieren von Richtlinien für alle BenutzerInnen und jede Anwendung, vereinfacht die Erstellung von Sicherheitsrichtlinien und fördert die Konsistenz der Richtliniendefinition für das gesamte Unternehmen • Eine einheitliche Quelle (BenutzerInnen, Geräte) und einheitliche Ressourcen (Anwendungen, Ziel) stellt sicher, dass die Sicherheitsrichtlinie den BenutzerInnen folgt, unabhängig von der Anschlussstelle und unabhängig davon, auf welche App zugegriffen wird • Reduziert laufende Aktivitäten zum Richtlinienmanagement • Verbessert die Transparenz und die Bedrohungserkennungszeit mit aggregierten Berichten • Vereinfacht den gesamten Untersuchungsprozess von SOC/SicherheitsanalystInnen
App-Anschlüsse	App-Anschlüsse vereinfachen administrative Aufgaben, damit eine sichere Netzwerkverbindung zu privaten Apps hergestellt werden kann. Sie verbinden Cisco Secure Access mit Kundenrechenzentren. • SSE-Teams sind bei Änderungen von Geräten oder Firewallregeln weniger abhängig von Netzwerkteams • Vermeidung komplexen Routings, wie z. B. bei der Einrichtung von dynamischem Routing oder überlappenden Subnetzen • In Szenarien wie einer Fusion werden Netzwerke häufig mit überlappenden IPs usw. getrennt gehalten, die Verwendung von Tunneln gestaltet sich komplex; App-Anschlüsse können diese Komplexität abschirmen • Schützt private Apps, indem ihr Standort (IP-Adresse) verdeckt wird und nur Verbindungen über die Zero-Trust-Richtlinien in Security Access zugelassen werden

Paketoptionen

Cisco Secure Access ist die umfassendste SSE-Lösung und in einem einzigen Abonnement erhältlich. Es dient der Erzielung von besseren Sicherheitsergebnissen und einer gesteigerten Produktivität. Es wird in Paketen angeboten, die es Kunden leicht machen, das richtige Maß an Schutz und Abdeckung für ihre Unternehmensanforderungen auszuwählen. Derzeit gibt es zwei Pakete: Cisco Secure Access Essentials und Cisco Secure Access Advantage.

Tabelle 2. Kernpaket

Kategorie	Merkmale	Secure Access Essentials	Secure Access Advantage
Sicherer Zugriff	Sicherer Internetzugriff • Roaming-Sicherheit	✓	✓

Kategorie	Merkmale	Secure Access Essentials	Secure Access Advantage
	• Cisco SD-WAN-DIA-Integration • VPNaaS		
	Sicherer privater Zugriff • Client-basierter ZTNA • Client-loser ZTNA • VPNaaS	✓	✓
Grundlegende Sicherheit	Cloud-basierte Firewall für Layer-3- und Layer-4-Kontrollen von Web-Apps und privaten Apps	✓	✓
	Secure Web Gateway (Proxy für Webdatenverkehr, URL-Filterung, Inhaltsfilterung, erweiterte App-Kontrollen)	✓	✓
	CASB – Erkennung von Cloud-Apps, Risikobewertung, Blockierung, Erkennung von Cloud-Malware;Tenant-Kontrollen	✓	✓
	Remote-Browser-Isolierung (riskant*)	✓	✓
	Cisco Secure Malware Analytics (Sandbox)	Begrenzt	Unbegrenzt
Erweiterte Sicherheitsmethoden	Cloud-basierte Layer-7-Firewall		✓
	IPS-Schutz		✓
	Schutz vor Datenverlust (DLP) für Webanwendungen		✓
	Remote-Browser-Isolierung (alle**)		✓
Support	Erweiterter Support von Cisco rund um die Uhr per E-Mail und Telefon	✓	✓

* Riskant: Isolierung nicht kategorisierter Websites und Sicherheitskategorien (einschließlich potenziell schädlicher)

** Alle: Isolierung aller ausgewählten Ziele, einschließlich Inhalts- und Sicherheitskategorien, Ziellisten, Anwendungen, nicht kategorisiert usw.

Weitere Informationen

Weitere Informationen finden Sie unter Cisco Secure Access.

Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien-Pazifik-Raum
Cisco Systems (USA) Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter **www.cisco.com/go/offices**.

Gedruckt in den USA C78-3777960-00 07/23