Cisco SECURE

Cisco Secure Access schützt User und Ressourcen in Hybrid-Umgebungen

Gesteigerte Flexibilität und umfassende Cloud-Nutzung bringen viele Vorteile. Leider vergrößert sich dadurch auch die Angriffsfläche, es entstehen Sicherheitslücken und das Benutzererlebnis wird beeinträchtigt.

Das neue Arbeitsmodell

Der hybride Arbeitsplatz wird bleiben

78 % der Unternehmen ermöglichen der Belegschaft den Wechsel zwischen Arbeit im Homeoffice und im Büro

Quelle: 2023 Security Service Edge (SSE) Adoption Report (Cyber Security Insiders, Axis)

Cloud-Nutzung wird immer verbreiteter

50 % der Workload in Unternehmen wird in der Public Cloud ausgeführt

Quelle: 2022 Flexera State of the Cloud

Sicherheitsbedenken bezüglich Remote-Arbeit wachsen

47 % der Unternehmen betrachten Remote-Arbeit als ihre größte Herausforderung

Quelle: 2022 Security Visibility Report (Cybersecurity Insiders)

Unternehmen und Security-Teams müssen sich anpassen

Für einen sicheren und nahtlosen Zugriff müssen IT-Verantwortliche:

- den Zugriff auf private Anwendungen vereinfachen
- den Zugriff kontextbasiert, kontinuierlich oder per Least-Privilege-Prinzip steuern
- Transparenz- und Sicherheitslücken verhindern
- sichere Konnektivität über verschiedene App-Typen und Ziele gewährleisten
- ein hochwertiges Benutzererlebnis bereitstellen
- die Anzahl der Tools und Komplexität der Infrastruktur reduzieren

Eine ganzheitliche Cybersecurity-Strategie

Security Service Edge (SSE) ist ein Ansatz, der Unternehmen dabei unterstützt, sich an die neue Realität anzupassen. Dabei wird der allgemeine Sicherheitsstatus verbessert und gleichzeitig die Komplexität für IT-Teams und EndbenutzerInnen reduziert. SSE schützt BenutzerInnen und Ressourcen und vereinfacht die Bereitstellung durch die Konsolidierung mehrerer Sicherheitsfunktionen, darunter Web Gateway, Broker für sicheren Cloud-Zugriff und Zero-Trust-Netzwerkzugriff. Das ermöglicht eine sichere, nahtlose und direkte Verbindung zum Web, zu Cloud-Services und zu privaten Anwendungen. Cisco Secure Access umfasst alle oben aufgeführten Komponenten und mehr und sorgt für ein noch höheres Sicherheitsniveau und herausragende Benutzerzufriedenheit.

Unternehmen setzen auf konsolidierte Cloud-basierte Sicherheit

65 % planen die Einführung von SSE innerhalb von 2 Jahren

Quelle: 2023 Security Service Edge (SSE) Adoption Report (Cyber Security Insiders, Axis)

80 % werden bis 2025 über einen einheitlichen Zugang zu Web- und Cloud-Services sowie privaten Anwendungen über SASE/SSE verfügen

Quelle: Gartner SASE Market Guide-2022

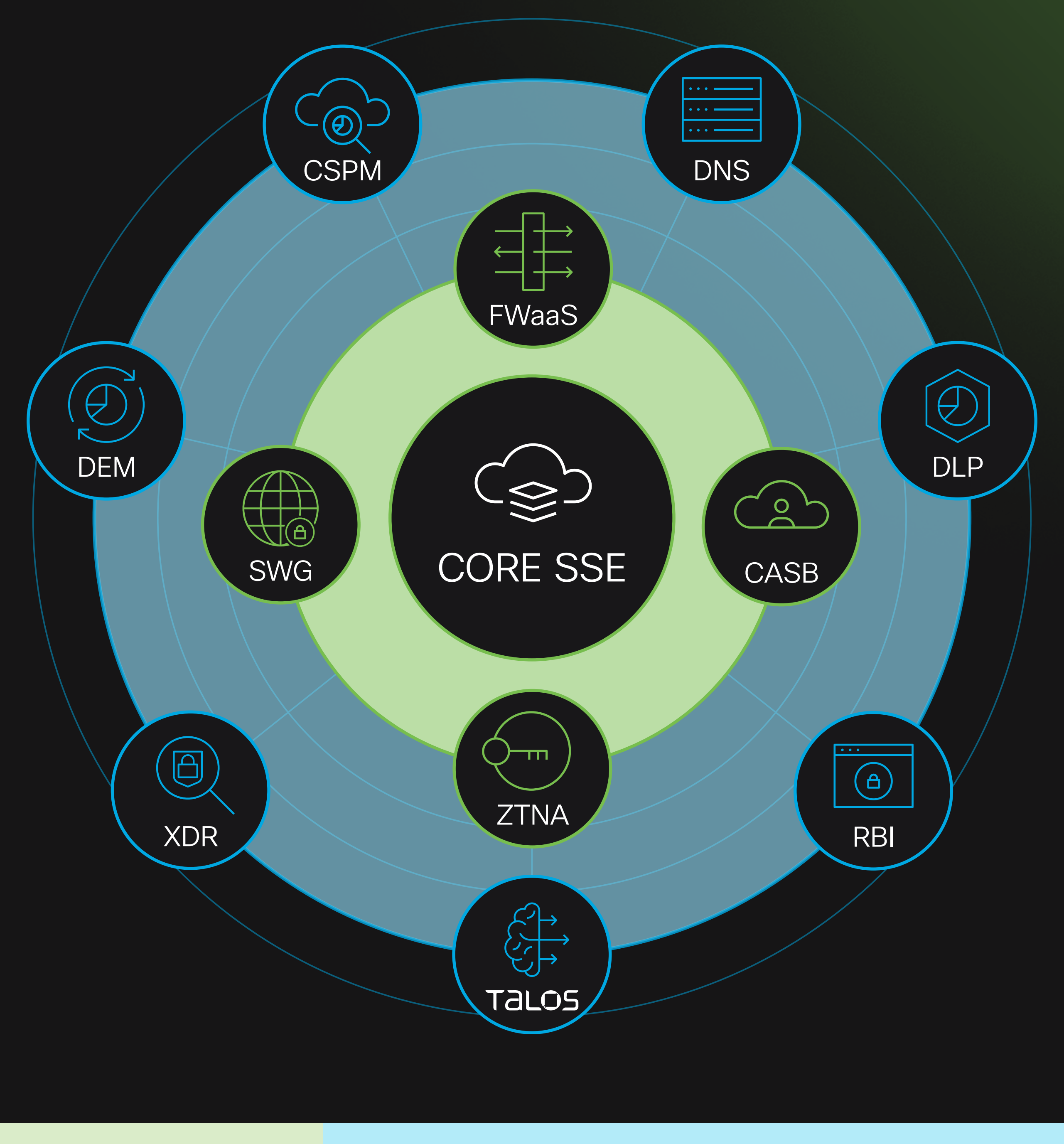
39 % betrachten eine SSE-Plattform als wichtigste Technologie für eine Zero Trust-Strategie

Quelle: 2023 Security Service Edge (SSE) Adoption Report (Cyber Security Insiders, Axis)

Vorteile von Cisco Secure Access

- Optimiertes Benutzererlebnis durch Minimierung der manuellen Schritte für den Schutz aller Aktivitäten
- Sicherer Schutz aller privaten nicht-standardmäßigen und individuell angepassten Anwendungen
- Verbesserte Wirksamkeit der Sicherheit mit branchenführender Threat-Intelligence von Cisco
- Unterstützt Zero Trust mit präziser Kontrolle basierend auf BenutzerIn, Gerät, Standort und Anwendung
- Vereinfachtes Management und leichtere Bedienung durch eine einheitliche Administrationskonsole

Konvergente Sicherheit bei Cisco



Core	Extended	
FWaaS: Firewall-as-a-Service	**DNS:** Domain Name Server	**XDR:** Extended Detection and Response
CASB: Cloud Access Security Broker	**DLP:** Data Loss Prevention	**DEM:** Digital Experience Monitoring
ZTNA: Zero Trust Network Access	**RBI:** Remote Browser Isolation	**CSPM:** Cloud Security Posture Management
SWG: Secure Web Gateway	**Talos:** Threat Intelligence	

So bringt Cisco Secure Access Ihre Sicherheitsstrategie auf das nächste Level

Vielfältige Vorteile von Cisco Secure Access

- Schutz von Anwendungen, Ressourcen und BenutzerInnen – selbst Subunternehmer und Lieferanten – im Netzwerk und darüber hinaus
- Schnellere Erkennung, Untersuchung und Eindämmung
- Vereinfachte Prozesse durch die Konsolidierung von Sicherheitsfunktionen in einem Cloud-basierten Tool
- Verbessertes Benutzererlebnis steigert die Produktivität
- Optimierte Bereitstellung und Verwaltung dank einheitlicher Konsole
- Durchsetzung von Zero Trust mit umfassender Zugriffskontrolle

Konvergente Sicherheit von Cisco senkt das Risiko und erhöht die Vorteile

Verbesserte Sicherheit

Das Risiko wird über alle Bedrohungsszenarien hinweg reduziert und die Angriffsfläche deutlich verkleinert. Schädliche Aktivitäten werden effizient erkannt und blockiert und Vorfälle schnell behoben, um Business Continuity zu gewährleisten.

30 % höhere Wirksamkeit der Sicherheit

1 Mio. $ weniger Kosten im Zusammenhang mit Sicherheitsverletzungen (über ~3 Jahre)

Quelle: Forrester Total Economic Impact (TEI)-Studie für Cisco Umbrella SIG/SSE, 2022

Kosten-Nutzen-Verhältnis

NetOps- und SecOps-Teams profitieren von konvergenter Sicherheit dank einer einheitlichen Cloud-Plattform, welche das Benutzererlebnis in Ihrem gesamten Unternehmen verbessert und schützt.

231 % 3-Jahres-ROI

2 Mio. $ Nettonutzen, 3-Jahres-NPV

<12 Monate Amortisierung

Quelle: Forrester Total Economic Impact (TEI)-Studie, für Cisco Umbrella SIG/SSE, 2022

Sie suchen nach einer SSE-Lösung oder einer einheitlichen SASE-Lösung? Mit Cisco kommen Sie schneller an Ihre Sicherheitsziele.

Mehr Infos

Cisco Secure Access: konvergente, Cloud-native Security-Services

Cisco+ Secure Connect: einheitliche, sofort einsatzfähige, Cloud-Managed SASE-Lösung

cisco The bridge to possible