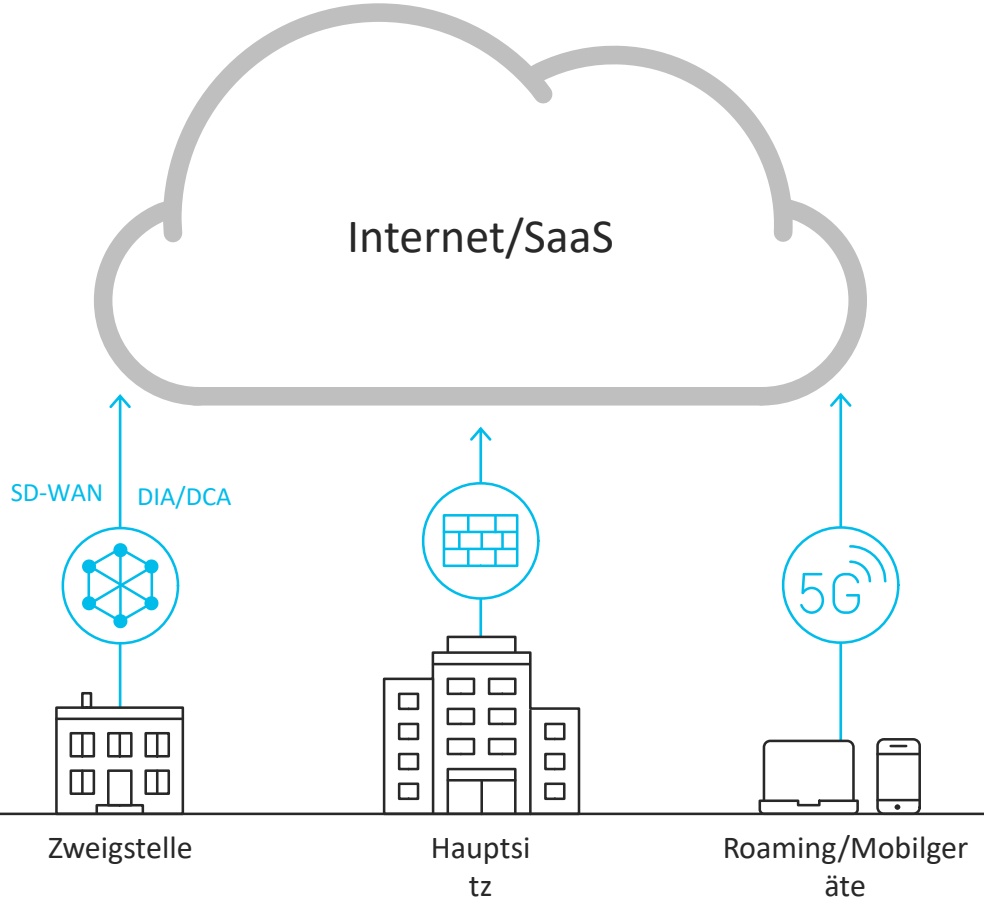
Cisco‘s Secure Internet Gateway (SIG)

Thomas Bier & Tim Christensen
Cloud Security Spezialist / Systems Engineer
it-sa 2019

Aktuelles Modell

Netzwerk:
dezentralisiert

Sicherheit:
Sicherheitsvorkehrungen im Rechenzentrum, in der Cloud und in den Zweigstellen (Edge)



Herausforderungen

Malware und Ransomware

Lückenhafte Transparenz und Abdeckung

Anzahl und Komplexität der Sicherheitstools

Begrenzte Sicherheits-ressourcen

Umstellung auf ein Secure Internet Gateway

- DNS-Layer-Sicherheit
- Web-Gateway
- Firewall
- DLP / CASB

Konsolidierung lokaler Sicherheitsvorkehrungen in der Cloud für einen effektiveren Schutz

Cisco Umbrella

Secure Internet Gateway

Sicheres Tor zum Internet, von jedem Standort aus

Transparenz

Im Unternehmensnetzwerk und außerhalb

Sämtlicher Datenverkehr (Internet/Web)

Alle Apps

Alle Geräte

Schutz

DNS-Layer-Sicherheit

Webprüfung

Dateiprüfung

Zugang zu Threat-Intelligence

Kontrolle

Listen mit blockierten/erlaubten URLs

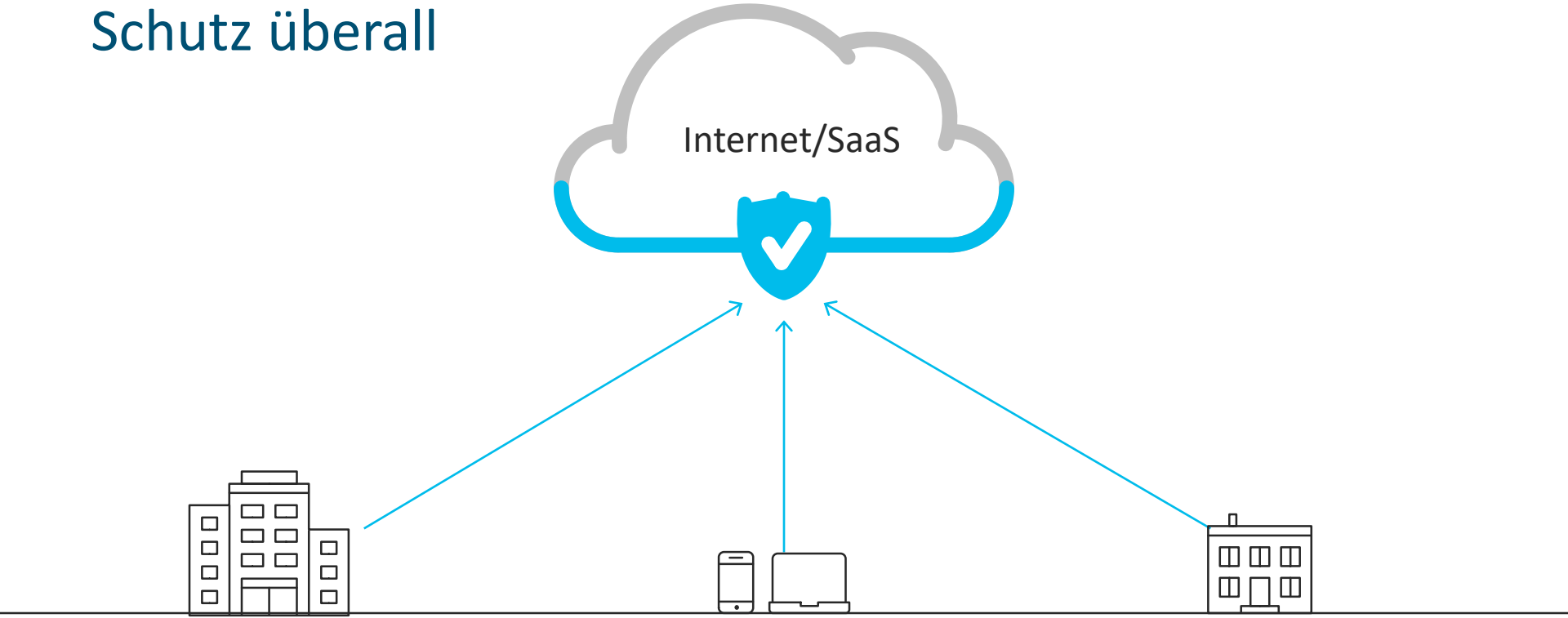
Port- und Protokollregeln

Inhaltsfilterung

App-Kontrolle

Basierend auf Threat-Intelligence von Cisco Talos

Schutz überall



Hauptsitz

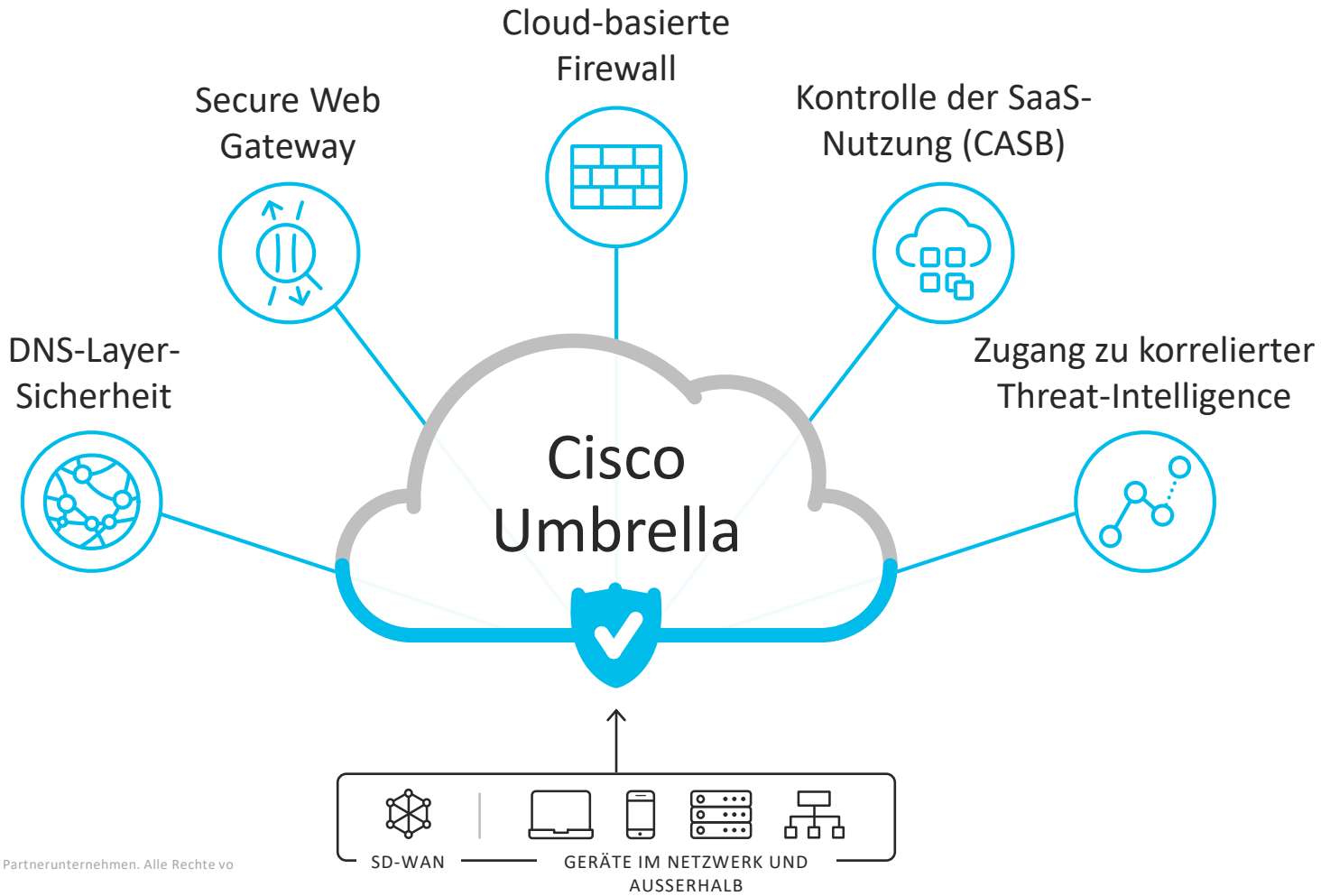
Stärkung der besehenden Sicherheitsinfrastruktur

Roaming/Mobilgeräte

Schutz außerhalb des Firmennetzwerks

DIA/DCA in Zweigstelle

Transformation der Edge-Sicherheit



DNS-Layer-Sicherheit

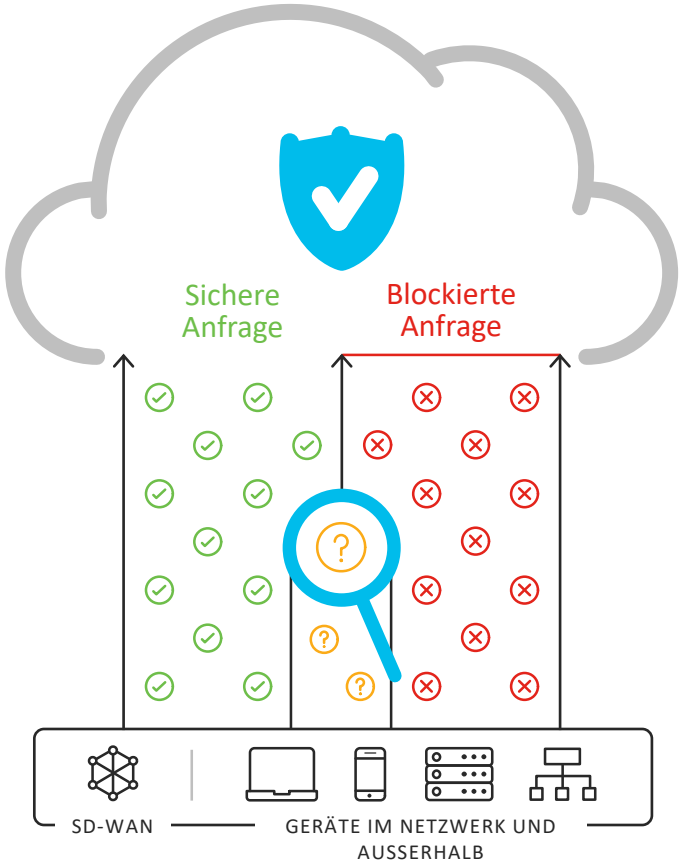
Erste Verteidigungslinie

Unternehmensweite Bereitstellung innerhalb von Minuten

Ortsunabhängige Blockierung von Malware, Phishing oder Command-and-Control-Callbacks

Frühestmögliche Abwehr von Bedrohungen und Eindämmung von Malware im Fall eines erfolgreichen Angriffs

Beeindruckendes Benutzererlebnis: schnellerer Internetzugriff, Proxyverbindungen nur für Zugriffe auf riskante Domänen



Secure Web Gateway: Webproxy

Gründliche Prüfung und Kontrolle von Web-Datenverkehr

Erfassung des gesamten Web-Datenverkehrs, einschließlich Protokollierung vollständiger URLs und URL-Blockierung

Durchsetzung von Richtlinien zur zulässigen Nutzung mittels Inhaltsfilterung und URL-Blockierung

Blockierung von mehr Malware dank SSL-Entschlüsselung und Dateiprüfung

Einführung weiterer Funktionen in zukünftigen Entwicklungsphasen

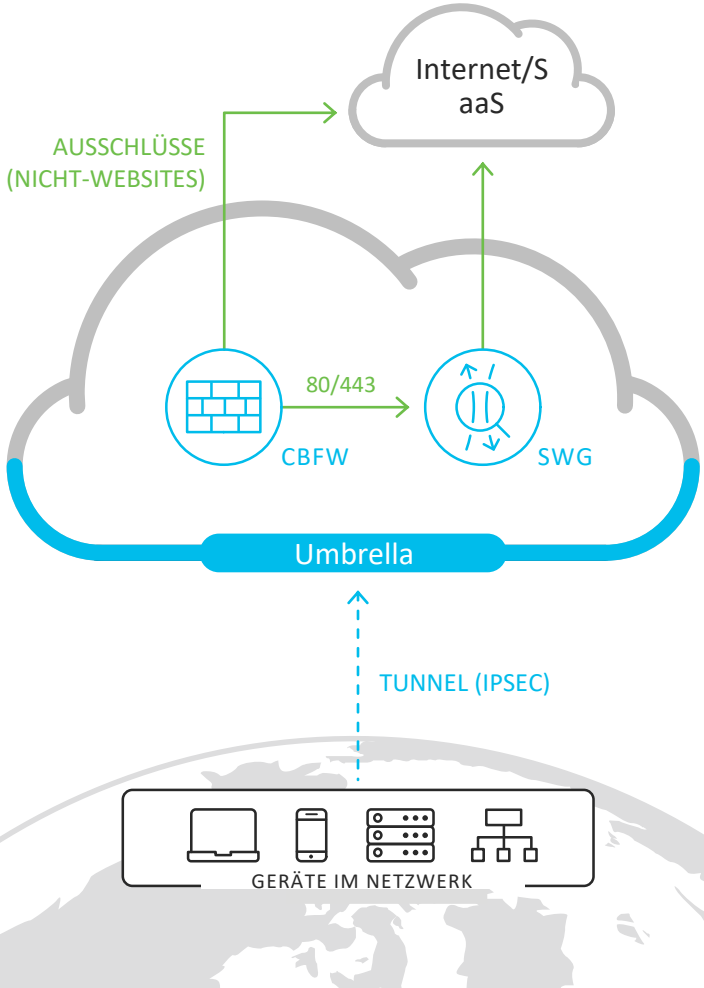
Cloud-basierte Firewall

Firewall für den Cloud-Edge

Tunneln des gesamten ausgehenden Datenverkehrs zu Umbrella

Zentrales Management von IP-Regeln, Portregeln und Protokollregeln (L3/L4)

IP-Anonymisierung zur Trennung von Gast- und Mitarbeiterdatenverkehr, zwecks Vermeidung negativer Auswirkungen auf das Sicherheitsrating (z. B. BitSight)



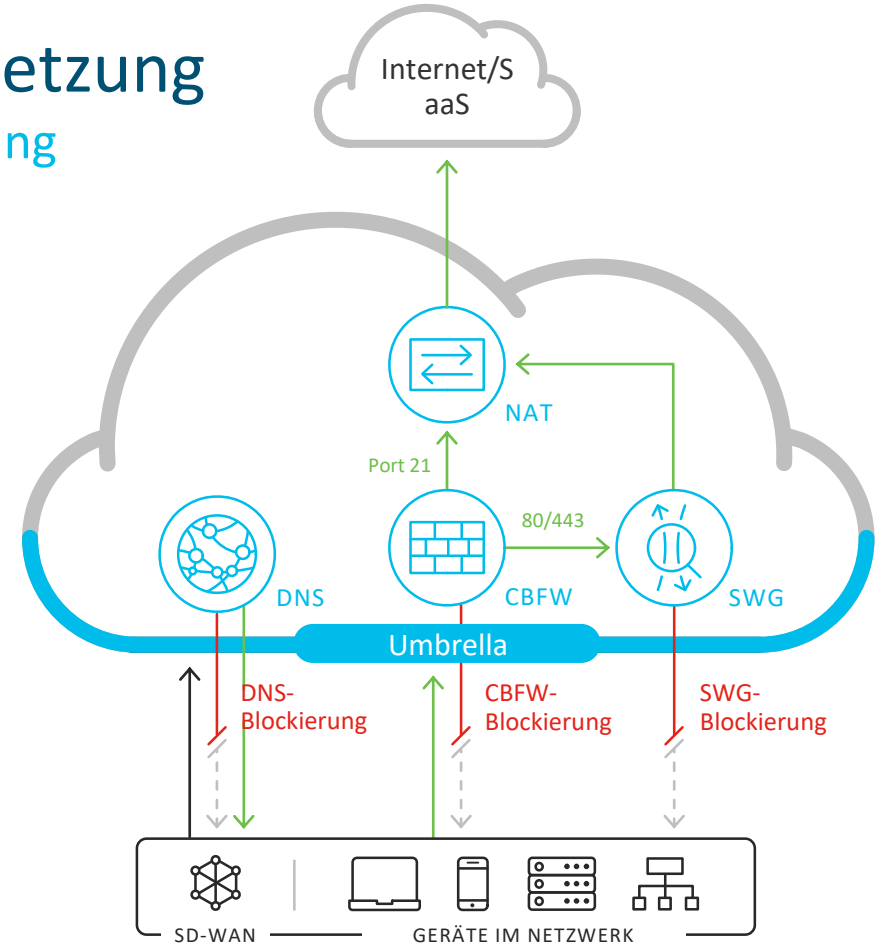
Ineinandergreifende Durchsetzung

Schnellere Reaktion und bessere Leistung

DNS-Layer-Sicherheit: erste Prüfung auf für Malware bekannte Domänen

Cloud-basierte Firewall (CBFW): nächste Prüfung auf Einhaltung von IP-Regeln, Portregeln und Protokollregeln

Secure Web Gateway (SWG): abschließende Prüfung sämtlichen Web-Datenverkehrs auf Malware und Richtlinienverstöße



Unkomplizierte Blockierung nicht genehmigter Apps

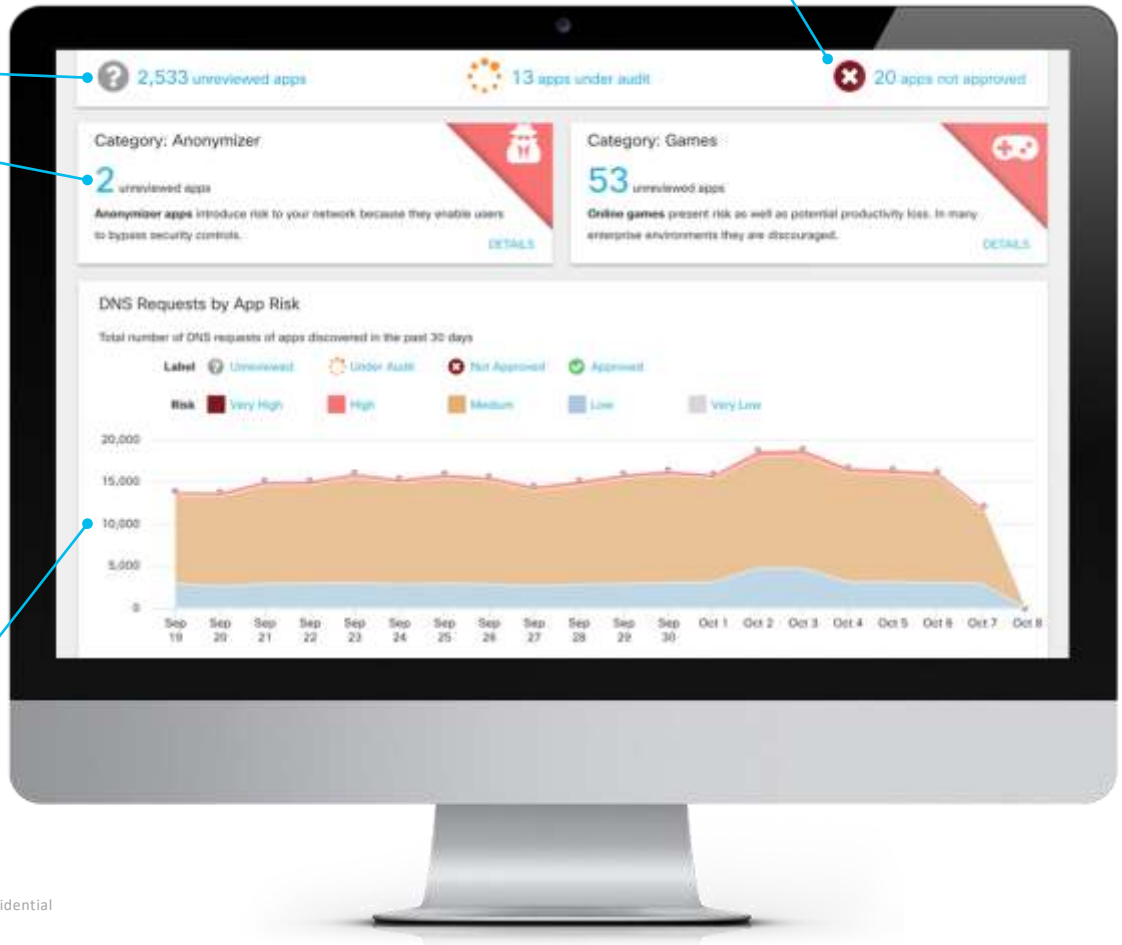
Status der entdeckten Anwendungen

Zusammenfassung für die riskantesten Kategorien

APP-ERKENNUNG UND APP-BLOCKIERUNG

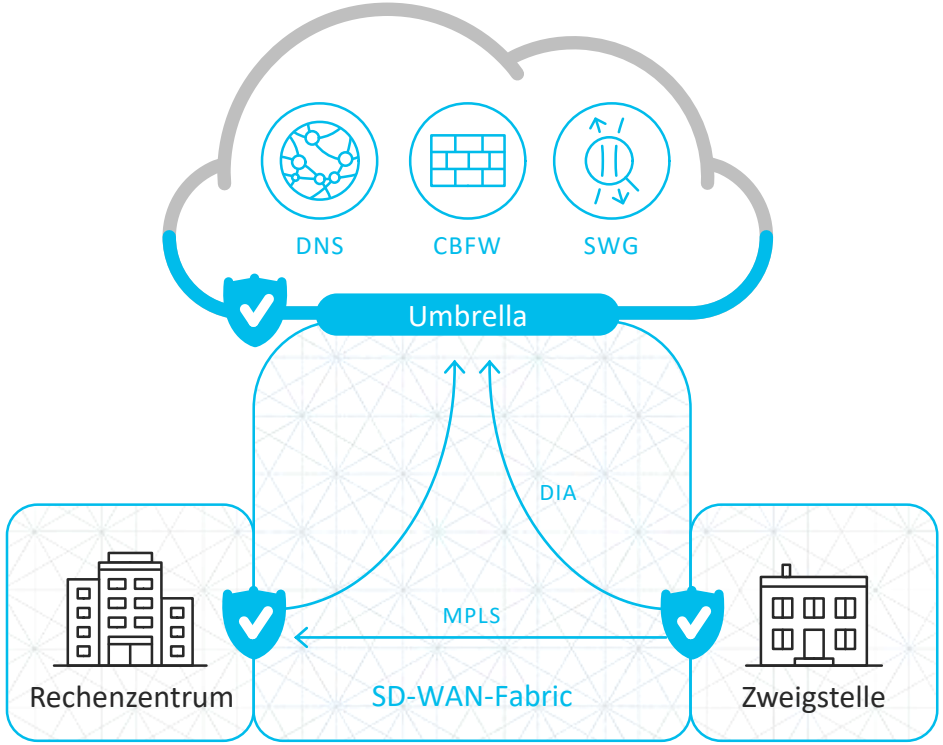
CASB-Funktion als Lösung für Schatten-IT und sichere Cloud-Implementierung

Transparenter Überblick über die Nutzung von Cloud-Apps nach Risiko, einschließlich Links zu App-Details



Integration mit Cisco SD-WAN

Einfacher, effektiver Schutz für Ihre gesamte Cisco SD-WAN-Fabric



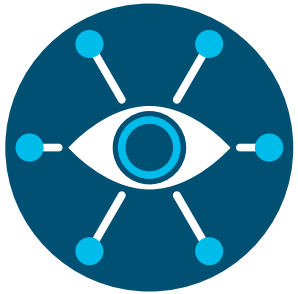
Schnelle Bereitstellung von DNS-Layer-Sicherheit als erste Verteidigungslinie

Umfassendere Prüf- und Kontrollmöglichkeiten über die Cloud-basierte Firewall und das Secure Web Gateway

Einfache Skalierung der Sicherheitslösung bei steigenden Volumina von SaaS- und Web-Datenverkehr

Cisco Talos: die größte nicht staatliche Threat-Intelligence-Organisation der Welt

Mehr als 250 Bedrohungsforscher und Data Scientists in Vollzeit



Analyse von 1,5 Mio. individuellen Malwarestichproben pro Tag

Blockierung von 20 Mrd. Bedrohungen täglich, also 20-mal mehr als jeder andere Anbieter

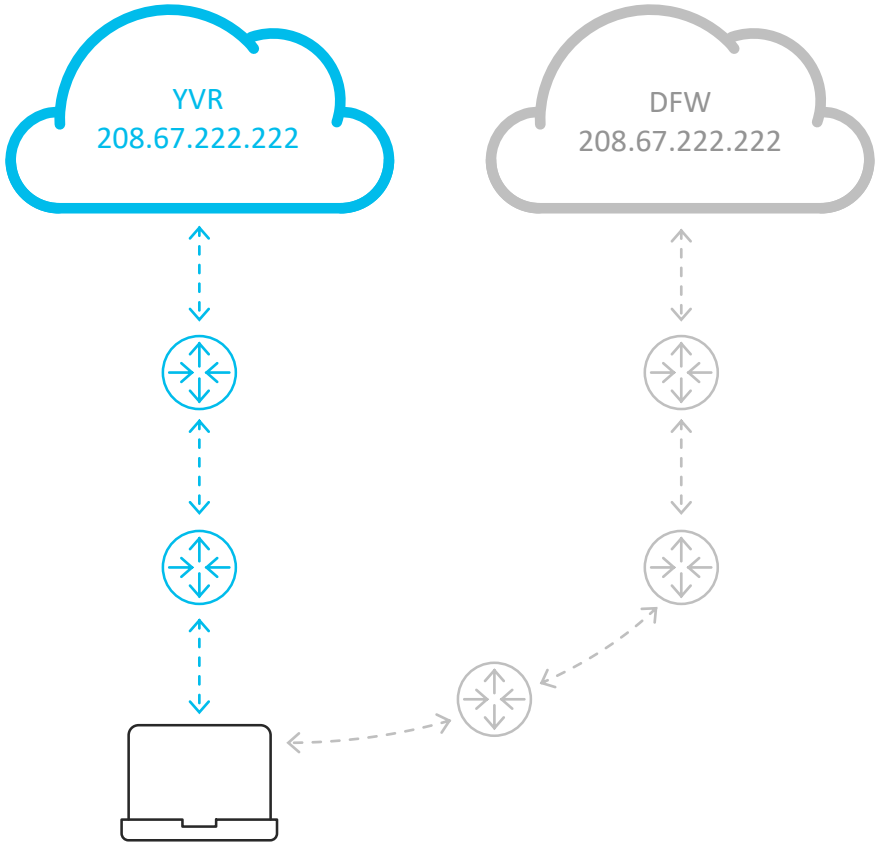
Wir **sehen mehr** , so dass Sie **mehr blockieren** und auf Bedrohungen **schneller reagieren** können.

Anycast-IP-Routing für Zuverlässigkeit

Alle Rechenzentren senden die gleiche IP-Adresse.

Die Kunden verweisen DNS-Datenverkehr an unsere IP-Adresse.

Anfragen werden per automatisiertem Failover transparent an das am schnellsten verfügbare Rechenzentrum gesendet.




CISCO