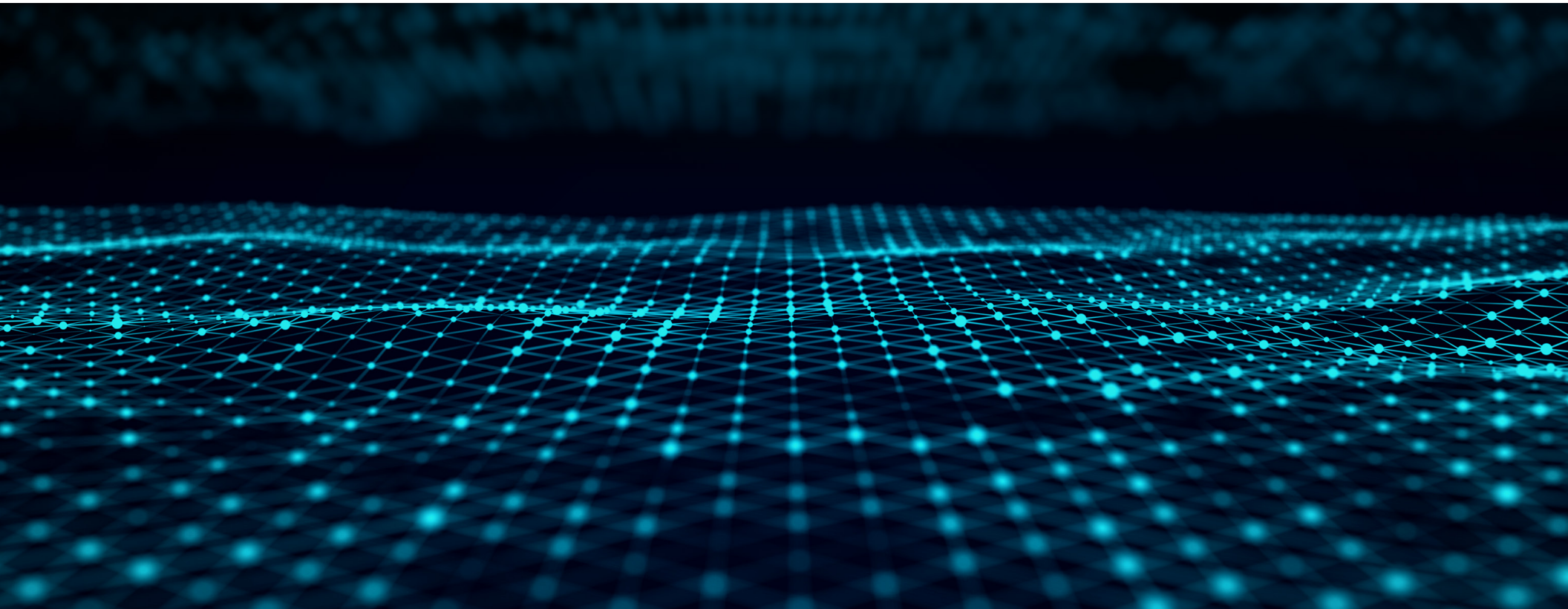
Cisco Hybrid Mesh Firewall auf einen Blick

Eine zukunftsweisende Sicherheitsarchitektur



IT-Umgebungen in Unternehmen sind heute stark verteilt und dadurch äußerst komplex.

Die Verbreitung von Anwendungen, die wachsende Nutzung von KI-Technologien und eine zunehmend mobile Belegschaft vergrößern die Angriffsfläche zusätzlich. Unternehmen müssen in der Lage sein, wichtige Traffic-Grenzen zu sichern, geschäftliche und KI-gestützte Anwendungen zu schützen und sicherzustellen, dass User und Geräte nur auf ausdrücklich zulässige Ressourcen zugreifen können.

Radikale Veränderungen erfordern radikales Denken. Deshalb denken wir Sicherheit neu, damit sie in jeder Umgebung und im Hyperscale funktioniert. Firewalls waren schon immer eine wichtige Grundlage für Unternehmenssicherheit und haben bis heute nicht an Bedeutung verloren. Cisco hebt die Leistungsfähigkeit von Firewalls auf ein völlig neues Niveau.

Die Hybrid Mesh Firewall-Lösung von Cisco ist eine hochgradig verteilte Sicherheits-Fabric, die dafür optimiert ist, komplexe Bedrohungen zu stoppen, Anwendungsschwachstellen zu sichern und Zero-Trust-Segmentierung über mehrere Umgebungen hinweg zu implementieren. Cisco bietet Ihnen ein einheitliches Cloud-Management, das Workflows optimiert und die Sicherheit verbessert. So können Sie Ihre Sicherheits-Fabric skalieren, ohne die vorhandene Infrastruktur komplett ersetzen zu müssen. Zur Steigerung der Produktivität können Sie jetzt KI-native Funktionen nutzen, um die Fehlerbehebung zu vereinfachen und die Leistung aller Ihrer Durchsetzungstools zu optimieren.

Unsere Hybrid Mesh Firewall ist einfach zu implementieren und schützt Ihre Investitionen mit flexibler Lizenzierung über die Cisco Cloud Protection Suite, sodass Sie bei Bedarf auf verschiedene Funktionen und Innovationen zugreifen können.

Vorteile

Vereinfachtes Sicherheitsmanagement: Greifen Sie auf alle Durchsetzungsfunktionen in Ihrer Hybrid-Umgebung zu und gewinnen Sie KI-basierte Einblicke über eine zentrale Schnittstelle.

Schutz vor modernen Bedrohungen: Sichern Sie Umgebungen an wichtigen Grenzen und schützen Sie sich gleichzeitig vor Zero-Day-Angriffen und Bedrohungen, die im verschlüsselten Datenverkehr verborgen sind.

Stoppen nicht autorisierter lateraler Bewegungen: Mit grober und fein abgestufter Segmentierung für herkömmliche und Kubernetes-Workloads können Sie die Angriffsfläche reduzieren und den Angriffsradius eindämmen.

Sichere KI-Transformation: Erkennen Sie dynamische Bedrohungen, die durch die Entwicklung und Bereitstellung von KI-Anwendungen entstehen, und schützen Sie sich davor.

Schließen Sie die Exploit-Lücke: Schützen Sie sich mit einer KI-nativen Regel-Engine, die Schwachstellen priorisiert und automatisch eine operative Eindämmung empfiehlt, in Minutenschnelle vor Exploits.

Cisco Hybrid Mesh Firewall-Komponenten

Hypershield:
KI-native verteilte Sicherheitsarchitektur für KI-Skalierung

Secure Firewall:
Branchenführende skalierbare Firewalls, die auch verschlüsselten Datenverkehr untersuchen

Secure Workload:
Erhalten Sie bessere Einblicke und wenden Sie Segmentierungsrichtlinien auf Anwendungen in hybriden Umgebungen mit oder ohne Agents an

Multicloud Defense:
Cloud-native Orchestrierung und Automatisierung vereinfacht die Bereitstellung, Vernetzung und Skalierung von Firewalls in der Public Cloud

AI Defense:
Schutzmaßnahmen für die Entwicklung und Bereitstellung von KI-Anwendungen

Isovalent Enterprise Platform:
Erkennung von Microservice-Interaktionen und Durchsetzung von Richtlinien in Kubernetes-Umgebungen

Security Cloud Control:
Zentrales Management aller Durchsetzungspunkte in der gesamten Sicherheits-Fabric

Was spricht für die Cisco Hybrid Mesh Firewall?

Hochgradig verteilte Sicherheits-Fabric mit einheitlichem Management von einem einzigen Anbieter

Cisco geht über die „Firewall in einer Box“ hinaus und vereinheitlicht die Sicherheit im Netzwerk, in der Cloud, im Container und in sämtlichen Workloads für eine hochgradig verteilte Fabric. Diese Lösung bietet Sicherheit genau dort, wo Sie sie benötigen, integriert Ihre vorhandenen Firewalls, ist skalierbar und bietet Richtlinienmanagement mit einem Skalierungsfaktor, den menschliche Anwender nicht leisten können. Verfügbar in Form einer flexiblen Lizenz, die sich mit Ihren Anforderungen und mit den Innovationen von Cisco weiterentwickelt.

Fünf Funktionen, durch die sich die Hybrid Mesh Firewall-Lösung von Cisco von anderen abhebt:

1. Intelligentes zentrales Management: Konfiguration, Bereitstellung und automatische Skalierung von Firewalls in Multicloud-Umgebungen ohne Skripting. Darüber hinaus reduziert der KI-Assistent den Managementaufwand und setzt Ressourcen und Fachwissen frei.
2. Advanced Threat Protection: Durch die branchenweit erste ML-basierte Encrypted Visibility Engine können Sie Bedrohungen in verschlüsseltem Traffic erkennen, ohne Abstriche bei der Leistung hinnehmen zu müssen. Wo eine Entschlüsselung unerlässlich ist, bietet die leistungsstarke Hardware-Offload-Architektur ein führendes Preis-Leistungs-Verhältnis und umfassende Transparenz. Mit Cisco Talos Threat Intelligence, branchenführendem Snort 3 IPS und Snort ML schützen Sie sich vor bekannten und unbekannten Bedrohungen.
3. Segmentierung: Verhindern Sie nicht autorisierte laterale Bewegungen und schützen Sie Anwendungen im gesamten Rechenzentrum und in den Clouds mit topologiesensitiver Sicherheit, die Anwendungsabhängigkeiten versteht und Zero-Trust-Segmentierungsrichtlinien in der gesamten Cisco Security-Fabric anwendet.
4. Schutz für KI-Modelle: Bindet KI-Leitfäden in die Netzwerk-Fabric ein, um in Echtzeit vor dynamischen Bedrohungen zu schützen, die durch die Entwicklung und die Bereitstellung von KI-Anwendungen entstehen.
5. Exploit-Schutz: Behebt Schwachstellen durch einen operativen Schutzschild, der im Anwendungspfad optimal platziert ist, um den Exploit zu blockieren – während gleichzeitig die Anwendungsverfügbarkeit gewährleistet ist.

Cisco Hybrid Mesh Firewall-Funktionen

Sicherheit, die sich schnell und flexibel mit dem Unternehmen entwickelt

- Sicherheits-Fabric aus Firewalls (physisch, virtuell und in der Cloud), Agents (herkömmliche und Kubernetes-Workloads) und Smart Switches, die Sicherheit fest in die Netzwerk-Fabric integrieren
- Bietet durch Einbindung in die Fabric von physischen, virtuellen, Cloud-, Container- und IoT-Umgebungen Sicherheit überall dort, wo sie benötigt wird
- Cloud-natives Firewalling ermöglicht einfache Vernetzung, automatische Skalierung und Self-Healing von Durchsetzungspunkten in Public-Cloud-Umgebungen
- Identifizieren und blockieren Sie Bedrohungen, die im verschlüsselten Datenverkehr verborgen sind, mit der Encrypted Visibility Engine
- Stoppen Sie bekannte und Zero-Day-Bedrohungen mit Snort 3 IPS, Snort ML und kontinuierlichen Threat-Intelligence-Updates von Cisco Talos
- Segmentieren Sie jede Anwendung in jeder Umgebung mit konsistenten Zero-Trust-Richtlinien mit einer Sicherheitsarchitektur, die moderne Rechenzentren im KI-Maßstab schützt
- Schutz von KI-Modellen in Echtzeit, um KI-gesteuerte Anwendungen vor Missbrauch, Datensicherheitsverletzungen, Denial-of-Service und komplexen Angriffen wie Prompt Injections zu schützen
- Schützen Sie sich vor Exploits mit einer KI-nativen Regel-Engine, die Schwachstellen priorisiert und automatisch eine präzise Eindämmung empfiehlt
- Die native Integration in die Cisco Identity Services Engine (ISE) ermöglicht eine einfache Segmentierung von IoT-Geräten durch die Nutzung von Sicherheitsgruppen-Tags
- Integration in Cisco Universal ZTNA zur Bereitstellung einer ganzheitlichen Zero-Trust-Plattform für das gesamte hybride Unternehmen

Reduzieren Sie mit intelligentem, zentralem Management die Komplexität bei jeder Skalierung

- Cloud-basiertes Management über mehrere Domänen hinweg, einschließlich Management aller Durchsetzungspunkte über eine zentrale Schnittstelle, Objektfreigabe in der gesamten Fabric, rollenbasierte Zugriffskontrolle (RBAC), Lizenzmanagement, AIOps und Richtlinien-Lifecycle-Management
- Cloud-Richtlinienmanagement über die Cisco Infrastruktur und Firewalls von Drittanbietern hinweg sowie Durchsetzung von Cisco Universal ZTNA-Richtlinien für jeden Benutzerzugriff, ob vor Ort oder remote
- Native Konfiguration, Bereitstellung und automatische Skalierung von Cloud-Firewalls in Multicloud-Umgebungen
- AI Assistant bietet einheitliche Einblicke in das Sicherheits-Mesh für Richtlinienkonfiguration, Fehlerbehebung und Optimierung
- AI Assistant kann Firewall-Regeln in der Umgebung schreiben, bereitstellen und optimieren und bietet Empfehlungen für gängige Aufgaben

Schützt Ihr Unternehmen

Erhöhen Sie die Widerstandsfähigkeit und vermeiden Sie Ausfallzeiten mit den richtigen Sicherheitskontrollen und den optimalen Durchsetzungspunkten.

Schützt Ihr Team

Steigern Sie mit dem zentralen Management von Security-Tools in der gesamten Fabric die Effizienz Ihres Teams drastisch und setzen Sie Ressourcen frei – mit einem autonomen, selbstlernenden System, das Ihr Vertrauen verdient.

Schützt Ihre Investitionen

Die Cloud Protection Suite ist Ihr Weg zur Hybrid Mesh Firewall. Sie vereint Einfachheit und Flexibilität, damit Sie Ihre Ziele leichter erreichen und Lösungsinnovationen in Ihrem eigenen Tempo nutzen können, wenn Ihr Unternehmen skaliert.

Weitere Informationen

Weitere Informationen zu Produkten und Services rund um die Cisco Hybrid Mesh Firewall finden Sie unter www.cisco.com/go/hybridmeshfirewall.

Um Kaufoptionen anzuzeigen und mit einem Cisco Vertriebsmitarbeiter zu sprechen, besuchen Sie www.cisco.com/site/us/en/buy/index.html.