Cisco Security Cloud: entwickelt für eine hybride Multicloud-Welt

Cisco Security Cloud ist eine offene, integrierte und vereinheitlichte Plattform für End-to-End-Sicherheit in hybriden Multicloud-Umgebungen, die für eine optimierte Performance und ein wirksameres Sicherheitskonzept sorgt. Sie bietet alle Funktionen, die für die sichere ortsunabhängige Vernetzung von Personen und Geräten mit Anwendungen und Daten sowie eine skalierbare Bedrohungsabwehr, Erkennung, Reaktion und Behebung erforderlich sind.

Cisco Security Cloud bietet umfassende, integrierte Sicherheits- und Netzwerkservices, die Ihnen die Wirtschaftlichkeit der Public Cloud ohne die Bindung an einen bestimmten Anbieter ermöglicht. So können Sie Ihr gesamtes IT-Ecosystem schützen und gleichzeitig das Endbenutzererlebnis vereinfachen.

Vorteile

- Vereinfachen Sie Ihr Sicherheitskonzept und Ihre Netzwerke mit einer Cloud-nativen Plattform, die BenutzerInnen, Geräte und IoT sicher mit den Systemen, Anwendungen und Daten Ihres Unternehmens verbindet – und das über mehrere Clouds und Netzwerke hinweg.
- Reduzieren Sie Reibungspunkte, indem Sie Ihre Sicherheitsvorkehrungen näher an Ihren BenutzerInnen und ihren jeweiligen Daten und Anwendungen ansiedeln und die Maßnahmen vereinfachen.
- Steigern Sie die Effizienz durch die Vereinheitlichung von Richtlinien, Management, Produktkonsolen und Dashboards, damit die Sicherheit von Anfang bis Ende nahtlos gegeben ist.
- Arbeiten Sie flexibel und skalierbar ohne Anbieterbindung. Nutzen Sie APIs für die Integration und ein robustes Entwicklungs-Ecosystem, damit sich Ihre Umgebung mit Ihrem Unternehmen weiterentwickeln kann.
- Verbessern Sie die Transparenz und den Schutz vor Bedrohungen durch aussagekräftige Einblicke in Netzwerke, Clouds, Endpunkte und Anwendungen, um SecOps-Teams bei der Suche, Untersuchung und Beseitigung von Bedrohungen zu unterstützen.

© 2022 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten.

Optimieren Sie die Performance und Sicherheit Ihres gesamten Netzwerks

Cisco Security Cloud unterscheidet sich von jeder anderen Sicherheitsplattform oder Punktlösung. Die umfassenden, integrierten Sicherheits- und Netzwerkservices von Cisco folgen einem Cloud-First-Ansatz, der Ihr gesamtes IT-Ecosystem schützt – in der Cloud, vor Ort oder in einer Kombination aus beidem.

- Einfache Skalierbarkeit: Dank der flexiblen Architektur von Cisco Security Cloud lässt sich die Plattform nach oben, unten oder nach außen skalieren, um den sich ändernden Workloads und Arbeitsaufkommen Ihres Unternehmens gerecht zu werden.
- Sicherheit in Ihrem gesamten Ecosystem: Eine offene, erweiterbare API ermöglicht die Integration von Drittanbieterlösungen und unterstützt dadurch den Aufbau eines Entwicklungs-Ecosystem.
- Zentrale Bereitstellung von Transparenz, Monitoring und Berichterstellung: Dank des einheitlichen Managements können Richtlinien an einem Ort festgelegt und auf allen Netzwerken, Endpunkten und Systemen repliziert werden – selbst auf denen von Drittanbietern.
- Richtlinienprozesse neu gedacht: Unsere KI-basierte Engine für vereinheitlichte Richtlinien verfolgt einen Intent-Based-Ansatz und unterstützt Sie mit einer verbesserten und automatisierten Richtlinienerstellung.
- Unterstützung echter Multicloud-Umgebungen: Security Cloud schützt Daten in allen wichtigen Public Clouds wie Microsoft, Google oder Amazon und bietet nicht nur für BenutzerInnen und herkömmliche Geräte, sondern auch für Datenströme von IoT-Endpunkten sichere Verbindungen.

© 2022 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten.

So setzt ISE Zero Trust durch

Wir verbinden vertrauenswürdige BenutzerInnen und Endpunkte mit vertrauenswürdigen Ressourcen.

Zugriffsanfrage auf Endpunkt

- Endpunkt wird identifiziert und Vertrauen hergestellt
- Status des Endpunkts wird zur Erfüllung der Compliance-Anforderungen überprüft

Vertrauen wird kontinuierlich überprüft

- Kontinuierliches Monitoring und Überprüfung der Endpunkt-Vertrauensstufe
- Schwachstellenanalysen zur Identifizierung von Identificators of Compromise
- Automatische Aktualisierung der Zugriffsrichtlinie

Endpunkte werden klassifiziert und in Gruppen eingeteilt

- Endpunkte werden mit „w/SGTs“ gekennzeichnet
- Richtlinie wird gemäß des Least-Privilege-Prinzips auf Gruppen angewendet

Autorisierter Endpunktzugriff basierend auf dem Least-Privilege-Prinzip

- Zugriff gewährt
- Netzwerksegmentierung erfolgreich

© 2022 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten.

„Sie sind am anfälligsten, wenn Sie isolierte Technologien haben. Diese Plattform vereint Transparenz und bezieht DevOps, SecOps und sogar die Infrastruktur in das Konzept mit ein.“

– Collin John,
Global Security Manager

Mehr erfahren Sie unserem E-Book:
Cisco Security Cloud

© 2022 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Cisco und das Cisco Logo sind Marken oder eingetragene Marken von Cisco und/oder Partnerunternehmen in den Vereinigten Staaten und anderen Ländern. Eine Liste der Marken von Cisco finden Sie unter: www.cisco.com/go/trademarks. Die genannten Marken anderer Anbieter sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. PROJ982354428 11/22

Das Besondere an Cisco

Funktionen	Details
Reputation	Wir bei Cisco sind für unsere Netzwerk- und Sicherheitsangebote weltweit bekannt. Diese globale Präsenz gibt uns Einblicke in unübertroffene Mengen an Telemetriedaten.
Skalierung	Keine Umgebung ist zu groß oder zu klein. Wir schützen bereits 840.000 Netzwerke, 67 Millionen Postfächer und 87 Millionen Endpunkte.
Architektur	Dank unserer offenen APIs und unserer einheitlichen Multicloud-Architektur gehören isolierte Technologien der Vergangenheit an. Stattdessen erhalten Sie die volle Kontrolle über Ihre gesamte Umgebung.
Innovation	Hochwertige, skalierbare Telemetrie, Intent-Based-Richtliniendefinition, KI-gesteuerte Automatisierung, Cisco Talos Threat-Intelligence und Reaktion, einzigartige hybride Arbeitslösungen und vieles mehr.