Cisco Secure Firewall für Finanzinstitute

Inhalte

Integration von Netzwerk und Sicherheit

Sicherheitskontrollen der Spitzenklasse

Einheitliche Richtlinien und Transparenz

Ihr gesamtes Netzwerk als Erweiterung Ihrer Sicherheitsarchitektur

Die Bereitstellung Ihrer geschäftskritischen Anwendungen erfolgt zunehmend über Hybrid- und Multicloud-Umgebungen, außerdem müssen MitarbeiterInnen inzwischen von überall aus auf sichere Weise auf Ressourcen zugreifen können. Dem kann das klassische Konzept der Firewall jedoch nicht mehr gerecht werden. Denn wo es in der Vergangenheit nur einen einzelnen Netzwerkperimeter gab, steht heute eine Vielzahl von Mikro-perimetern. So bildet für viele Finanzinstitute nun die Anwendung den neuen Perimeter. In diesem Zuge sind herkömmliche Firewall-Bereitstellungen mittlerweile einer Kombination aus physischen, virtuellen und Cloud-nativen Appliances gewichen. Infolgedessen haben Unternehmen Schwierigkeiten, den Support für moderne Anwendungsumgebungen zu operationalisieren. Die Herausforderung besteht darin, konsistente Transparenz, Richtliniendurchsetzung und einheitliche Bedrohungstransparenz aufrechtzuerhalten, ohne dass Schwachstellen entstehen, die das Unternehmen einem Risiko aussetzen.

Cisco adressiert dies mit NetWORK, seiner Vision für starke Netzwerksicherheit, die für agilere, stärker auto-matisierte und integrierte Konzepte zur Harmonisierung und konsequenten Durchsetzung von Richtlinien für moderne dynamische Anwendungen in den zunehmend heterogenen Netzwerken von heute steht. Hierzu bietet Cisco Secure Firewall Integrationen zwischen zentralen Netzwerkoperationen und Security-Funktionen in einer Tiefe, die eine Architektur von bislang unerreichter Sicherheit schaffen. Das Ergebnis ist ein umfassendes Security-Portfolio, das Ihre Anwendungen und BenutzerInnen jederzeit und überall schützt.

Vorteile

- Profitieren Sie von einheitlicher Workload- und Netzwerksicherheit in Echtzeit für integrierte Kontrolle in dynamischen Anwendungsumgebungen.
- Unser plattformbasierter Ansatz für Netzwerksicherheit sowie die Nutzung und der Austausch von Intelligence aus wichtigen Quellen sorgt für eine schnellere Erkennung, Reaktion und Problembehebung. Schützen Sie Remote-MitarbeiterInnen mit hochgradig sicherem Unternehmenszugriff jederzeit, überall und von jedem Gerät aus und profitieren Sie dabei von leistungsstarken Funktionen zur Bedrohungs-abwehr, die das Unternehmen, BenutzerInnen und kritische Anwendungen umfassend schützen.
- Die SecureX™-Berechtigung ist in jeder Cisco® Secure Firewall enthalten und sorgt für einen eng integrierten Sicherheitsansatz, der die Korrelation von Bedrohungen im gesamten Cisco Secure-Portfolio ermöglicht und die Incident Response beschleunigt.

Hervorragende Transparenz und Kontrolle

Auf der einen Seite stehen immer raffiniertere Bedrohungen, auf der anderen zunehmend komplexe Netzwerke. Doch welches Finanzinstitut verfügt schon über die Ressourcen, die nötig wären, um diese hochdynamischen Bedrohungen laufend im Auge behalten und erfolgreich abwehren zu können?

Angesichts der zunehmenden Komplexität von Bedrohungen und Netzwerken ist es unerlässlich, dass Sie die richtigen Tools zum Schutz Ihrer Daten, Anwendungen und Netzwerke an der Hand haben. Cisco Secure Firewalls bieten die Leistung und Flexibilität, die Sie benötigen, um Bedrohungen einen Schritt voraus zu bleiben. Gegenüber der vorherigen Appliance-Generation bieten sie eine um das Dreifache höhere Leistung. Durch herausragende hardwarebasierte Funktionen ermöglichen sie zudem Untersuchungen von verschlüsseltem Datenverkehr in großem Maßstab. Für BenutzerInnen lesbare Regeln von Snort 3 IPS vereinfachen die Security. Dynamische Anwendungstransparenz und -kontrolle werden über die Cisco Secure Workload-Integration umgesetzt, die konsistenten Schutz für die modernen Anwendungen von heute über das gesamte Netzwerk sowie sämtliche Workloads hinweg gewährleistet.

Finden Sie die ideale Firewall für Ihr Unternehmen

Unkompliziertes, konsistentes Richtlinienmanagement

Mit dem Cisco Secure Firewall-Portfolio stärken Sie Ihren Sicherheitsstatus und profitieren von zukunftssicherem, flexiblem Management. Cisco bietet eine Vielzahl von Managementoptionen, die auf Ihre Geschäftsanforderungen zugeschnitten sind.

- **Cisco Secure Firewall Device Manager:** On-Device-Management-Lösung für Firewall Threat Defense, die eine einzelne Firewall lokal managt.
- **Cisco Secure Firewall Management Center:** managt eine umfangreiche Firewall-Bereitstellung. Verfügbar in allen Formfaktoren, wie On-Premises, Private Cloud, Public Cloud und Software-as-a-Service (SaaS).
- **Cisco Defense Orchestrator:** ein Cloud-basierter Manager, der Sicherheitsrichtlinien und das Gerätemanagement für mehrere Cisco Produkte wie Cisco Secure Firewall, Meraki® MX und Cisco IOS®-Geräte optimiert.

Für skalierbares Protokollmanagement steht außerdem Cisco Security Analytics and Logging zur Verfügung. Die Lösung verbessert die Erkennung von Bedrohungen und erfüllt Compliance-Anforderungen im gesamten Unternehmen mit Funktionen für längere Aufbewahrung und Verhaltensanalyse.

Erfolgsgeschichte der Lake Trust Credit Union

Warum Cisco?

Die Bedrohungen für Ihr Netzwerk nehmen ständig zu und werden immer komplexer. Mit dem Cisco Secure Firewall-Portfolio sind Sie dagegen bestens gewappnet, denn bei Cisco bauen Sie Security auf einem Fundament auf, das Ihren Sicherheitsstatus durch Agilität und Integration sowohl heute als auch in der Zukunft zu maximaler Stärke verhilft.

Ganz gleich, ob im Rechenzentrum, in Zweigstellen oder der Unternehmensniederlassung, ob in Cloud-Umgebungen oder überall dazwischen: Die Funktionsstärke von Cisco macht Ihre Netzwerkinfrastruktur an jedem Punkt zur Verlängerung ihrer Firewall-Lösung – für erstklassige Sicherheitskontrollen genau dort, wo Sie sie benötigen.

Mit einer Cisco Secure Firewall-Appliance investieren Sie in den Schutz vor komplexesten Bedrohungen, ohne bei der Untersuchung von verschlüsseltem Datenverkehr Performance-Abstriche hinnehmen zu müssen. Außerdem bieten Ihnen Integrationen mit weiteren Cisco Lösungen und Lösungen von Drittanbietern ein umfassendes Portfolio an Security-Produkten, die im Verbund zusammenarbeiten, um bislang voneinander isolierte Ereignisse zu korrelieren, irrelevante Warnungen zu minimieren und Bedrohungen schneller aufzuhalten.

Die leistungsstarken Funktionen von Cisco Secure Firewall im Überblick

Leistungsstarke Funktionen	Details
Integration mit Cisco Secure Workload	• Die Integration mit Cisco Secure Workload (ehemals Tetration) ermöglicht umfassende Transparenz und Richtliniendurchsetzung für moderne verteilte und dynamische Anwendungen über das gesamte Netzwerk sowie sämtliche Workloads hinweg. Dies sorgt für eine ebenso konsistente wie skalierbare Durchsetzung.
Cisco Secure Firewall Cloud Native	• Die mit Kubernetes entwickelte und erstmals in AWS verfügbare Cisco Secure Firewall Cloud Native ist eine entwicklerfreundliche Anwendungszugriffslösung für den Aufbau einer hochelastischen, Cloud-nativen Infrastruktur.
Dynamische Richtlinien-unterstützung	• Dynamische Attribute unterstützen VMware-, AWS- und Azure-Tags für Situationen, in denen statische IP-Adressen nicht verfügbar sind. • Cisco ist ein Pionier bei tagbasierten Richtlinien mit Security Group Tags (SGTs) und Cisco Identity Services Engine(ISE)-Attributunterstützung.
Snort 3 Intrusion Prevention System	• Snort 3 ist das branchenführende Open-Source-Bedrohungsabwehrsystem und verbessert die Erkennung von Bedrohungen, vereinfacht die Anpassungsmöglichkeiten und steigert die Performance.
Transport Layer Security(TLS)-Serveridentität und -erkennung	• Ermöglicht die Aufrechterhaltung von Layer-7-Richtlinien für verschlüsselten TLS-1.3-Datenverkehr. Sorgen Sie für Transparenz und Kontrolle in einer verschlüsselten Welt, in der nicht jeder Datenverkehrsfluss entschlüsselt und überprüft werden kann. Konkurrierende Firewalls verstoßen gegen Ihre Layer-7-Richtlinien mit verschlüsseltem TLS-1.3-Datenverkehr.
Cisco Secure Firewall Management Center	• Ermöglicht umfassendes Management von der Firewall über die Anwendungskontrolle bis hin zu Intrusion-Prevention, URL-Filterung und Richtlinien zur Verteidigung gegen Malware. • Die Integration mit Cisco Secure Workload (ehemals Tetration) ermöglicht konsistente Transparenz und Richtliniendurchsetzung für dynamische Anwendungen über das gesamte Netzwerk sowie sämtliche Workloads hinweg.
Cisco Defense Orchestrator	• Cloud-basiertes Firewall-Management zur konsistenten und einfachen Verwaltung von Richtlinien in Ihren Cisco Secure Firewalls.
Cisco Security Analytics and Logging	• Hochgradig skalierbares On-Premises- und Cloud-basiertes Firewall-Protokollmanagement mit Verhaltensanalysen zur Echtzeit-Bedrohungserkennung – für schnellere Reaktionszeiten. Hinzu kommen kontinuierliche Analysen, um Ihren Sicherheitsstatus weiterzuentwickeln und zukünftige Angriffe besser abzuwehren. • Erfüllen Sie Ihre Compliance-Anforderungen mit Protokollaggregation für alle Cisco Secure Firewalls. • Enge Integration in Firewall-Manager für erweiterte Protokollierung und Analyse sowie Aggregation von Firewall-Protokolldaten in einer einzigen intuitiven Ansicht.
Cisco SecureX	• Nutzen Sie die SecureX-Plattform, um die Erkennung und Beseitigung von Bedrohungen zu beschleunigen. Jede Cisco Secure Firewall beinhaltet eine Berechtigung für Cisco SecureX. Das neue SecureX-Menüband im Firewall Management Center ermöglicht es SecOps, sofort auf die offene Plattform von SecureX zu wechseln und die Incident Response zu beschleunigen.
Cisco Talos® Threat-Intelligence	• Die Cisco Talos Intelligence Group gehört zu den größten kommerziellen Threat-Intelligence-Teams weltweit. Sie liefert schnelle und aussagekräftige Threat-Intelligence für die Kunden, Produkte und Services von Cisco. Talos pflegt die offiziellen Regelsätze von Snort.org, ClamAV und SpamCop.

Nächste Schritte

Noch mehr über Cisco Secure Firewall erfahren Sie auf der entsprechenden Produktseite. Besuchen Sie außerdem unseren Portfolio-Explorer, um weitere Security-Lösungen für Finanzdienstleister kennenzulernen. Für Kaufoptionen oder zur Kontaktaufnahme mit dem Cisco Sales-Team besuchen Sie bitte diese Seite.

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 **www.cisco.com/go/offices**.

Gedruckt in den USA C45-3380706-00 02/23