



Cisco **SecureX** Produktbroschüre

Sicherheit – ein hoch relevantes Thema

Ursprünglich bestand die Aufgabe von Sicherheitslösungen in erster Linie darin, die Infrastruktur innerhalb des Netzwerks vor Bedrohungen und Malware von außerhalb zu schützen.

Heutzutage gilt es jedoch, auch mobile Geräte wie Smartphones und iPads sowie die rasant zunehmende Konsumerisierung der IT und die damit verbundene Nutzung von Social Media am Arbeitsplatz abzusichern. Gleiches gilt für die immer komplexer werdenden Unternehmensstrukturen: Telearbeiter, Subunternehmer, Partner und geschäftskritische Services sind aus der heutigen Geschäftspraxis nicht mehr wegzudenken. Dies sind nur einige der Gründe für die wachsende Bedeutung leistungsfähiger Sicherheitssysteme für die Unternehmens-IT. Gleichzeitig gestaltet sich deren Umsetzung jedoch weitaus komplexer, als es früher der Fall war.

Die Grenzen von Netzwerken lassen sich heutzutage nicht mehr klar definieren. Daher müssen Unternehmen neue Ansätze verfolgen, um Sicherheitsbedrohungen abzuwehren sowie geschäftskritische Daten und Ressourcen zu schützen. Darüber hinaus sind leistungsfähige Kontrollmechanismen erforderlich, um die Einhaltung von gesetzlichen Vorschriften zu gewährleisten. So beispielsweise wird zwar durch die Möglichkeit der Nutzung verschiedenster Endgeräte eine produktivere und vielseitigere Zusammenarbeit an allen nur erdenklichen Standorten ermöglicht, diese Vorteile gehen jedoch auch mit immensen Herausforderungen für IT- und Sicherheitsexperten einher, die eine sichere, zuverlässige und nahtlose Sprach-, Video- und Datenübertragung gewährleisten müssen.





Cisco SecureX Architektur





Die Cisco SecureX Architecture™ ist ein Sicherheits-Framework der nächsten Generation, das flexible Lösungen, Produkte und Services zur Durchsetzung konsistenter Unternehmensrichtlinien in geografisch verteilten Netzwerken kombiniert. Immer mehr mobile Benutzer, die mit den verschiedensten Endgeräten auf das Netzwerk zugreifen möchten, und der Trend hin zu Cloud-basierten Infrastrukturen und Services stellen neue Anforderungen an die Netzwerksicherheit. Die Cisco SecureX Architektur adressiert diese Problematik. Durch die Verbindung von Global Threat Correlation mit kontextbasierten Zugriffsrichtlinien wird umfassender Schutz von Informationen, Anwendungen, Geräten und Benutzern gewährleistet.

Die Grenzen heutiger Unternehmensnetzwerke verschwimmen zusehends. Um dieser Entwicklung Rechnung zu tragen, gewährleistet die Cisco SecureX Architektur sichere Verbindungen zum Netzwerk für jeden Benutzer, unabhängig davon, wo er sich gerade befindet, welches Gerät er verwendet und zu welchem Zeitpunkt er auf das Netzwerk zugreifen möchte. Gewährleistet wird dies durch eine kontextbezogene Analyse anhand einer übergeordneten Policy Language, die Informationen darüber auswertet, wo welcher Benutzer momentan arbeitet, worin seine Rolle im Unternehmen besteht und auf welche Ressourcen er zugreifen darf. Diese dezentrale Durchsetzung von Sicherheitsrichtlinien ermöglicht einen besseren Schutz von Netzwerkressourcen, da der Netzwerkzugriff auch über Unternehmensgrenzen hinweg stets umfassend gesichert ist.

Im Folgenden werden die im Rahmen der Cisco SecureX Architektur verfügbaren Cisco® Sicherheitslösungen näher erläutert.

Netzwerksicherheit

Cisco hat eine Sicherheitsinfrastruktur für Netzwerke entwickelt, die Angriffe sowie Daten- und Anwendungsmisbrauch erkennt und effektiv blockt. Unser Portfolio umfasst Firewall- und Intrusion Prevention-Systeme für Standalone- sowie integrierte Implementierungen, mit denen Angriffe effektiver abgewehrt und Compliance-Anforderungen wie der PCI-Standard für die Datensicherheit bei Kartenzahlungen (PCI DSS) effizienter erfüllt werden können.

			
Cisco Adaptive Security Appliance der Serie ASA 5500	Cisco Intrusion Prevention System	Cisco Integrated Services Router Generation 2	Cisco Security Manager
<ul style="list-style-type: none"> • Kombiniert branchenführende Firewall-, VPN- und Intrusion Prevention-Technologie in einer umfassenden Plattform • Proaktiver Echtzeit-Schutz vor Bedrohungen und Services für eine sichere Unternehmenskommunikation • Geringere Bereitstellungs- und Betriebskosten sowie umfassende Sicherheit für Netzwerke aller Größen • Vielseitige, stets verfügbare Remote-Verbindungen mit integrierten Intrusion Prevention- und Web-Sicherheit-Funktionalitäten, um extrem sicheren Zugriff mobiler Mitarbeiter sowie erhöhte Produktivität sicherzustellen 	<ul style="list-style-type: none"> • Identifikation, Klassifizierung und Blockieren von Anwendungsmisbrauch und Malware wie Würmer, Spyware, Adware sowie Viren • Leistungsfähige, intelligente Erkennung von und Schutz vor Bedrohungen für zahlreiche Implementierungsformen • Zuverlässige Eliminierung von Bedrohungen dank globaler Datenanalyse über Cisco SIO und Reputationsfilter • Umfassende Sicherheit durch garantierte Abdeckung, Reaktionszeit und Leistungsfähigkeit gegenüber Sicherheitslücken bei Anwendungen von Microsoft und Cisco sowie anderen geschäftskritischen Applikationen im Unternehmen¹ • Gewährleistung von Geschäftskontinuität und effiziente Erfüllung von Compliance-Anforderungen 	<ul style="list-style-type: none"> • Integrierte Funktionen wie Firewall, Intrusion Prevention, VPN und Cloud-basierte Web-Sicherheit • Vereinfachte Integration neuer Netzwerksicherheitsfunktionen auf vorhandenen Routern • Zusätzliche Schutzfunktionen für maximale Netzwerksicherheit ohne Einsatz zusätzlicher Hardware • Geringere Kosten für Support und Verwaltung durch Reduzierung der Anzahl erforderlicher Geräte 	<ul style="list-style-type: none"> • Umfassende Management-Lösung für Netzwerk und Sicherheitsgeräte von Cisco • Konsistente Richtliniendurchsetzung, schnelle und effektive Reaktion auf Sicherheitsvorfälle sowie Erstellung von Berichten über das gesamte Netzwerk hinweg • Rollenbasierte Zugriffskontrolle und Freigabe-Framework zur Vorlage und Integration von Änderungen • Leistungsstarkes Richtlinien-, Objekt- und Ereignis-Management sowie Funktionen für Reporting und effiziente Fehlerbehebung

1. Der zugesicherte Leistungsumfang bezieht sich auf die Verfügbarkeit von Signaturen für unterstützte Cisco und Microsoft Anwendungen sowie weitere geschäftskritische Applikationen im Unternehmen. Vollständige Informationen zu den Service-Level Vereinbarungen inklusive Abdeckung von Anwendungen, Fehlerbehebung sowie die allgemeinen Geschäftsbedingungen stehen bei Cisco ab dem Datum der Veröffentlichung zur Verfügung (voraussichtlich im ersten Halbjahr 2011). Weitere Informationen erhalten Sie bei Ihrem Cisco Reseller.

E-Mail und Web Security

Cisco E-Mail- und Web-Sicherheitslösungen schützen vor kostspieligen Ausfallzeiten, die mit Spam, Viren und Bedrohungen aus dem Internet einhergehen. Die Lösungen sind als Implementierungen am Standort (On-Premises), Cloud-Services und als Hybrid-Modell mit zentralisiertem Management erhältlich.

		
<p><u>Cisco IronPort Email Security – Cloud, Hybrid und On-Premises</u></p>	<p><u>Cisco Web Security – Cloud und On-Premises</u></p>	<p><u>Cisco IronPort Security Management Appliance</u></p>
<ul style="list-style-type: none"> • Mehrschichtiger Ansatz zum Schutz vor Spam, Viren und kombinierten Bedrohungen für Unternehmen aller Größen • Vollständig integrierte Kontrolle des ausgehenden Datenverkehrs durch Funktionen wie Data Loss Prevention (DLP) und Verschlüsselung • Weniger Ausfälle, einfachere Administration der Mail-Systeme im Unternehmen und reduzierter Support-Aufwand • Umfassende Berichterstellung und Nachrichtenverfolgung für mehr Flexibilität von Administratoren • Flexible Lösungen, die an wachsende Unternehmensanforderungen angepasst werden können 	<ul style="list-style-type: none"> • Branchenführende Funktionen zum Schutz vor webbasierter Malware durch Web-Reputation und Inhaltsanalyse mithilfe von Cisco SIO • Umfassende, flexible Richtlinienkontrolle für Web 2.0-Seiten mit dynamischen Inhalten und integrierten Anwendungen • Zahlreiche Reporting-Funktionen für mehr Flexibilität bei der Überwachung der Internetnutzung • Verschiedene Bereitstellungsoptionen mit branchenführender ScanSafe- und IronPort Web Security-Technologie 	<ul style="list-style-type: none"> • Einfacheres Management aller Komponenten der Cisco IronPort Email und Web Security Appliance • Zentrales Reporting, Tracken von E-Mails sowie Spam-Quarantäne der Cisco IronPort Email Security Appliance • Zentrale Verwaltung der Web-Richtlinien für die Cisco IronPort Web Security Appliance • Möglichkeit zur Übertragung von Administrationsrechten für Web-Zugriffs-Richtlinien und individuelle URL-Kategorien

Proaktiver Sicherheitsansatz

Für die schnellstmögliche Erkennung und Analyse neuer Bedrohungsformen nutzen Cisco Sicherheitslösungen Echtzeit-Informationen aus der Cisco Security Intelligence Operations (SIO). Mit fast einer Million Live-Datenströmen von implementierten Cisco E-Mail-, Web-, Firewall- und Intrusion Prevention System (IPS)-Lösungen ist die Cisco SIO das umfangreichste Sicherheitssystem der Welt.

Nach der Auswertung und Verarbeitung der Datenströme erstellt die Cisco SIO mithilfe von über 200 Parametern Regeln zum Schutz vor Bedrohungen. Unsere Experten aus der SIO sammeln zudem kontinuierlich Informationen zu sicherheitsrelevanten Ereignissen, die kritische Auswirkungen auf Netzwerke, Anwendungen und Geräte haben können, und stellen diese zur Verwendung durch die Sicherheitslösungen bereit.

Dabei werden alle drei bis fünf Minuten dynamisch Regeln an implementierte Cisco Sicherheitslösungen übermittelt. Zusätzlich veröffentlicht das Cisco SIO-Team Best Practices und taktische Richtlinien zur Abwehr von Bedrohungen.

Weitere Informationen finden Sie unter: www.cisco.com/go/sio.

Sichere Mobilität

Cisco bietet leistungsfähige VPN-, Wireless- und Remote-Sicherheitslösungen für den einfachen und sicheren mobilen Netzwerkzugriff. Hierbei werden die verschiedensten Endgeräte und Plattformen unterstützt. Dies liefert die erforderliche Flexibilität, um wachsenden Mobilitätsanforderungen in den verschiedensten Einsatzbereichen gerecht zu werden.



[Cisco AnyConnect Secure Mobility Client](#)

- Hochsichere Remote-Verbindungen zwischen dem Unternehmensnetzwerk und verschiedensten verwalteten und nicht verwalteten Mobilgeräten
- Sicherer Netzwerkzugriff unabhängig vom Standort oder Endgerät
- Bereitstellung einer sicheren Konnektivätslösung durch Kombination mit der ASA Security Appliances sowie ISRs und ASRs
- Sichere Mobilität in den verschiedensten Umgebungen durch Integration in vorhandene Netzwerke



[Cisco Adaptive Wireless IPS Software](#)

- Automatisierte Analyse von Sicherheitsschwachstellen und der Übertragungsleistung für mehr Transparenz und Kontrolle im gesamten Netzwerk
- Geeignet für die Anforderungen von Netzwerken jeglicher Größenordnung dank konstanter Berücksichtigung der Funkumgebung
- Automatische Überprüfung des Wireless-Netzwerks auf Anomalien und Identifikation unbefugter Zugriffsversuche
- Integration mit Netzwerksicherheitslösungen von Cisco zur Etablierung eines mehrstufigen Ansatzes für Wireless-Sicherheit



[Cisco Virtual Office](#)

- Sichere, umfassende und verwaltbare Netzwerkservices auch für Mitarbeiter jenseits der herkömmlichen Arbeitsumgebung
- Kostengünstige Skalierbarkeit je nach Anforderungen
- Enthält Remote-Site und Headend-Systeme, Aggregation geografisch verteilter Standorte sowie Services von Cisco und autorisierten Partnern
- Büroähnliches Umfeld unabhängig vom Standort mithilfe von IP-Telefonen sowie Wireless-, Daten- und Video-Services

Sicherheit im Rechenzentrum

Cisco unterstützt Sie bei der Absicherung wertvoller Ressourcen und Server im Rechenzentrum. Zu diesem Zweck wird ein breites Portfolio an leistungsfähigen Funktionen zum Schutz vor Bedrohungen, zur sicheren Segmentierung des Netzwerks sowie zur effektiven Durchsetzung von Richtlinien geboten.

		
<p><u>Cisco ASA 5585-X Adaptive Security Appliance</u></p>	<p><u>Cisco Catalyst 6500 ASA Services Module</u></p>	<p><u>Cisco Virtual Security Gateway (VSG)</u></p>
<ul style="list-style-type: none"> · Bewährte Firewall mit umfassendem Intrusion Prevention System und leistungsstarkem VPN in einem integrierten System - Acht Mal höhere Leistungsdichte im Vergleich zu Firewalls anderer Hersteller dank Unterstützung der höchsten Anzahl an VPN-Sitzungen, doppelter Anzahl an Verbindungen pro Sekunde sowie vier Mal höherer Verbindungskapazität - Integration von Intrusion Prevention-Funktionalitäten, welche über die Verbindung mit der globalen Bedrohungsanalyse über Cisco SIO doppelt so effektiv sind wie frühere Intrusion Prevention Systeme · Kontextsensitive Firewall-Funktionen für detailliertere Analysen, stärkere Sicherheit und erhöhte Betriebseffizienz 	<ul style="list-style-type: none"> · Kombination umfassender Switching-Funktionen mit branchenführenden Sicherheitstechnologien in einer integrierten Sicherheitslösung · Bereitstellung von Sicherheitsfunktionen im Backbone des Rechenzentrums durch die Integration mit Cisco Catalyst 6500 Series Switches · Multiprotokoll-Datendurchsatz mit bis zu 16 Gbit/s, 300.000 Verbindungen pro Sekunde und 10 Millionen gleichzeitigen Sitzungen · Möglichkeit zur Bereitstellung von bis zu vier Modulen in einem Chassis bei einem Durchsatz von bis zu 64 Gbit/s pro Chassis 	<ul style="list-style-type: none"> · Integration mit Cisco Nexus 1000V Virtual Switch und Hypervisoren · Durchsetzung von Sicherheitsrichtlinien und bessere Transparenz auf virtuellen Maschinen · Logische Isolierung von Anwendungen in virtualisierten Rechenzentren und in Multi-Tenant-Umgebungen · Klare Trennung der Aufgaben von Sicherheits- und Netzwerkadministratoren

Sicherer Netzwerkzugriff

Cisco TrustSec® gewährleistet einen sicheren Zugriff auf Netzwerke und Netzwerkressourcen mithilfe von richtlinienbasierter Zugriffskontrolle, identitätsbasierter Netzwerkfunktionen sowie Services zur Gewährleistung der Datenintegrität und -sicherheit. Auf diese Weise können Compliance-Anforderungen effizienter erfüllt und Geschäftsprozesse bei erhöhter Sicherheit optimiert werden. Zudem wird so die Zugriffskontrolle auf das gesamte Netzwerk erweitert. Cisco TrustSec ist erhältlich als Appliance-basierte Lösung oder als integrierter Service basierend auf der 802.1X-Infrastruktur.



[Cisco Identity Services Engine](#)

- Durchsetzung konsistenter, kontextbasierter Unternehmensrichtlinien im gesamten Netzwerk durch die Erfassung von Daten zu Benutzern, Geräten, Infrastrukturen und Netzwerkservices
- Optimierte Fehlererkennung und -behebung dank erhöhter Transparenz hinsichtlich der Benutzer und Inhalte im Netzwerk
- Durchsetzung von Sicherheitsrichtlinien auf allen Geräten, die eine Verbindung mit dem Netzwerk herstellen
- Kombination von AAA-Daten (Authentication, Authorization, Accounting), Sicherheitsstatus, Profilerstellung und Gastzugriffsverwaltung



[Cisco Secure Access Control System](#)

- Steuerung des Netzwerkzugriffs auf Basis dynamischer Bedingungen und Attribute über eine einfach zu verwendende Management-Schnittstelle
- Erfüllung wachsender Zugriffsanforderungen durch ein regelbasiertes Richtlinienmodell für mehr Flexibilität und vereinfachtes Management
- Einfachere Verwaltung und optimierte Compliance durch Integration von Funktionen für Überwachung, Reporting und Fehlerbehebung
- Etablierung einer Zugriffsrichtlinie auf Basis integrierter Funktionen und verteilter Bereitstellungsoptionen

Vorteile der Cisco SecureX Architektur

Cisco SecureX:

- Adressiert die verschiedensten Anforderungen von Unternehmen über ein umfassendes und innovatives Sicherheitsprofil.
- Ermöglicht die dynamische Erkennung von Bedrohungen und den effektiven Schutz durch kontextsensitive Sicherheitsmechanismen und Echtzeit-Informationen.
- Gewährleistet eine grenzenlose Arbeitsumgebung mittels konsistenter Richtliniendurchsetzung im gesamten Unternehmen.
- Steigert die Produktivität von Mitarbeitern in Zweigstellen, von Telearbeitern sowie von mobilen Mitarbeitern durch die Möglichkeit zur Nutzung aller Funktionen und Services, die auch in der normalen Büroumgebung zur Verfügung stehen.
- Erleichtert die Einführung neuer Geschäftsmodelle wie SaaS und neuer Applikationen z. B. für die Videokommunikation ohne Einbußen bei der Sicherheit oder der Netzwerkleistung.
- Sorgt dank eines offenen, jedoch kontrollierten Architekturkonzepts für eine Minimierung von Risiken und eine effizientere Erfüllung gesetzlicher Auflagen.

Warum Cisco?

Cisco verfolgt einen umfassenden Ansatz für Sicherheitslösungen. Durch die Integration der Sicherheitsfunktionen in alle Bereiche des Netzwerks vereinfachen Cisco Lösungen unabhängig von der Anwendung oder dem Service die Erfüllung heutiger Sicherheits- und Geschäftsanforderungen. Die Cisco SecureX Architektur ermöglicht die Durchsetzung von Richtlinien über verteilte Standorte hinweg und bietet dabei umfassende Transparenz sowohl für mobile Benutzer als auch für Cloud-basierte Services. Dank umfassender Skalierbarkeit und hoher Flexibilität bietet die Architektur optimale Implementierungsmöglichkeiten für die Anforderungen von Unternehmen jeder Größe. Der einzigartige Sicherheitsansatz der Cisco SecureX Architektur bietet umfassende Kontrollmöglichkeiten bei maximaler Sicherheit und ermöglicht Unternehmen, ihre Ziele erfolgreich umzusetzen.

Weitere Information zu Cisco Sicherheitsprodukten und -services finden Sie unter www.cisco.com/go/security und www.cisco.com/go/services/security.

