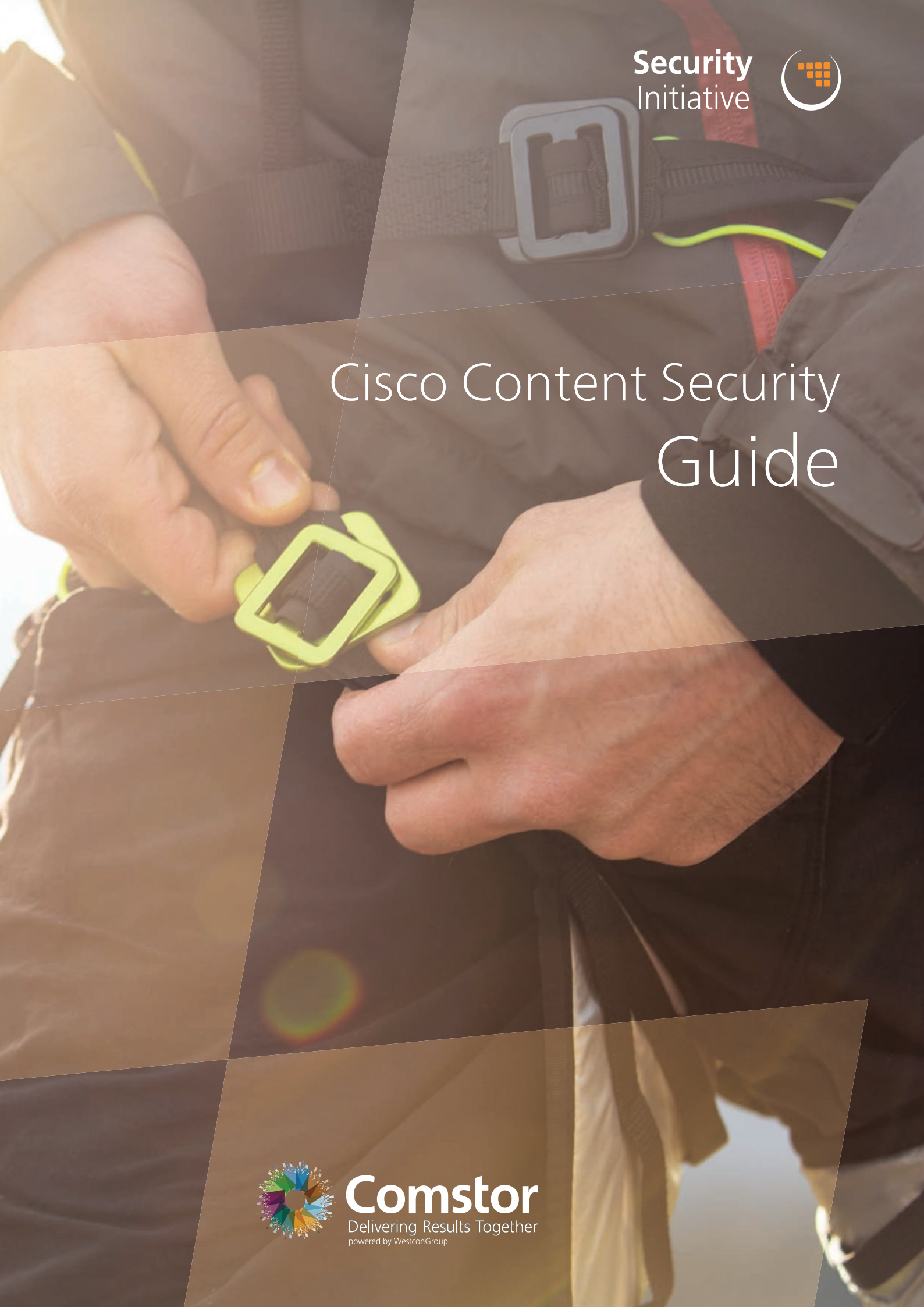


Security
Initiative

Cisco Content Security Guide

Comstor
Delivering Results Together
powered by WestconGroup

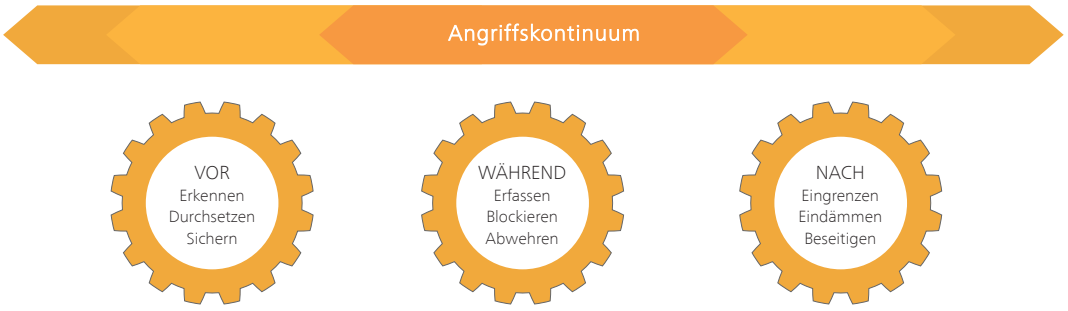
INHALT

CISCO CONTENT SECURITY

Unternehmen stehen heute unter ständigem Beschuss. Täglich brechen Security Angriffe auf sie herein, die mit immer raffinierteren Techniken selbst die leistungsfähigsten Sicherheitsprogramme und IPS nicht aufhalten können. Es hat sich herauskristallisiert, dass eine Point-in-Time-Erkennung der Security Tools den Datenverkehr nur beim Eintritt in das erweiterte Netzwerk untersucht.
Und an diesem Punkt lässt sich niemals sicherstellen, dass alle Bedrohungen in ihrer Gesamtheit erkannt werden.
Darüber hinaus bieten diese Tools nicht ausreichend Einblick in die Aktivitäten der Bedrohungen, wenn diese an den ersten Verteidigungslinien vorbei gelangt sind. Daher tappen die IT-Sicherheitsteams oft im Dunkeln, was den Umfang der jeweiligen Bedrohung betrifft, und können bspw. Malware nicht schnell genug erkennen und bekämpfen.

Um sich effektiv vor den Bedrohungen von heute schützen zu können, benötigen Unternehmen eine Lösung, die verschiedene Angriffsvektoren abdeckt, Informationen austauscht und die Komplexität verringert. So entsteht die erforderliche umfassende Transparenz und Kontrolle, um Sicherheitsverletzungen zu verhindern. Daher ist ein bedrohungsorientierter Sicherheitsansatz gefragt, der vor, während und nach einem Angriff greift.

Effektiver Schutz vor komplexen Bedrohungen



Firewall	VPN	NGIPS	Advanced Malware Protection
NGFW	UTM	Web Security	Network Behavior Analysis
NAC + Identity Services		E-Mail Security	
Sichtbarkeit und Kontext			

Cisco bietet im Bereich E-Mail und Web Security umfassende Technologien an und hat speziell für die Prüfung von Web und E-Mail Inhalten sowie von Transaktionen eine Lösung entwickelt, die diese anhand von Echtzeit-Bedrohungsinformationen analysiert.
Zudem verfügt Cisco über das weltweit umfangreichste Netzwerk für die Erkennung von Sicherheitsbedrohungen.
Mit den Experten und Analysten von Cisco Talos werden rund um die Uhr weltweit Datenverkehrsaktivitäten analysiert und Bedrohungen somit frühzeitig erkannt sowie Abwehrmaßnahmen entwickelt.

Das Cisco Content Security Lösungsportfolio umfasst E-Mail Security, Web Security und das Content Security Management.
Vorab sollte festgelegt werden, ob der Lizenzkauf für ein, drei oder fünf Jahre getätigt werden soll und für wie viele Nutzer die Bundles lizensiert werden sollen. Zur Orientierung dient die User Band Aufschlüsselung im Anhang.

Cisco E-Mail Security

Komplexe und kombinierte Angriffe per E-Mail und über das Internet vergrößern die Anzahl der Bedrohungen. Mobile Anwendungen und Cloud-Plattformen vervielfachen dieses Risiko zusätzlich. Ein globaler Überblick über die Bedrohungslage und eine E-Mail-Sicherheitsinfrastruktur, die umgehend darauf reagieren kann, sind für den Schutz geschäftskritischer Systeme entscheidend.
Die marktführenden E-Mail-Security-Lösungen von Cisco bieten starke Leistung, Echtzeitschutz, niedrige Gesamtbetriebskosten und flexible Bereitstellungsoptionen.

SECURITY MANAGEMENT FEATURES		BESCHREIBUNG
Abwehr von Bedrohungen	ANTI-SPAM	Schutz vor Spam bei eingehenden E-Mails durch mehrere Anti-Spam-Engines.
	ANTI-VIRUS (SOPHOS)	Branchenführender und leistungsstarker Schutz vor Virenangriffen per E-Mail.
	OUTBREAK FILTERS	Untersuchung ein- und ausgehender E-Mails auf deren Bedrohungspotential und Erstellen eines Threat-Scores. Verdächtige E-Mails (erhöhter Threat-Score) werden temporär in einen Quarantäne-Server geleitet und nach Veröffentlichung des Viren-Pattern von den traditionellen, reaktiven Anti-Virus-Lösungen gefiltert.
	ADVANCED MALWARE PROTECTION (AMP)	AMP ist eine umfassende Lösung zum Schutz gegen schädliche Dateien im E-Mail und Web-Traffic. Sie verwendet eine Kombination aus File-Reputation, File-Sandboxing und retrospektiver Dateianalyse, um Bedrohungen zur erkennen und zu stoppen.
Datensicherheit und Kontrolle ausgehender Nachrichten	DATA LOSS PREVENTION (DLP)	DLP hilft zu verhindern, dass vertrauliche und sensible Daten das Unternehmensnetzwerk verlassen. Es ist ein Sicherheitssystem für ausgehenden Datenverkehr, um Compliance sicherzustellen und vertrauliche Informationen zu schützen.
	E-MAIL ENCRYPTION	Sicheres und leistungsstarkes E-Mail-Verschlüsselungssystem.

Auswahl der Plattform: Hardware + Smart Net Total Care Support (SNTC), virtuelle Appliance oder Cloud Service

EINSATZ	APPLIANCE (ESA)	VIRTUELLE APPLIANCE* (ESAv) - SPEZIFIKATION	CLOUD (CES)
Evaluierung & Test		C000v (Evaluation only) • 200 GB, 10k SAS HDD • 4 GB Memory • 1 CPU Kern (2,7 GHz)	
Kleine Unternehmen / Zweigstellen	C190 (ca. 2.000 User) (ESA-C190-K9 + SNTC)	C100v (bis 1.000 User) • 200 GB, 10k SAS HDD • 6 GB Memory • 2 CPU Kerne (2,7 GHz)	Cloud E-Mail Security (ab 100 Nutzer)
Mittlere Unternehmen / Niederlassungen	C390 (bis ca. 10.000 User) (ESA-C390-K9 + SNTC)	C300v (bis 5.000 User) • 500 GB, 10k SAS HDD • 8 GB Memory • 4 CPU Kerne (2,7 GHz)	
Großunternehmen und Service Provider	C690 (ab ca. 10.000 User) (ESA-C690-K9 + SNTC)	C600v (User: Sizing erforderlich) • t500 GB, 10k SAS HDD • 8 GB Memory • 8 CPU Kerne (2,7 GHz)	

Hinweis: On-Premise und Cloud E-Mail Security kann durch die "Cisco Hybrid E-Mail Security" kombiniert werden.

* VMware ESX/ESXI Hypervisor erforderlich

E-Mail Security

Welche E-Mail Security Features werden für die Appliance und virtuelle Appliance benötigt?

SOFTWARE SUBSCRIPTION	BESCHREIBUNG	PRODUKT SKU (ESA / ESAv)
Cisco E-Mail Security Inbound Essentials Bundle**	Anti-Spam Scanning + Sophos Anti-Virus + Virus Outbreak Filters + Clustering	ESA-ESI-LIC=
Cisco E-Mail Security Outbound Essentials Bundle **	Data Loss Prevention + E-Mail Encryption + Clustering	ESA-ESO-LIC=
Cisco E-Mail Security Premium Bundle **	Kombination aus E-Mail Security Inbound und Outbound Essentials Bundles.	ESA-ESP-LIC=

? Werden zusätzliche Features benötigt, die nicht in einem Software Bundle lizenziert sind?

Advanced Malware Protection (AMP)	Bietet File Reputation, File Sandboxing sowie retrospektive Dateianalyse.	ESA-AMP-LIC=
Graymail Safe-Unsubscribe	Einfache und sichere Möglichkeit, um unerwünschte E-Mails abzubestellen, bei gleichzeitigem Schutz vor Bedrohungen oder Phishing-Attacken durch illegitime „Unsubscribe" Links.	L-ESA-GSU-LIC=
Cloudmark Antispam	Anti-Spam Lösung für hochperformante Umgebungen.	ESA-CLM-LIC=
Image Analyzer	Ermittelt rechtswidrige Inhalte bei ein- und ausgehenden E-Mails.	ESA-IA-LIC=
McAfee AntiVirus	Scannen mit McAfee Antivirus Engine.	ESA-MFE-LIC=
Intelligent Multi-Scan	Kombiniert mehrere Antispam Technologien für eine sehr hohe Genauigkeit.	ESA-IMS-LIC=
ZixGateway mit Cisco Technology (ZCT)	ZCT ist ein on-premise Verschlüsselungsservice für die E-Mail Security Appliance. Die Schlüssel werden on-premise gespeichert, statt in der Cloud.	CCS-ZCT201-K9 CCS-ZCT400-K9 L-ZCTV-K9-LIC + Subscription

E-Mail Centralized Management (gleichzeitiges Management und Konfiguration mehrerer Appliances) ist in den Bundles inklusive und kann bei a la carte Konfigurationen kostenfrei mitbestellt bzw. über das Lizenzcenter von Cisco angefordert werden.

** Es kann nur ein Software Bundle ausgewählt werden. Alle Bundles und a la carte Angebote beinhalten die Lizenz für die Virtuelle Appliance (ESAv).

Cloud E-Mail Security (CES)

Welche Features werden für Cisco Cloud E-Mail Security (CES) benötigt?

SOFTWARE SUBSCRIPTION	BESCHREIBUNG	PRODUKT SKU (CES)
Cisco E-Mail Security Inbound Essentials Bundle	• IPAS (Anti-Spam Filtering) • AV (Sophos Anti-Virus Filtering) • VOF (Virus Outbreak Filters für Zero-Hour Virenschutz und URL Filtering)	L-CES-ESI-LIC=
Cisco E-Mail Security Outbound Essentials Bundle	• DLP (RSA Data Loss Prevention Scanning) • E-Mail Encryption (Cisco Registered Envelope Service)	L-CES-ESO-LIC=
Cisco E-Mail Security Premium Bundle	Kombination aus E-Mail Security Inbound und Outbound Essentials Bundles.	L-CES-ESP-LIC=
Cloud E-Mail Security O365 Inbound oder Premium	Identisch zu Inbound Essentials oder Premium Bundles, jedoch ohne AV Engine, diese wird von Microsoft bereit-gestellt.	L-CES-O365I-LIC= L-CES-O365P-LIC=

? Werden zusätzliche Features benötigt, die nicht in einem CES Software Bundle lizenziert sind?

Advanced Malware Protection (AMP) Add-on	File Reputation + File Sandboxing + retrospektive Datei-analyse.	L-CES-AMP-LIC=
DLP	DLP (RSA Data Loss Prevention Scanning) für Inbound Bundle.	L-CES-DLP-LIC=
PXE Encryption	Cisco Registered Envelope Service für Inbound Bundle.	L-CES-PXE-LIC=
Image Analyzer	Ermittelt rechtswidrige Inhalte in E-Mails.	L-CES-IA-LIC=
McAfee AntiVirus	Scannen mit McAfee Antivirus Engine.	L-CES-MFE-LIC=
Intelligent Multi-Scan	Kombiniert mehrere Antispam Technologien für eine sehr hohe Genauigkeit.	L-CES-IMS-LIC=
Safe unsubscribe add-on	Sicheres Abbestellen unerwünschter E-Mails.	L-CES-GSU-LIC=

E-Mail-Security-Lösungen von Cisco bieten starke Leistung, Echtzeitschutz und flexible Bereitstellungsoptionen.

Comstor bietet die passende Beratung & Support.

Cisco Web Security

In der hochgradig vernetzten und zunehmend mobilen Welt von heute benötigen Unternehmen zuverlässigen Schutz. Cisco Web Security schützt das Netzwerk vor Malware und unterstützt Unternehmen jeder Größe bei der effizienten Kontrolle und Sicherung der Internetnutzung. Sie bietet Schutz vor Bedrohungen, die den Geschäftsbetrieb unterbrechen können. Die Web Security Lösung von Cisco kann als Hardware Appliance, virtuelle Appliance oder Cloud Service erworben werden.

Zudem lassen sich einzelne Cisco Security Lösungen um die Web Security erweitern. Es besteht die Möglichkeit den ISR G2 Router um den Cloud Web Security Connector zu erweitern, um die Benutzer vor webbasierten Bedrohungen wie Viren zu beschützen. Zudem lässt sich mit dem Cisco AnyConnect Secure Mobility Client die Web Security auf mobile Geräte ausdehnen, indem er den ein und ausgehenden Datenverkehr auf mobilen Geräten wie Smartphones und Tablets schützt.

WEB SECURITY FEATURES		BESCHREIBUNG
Starker Schutz	LAYER 4 TRAFFIC MONITORING	Der Layer 4 Traffic Monitor scannt kontinuierlich alle Zugriffe, Ports und Protokolle an einem Standort. Er erkennt und blockiert Spyware wie z.B. eine "Call-Home"-Kommunikation und stoppt Malware, die versucht die klassischen Web Security Lösungen zu umgehen.
	MALWARE-SCHUTZ IN ECHTZEIT	Mehrere Ebenen von Anti-Malware-Technologien bieten umfassenden Schutz vor Advanced Persistent Threats und Malware. Web-Reputation-Filter analysieren mehr als 200 verschiedene Web-Traffic-und Netzwerkparameter, um für eine leistungsfähige äußere Schicht der Malware-Abwehr zu sorgen. Auf einer einzigen Appliance können mehrere Anti-Malware-Engines parallel eingesetzt werden.
	ADVANCED MALWARE PROTECTION (AMP)	AMP ist eine umfassende Lösung zum Schutz gegen schädliche Dateien im E-Mail und Web-Traffic. Sie verwendet eine Kombination aus File-Reputation, File-Sandboxing und retrospektiver Dateianalyse, um Bedrohungen zu erkennen und zu stoppen.
Vollständige Kontrolle	DYNAMIC URL-FILTERING	Kombination aus traditioneller URL-Filterung und einer dynamisch aktualisierten URL-Datenbank zur Absicherung gegen Compliance-, Zuverlässigkeits- und Produktivitätsrisiken. Die Cisco Dynamic Content Analysis Engine (DCA) analysiert Seiteninhalte auf unbekannten URLs, um sie in Echtzeit zu kategorisieren. Kategorisierungen werden alle drei bis fünf Minuten von den Cisco aktualisiert.
	APPLICATION VISIBILITY & CONTROL (AVC)	Einfache Festlegung und Durchsetzung von Sicherheitsrichtlinien und Kontrolle der Nutzung von Hunderten von Web 2.0-Anwendungen und mehr als 150.000 Mikroanwendungen. Die präzise Richtliniensteuerung ermöglicht es Administratoren, die Nutzung von Anwendungen wie Facebook oder Dropbox zu erlauben und zugleich Aktivitäten wie das Hochladen von Dokumenten oder das Klicken auf „Gefällt mir" zu sperren.
	DATA LOSS PREVENTION (DLP)	Verhindert, dass vertrauliche Daten das Netzwerk verlassen, indem kontextbasierte Regeln für einen grundlegenden Schutz vor Datenverlusten erstellt werden. Cisco Web Security nutzt das Internet Content Adaptation Protocol (ICAP) für die Integration in DLP-Lösungen von Drittanbietern zur umfassenden Prüfung von Inhalten und für eine DLP-Richtliniendurchsetzung.
	CISCO ANYCONNECT SECURE MOBILITY CLIENT	Schutz von Daten, die von Roaming-Laptops angefordert werden. AnyConnect baut dynamisch ein VPN auf, das den Datenverkehr auf den primären Web Access Point umleitet. So kann eine Echtzeitanalyse erfolgen, bevor der Zugriff gewährt wird.

Auswahl der Plattform: Hardware + Smart Net Total Care Support (SNTC), virtuelle Appliance oder Cloud Service

EINSATZ	APPLIANCE (WSA)	VIRTUELLE APPLIANCE* (WSAv) - SPEZIFIKATION	CLOUD (CWS)
KLEINE UNTERNEHMEN UND ZWEIGSTELLEN	S190 (100 – 1.500 User) (WSA-S190-K9 + SNTC)	S000v (< 1.000 Web User) • 250 GB HDD • 4 GB Memory • 1 CPU Kern	Cloud Web Security (ab 25 User)
MITTLERE UNTERNEHMEN	S390 (ca. 1.500 – 6.000 User) (WSA-S390-K9 + SNTC)	S100v (1.000 – 2.999 Web User) • 250 GB HDD • 6 GB Memory • 2 CPU Kerne	
GROSSUNTERNEHMEN UND SERVICE PROVIDER	S690 (ca. 6.000 – 12.000 User) (WSA-S690-K9 + SNTC)	S300v (3.000 – 6.000 Web User) • 1 TB HDD • 8 GB Memory • 4 CPU Kerne	

Web Security

Welche Web Security Features werden für die Appliance und virtuelle Appliance benötigt?

SOFTWARE SUBSRCIPTION	BESCHREIBUNG	PRODUKT SKU
Cisco Web Security Essentials Bundle**	Web Reputation + Web Usage Controls • Reputation • URL Filtering • Application Visibility and Control (AVC)	WSA-WSE-LIC=
Cisco Web Security Anti-Malware Bundle**	Web Reputation + Deep Content Scanning • Sophos Anti-Malware • Webroot Anti-Malware	WSA-WSM-LIC=
Cisco Web Security Premium Bundle**	Kombination aus Web Security Essentials und Anti-Malware Bundles.	WSA-WSP-LIC=

? Werden zusätzliche Features benötigt, die nicht in einem Software Bundle lizenziert sind?

Advanced Malware Protection (AMP)	File Reputation + File Sandboxing + retrospektive Dateianalyse + CTA	WSA-AMP-LIC=
McAfee Anti-Malware	Virus und Anti-Malware Scanning (signature- and heuristics-based scanning)	WSA-AMM-LIC=
Sophos Anti-Malware	Malware Scanning und Schutz vor bekannten und unbekannten Bedrohungen (Genotype / Behavioral Genotype Protection).	WSA-AMS-LIC=
Webroot Anti-Malware	Alle Web-Anfragen und -Antworten werden gescannt. Bedrohungen werden durch Zugriff auf Datenbanken identifiziert, die täglich Millionen von Webseiten intelligent durchscannen.	WSA-AMW-LIC=
Cognitive Threat Analytics	Verhaltensanalyse des Netzwerkverkehrs. Identifiziert Symptome einer Malware Infektion, Anomalien und Command-and-Control Aktivitäten.	L-WSA-CTA-LIC=

* VMware ESX/ESXI Hypervisor erforderlich

** Es kann nur ein Software Bundle ausgewählt werden. Alle Bundles und a la carte Angebote beinhalten die Lizenz für die virtuelle Appliance (WSAv).

Weitere Bereitstellungsoptionen

ISR G2 mit CWS Connector	Schutz der Benutzer vor webbasierten Bedrohungen wie Viren. Der Internetverkehr wird intelligent in die Cloud umgeleitet.
AnyConnect Secure Mobility Client	Ausdehung der Web Security auf mobile Geräte. Diese Software stellt eine ständig aktive VPN-Verbindung für alle Laptops, Tablets und Smartphones her und umfasst die Möglichkeit, den CWS-Client zu lizenzieren.

Cloud Web Security

Welche Features werden für Cisco Cloud Web Security (CWS) benötigt?

SOFTWARE SUBSRCIPTION	BESCHREIBUNG	PRODUKT SKU (CWS)
Cisco Web Security Essentials Bundle*	• Web Filtering (Application Visibility und Web Usage Control) • Malware Scanning (Antimalware Protection und Content Analysis) • Secure Mobility (Integration mit AnyConnect Client)	CWS-LIC=
Advanced Threat Detection Bundle* (Add-On für Essentials Bundle)	• Cognitive Threat Analytics • Advanced Malware Protection	CWS-ATD-LIC=
Cisco Web Security Premium Bundle*	• Kombination aus Web Security Essentials und Advanced Threat detection Bundles.	CWS-WSP-LIC=

? Werden zusätzliche Features benötigt, die nicht in einem CWS Software Bundle lizenziert sind?

Cognitive Threat Analytics für CWS	• Verhaltensanalyse des Netzwerkverkehrs • Identifiziert Symptome einer Malware Infektion, Anomalien und Command-and-Control Aktivitäten	L-CWS-CTA-LIC=
Advanced Malware Protection für CWS	• Malware Erkennung, Malware Blockierung und retrospektive Dateianalyse • File Reputation + File Sandboxing	CWS-AMP-LIC=
Log Extraction API für CWS	• Log Daten in W3C Text Format	L-CWS-LOG-LIC=

* Es kann nur ein Software Bundle ausgewählt werden. Alle Bundles und a la carte Angebote beinhalten die Lizenz für die virtuelle Appliance (WSAv).

Cisco Web Security schützt das Netzwerk Ihrer Kunden vor Malware und unterstützt Unternehmen jeder Größe bei der effizienten Kontrolle und Sicherung der Internetnutzung.

Cisco Content Security Management

Die Cisco Content Security Management Appliance (SMA) vereinfacht die Administration von mehreren Cisco E-Mail Security und Web Security Appliances. Das flexible Management-Tool zentralisiert und konsolidiert die Sicherheitsrichtlinien und bietet eine einzige Management-Schnittstelle für E-Mail und Web Sicherheit. Änderungen und Einstellungen werden zentral auf einer Konsole und nicht auf den einzelnen Geräten verwaltet.

SECURITY MANAGEMENT FEATURES		BESCHREIBUNG
E-Mail Security 	ADVANCED MESSAGE TRACKING	Ermöglicht Administratoren die Analyse, wo und wann eine E-Mail Kommunikation stattgefunden hat. Die Daten werden von mehreren Cisco ESAs erfasst, einschließlich der Kategorisierung nach Sender, Empfänger, Betreff und anderen Parametern. Scan-ergebnisse, etwa durch Spam-und Viren-Urteile, werden ebenfalls angezeigt, ebenso wie Richtlinienverletzungen.
	CENTRALIZED SPAM QUARANTINING	Spam E-Mails werden zentral in einer Spam Quarantäne gespeichert. Die Self-Service Lösung verfügt über ein einfach zu bedienendes Web- oder E-Mail-In-terface und lässt sich einfach in bestehende Verzeichnisse und E-Mail-Systeme integrieren.
	E-MAIL REPORTING	Bietet kurze Szenario-basierte Berichte und hilft Administratoren, den E-Mail-Verkehr im Auge zu behalten sowie bei der Fehlersuche.
Web Security 	WEB REPORTING	Web-Tracking-Informationen werden in Echtzeit zusammengefasst und in einem einfach zu bedienenden grafischen Format angezeigt. Berichtsfunktionen helfen Administratoren die Webseiten, URL-Kategorien und Anwendungen zu bestimmen, auf die Mitarbeiter mit zugreifen.
	THREAT MONITORING	Daten über Web-basierte Bedrohungen werden in Echtzeit zur Verfügung gestellt. Neben der Anzeige mit blockierter Malware, werden Benutzer aufgezeigt, die gegen die meisten Warnungen verstoßen und welche Webseiten oder URL-Kategorien die größten Risiken darstellen.
	REPUTATION SCORING	Diese Funktion bietet detaillierte Informationen über die Reputationswerte der Websites, auf die Benutzer zugreifen. Die Werte basieren auf Daten, die von Cisco WSA's bereitgestellt werden, die Webserver analysieren und jeder URL eine Punktzahl zuweisen. Diese Punktzahl spiegelt die Wahrscheinlichkeit auf Malware wider.
	BOTNET DETECTION	Angezeigt werden Ports und Systeme mit potenziellen Malware-Verbindungen. Diese Daten aus dem Layer-4-Traffic Monitoring helfen, Botnet-infizierte Rechner zu erkennen.
	WEB POLICY UND CONFIGURATION MANAGEMENT	Ermöglicht dem Web-Administrator von einem einzelnen Standort aus, die Richtlinien für mehrere Web Security Appliances zu erstellen und zu veröffentlichen.

Auswahl der Plattform: Hardware + Smart Net Total Care Support (SNTC) oder virtuelle Appliance

EINSATZ	APPLIANCE (SMA)	VIRTUELLE APPLIANCE* (SMAv) - SPEZIFIKATION
Evaluierung & Test	-	M000v (Evaluation only) • 250 GB, 10k SAS HDD • 4 GB Memory • 1 CPU Kern (2,7 GHz)
Kleine Unternehmen und Zweigstellen	M190 (> 1.500 User) SMA-M190-K9 + SNTC	M100v (bis 1.000 User) • 250 GB, 10k SAS HDD • 6 GB Memory • 2 CPU Kerne (2,7 GHz)
Mittlere Unternehmen	M390 (1.500 – 10.000 User) SMA-M390-K9 + SNTC	M300v (bis 5.000 User) • 1 TB, 10k SAS HDD • 8 GB Memory • 4 CPU Kerne (2,7 GHz)
Großunternehmen und Service Provider	M690 (> 10.000 User) SMA-M690-K9 + SNTC	M100v (bis 1.000 User) • 2 TB, 10k SAS HDD • 8 GB Memory • 8 CPU Kerne (2,7 GHz)

Security Management Software Bundles

SOFTWARE SUBSCRIPTION	BESCHREIBUNG	PRODUKT SKU
Cisco E-Mail Security Management Software Subscription	E-Mail Reporting + Message Tracking + Centralized Quarantines für mehrere E-Mail Appliances	SMA-EMGT-LIC=
Cisco Web Security Management Software Subscription	Web Reporting + Web Policy und Configuration Management für mehrere Web Appliances	SMA-WMGT-LIC=

? Werden zusätzliche Features benötigt, die nicht in einem Software Bundle lizenziert sind?

Advanced Web Security Reporting – Lower Tier **	• nur Reporting Lizenz • max 2 MB pro User pro Tag	SMA-WSPL-LOW-LIC=
Advanced Web Security Reporting – Higher Tier **	• nur Reporting Lizenz • max 6 MB pro User pro Tag	SMA-WSPL-HIGH-LIC=

* VMware ESXi/ESXI Hypervisor erforderlich

** Die beiden Advanced Lizenzen eignen sich inbesondere für Unternehmen mit hohem Internet Traffic und ermöglichen eine Erweiterung des Web Security Reporting für WSA und CWS.

ANHANG

Wie viele Nutzer sollen lizenziert werden?

ANZAHL	USER BAND	ANZAHL	USER BAND
100–199 Nutzer (CWS: 25 – 199 Nutzer)	S1	10.000–19.999 Nutzer	S9
200–499 Nutzer	S2	20.000–49.999 Nutzer	S10
500–999 Nutzer	S3	50.000–99.999 Nutzer	S11
1.000–1.999 Nutzer	S4	100.000–249.999 Nutzer	S12
2.000–2.999 Nutzer	S5	250.000–499.999 Nutzer	S13
3.000–3.999 Nutzer	S6	500.000–999.999 Nutzer	S14
4.000–4.999 Nutzer	S7	Mehr als 1.000.000 Nutzer	S15
5.000–9.999 Nutzer	S8		

HARDWARE SUPPORT

Hardware Support: Cisco Smart Net Total Care (SNTC) Service ist als Option erhältlich

- ✓ Schneller technischer Support von Cisco Experten
- ✓ 24 Stunden Online Support
- ✓ Laufende Aktualisierungen des Betriebssystems der Appliance
- ✓ Schneller Hardware Austausch (SNTC – 8x5xNBD)

Cisco weitet sein Security Lösungsportfolio kontinuierlich aus. Wir möchten Ihnen helfen, mit diesen Entwicklungen Schritt zu halten und bieten Ihnen unser fokussiertes Partnerprogramm Comstor Security Initiative (CSI) an.

Dieses ermöglicht Ihnen komplette Sicherheitslösungen, die auf Cisco's Security Portfolio aufbauen, zu entdecken, zu testen und zu verkaufen. Die Bestandteile des breitgefächerten Programms sind fachspezifische Ausbildung und Schulung, eine gemeinsame Geschäftsplanung sowie Demand Generation Aktivitäten für Ihre Geschäftsentwicklung. Verstehen Sie das CSI Programm als eine Partnerschaft zwischen Ihnen und Comstor, wo alles, was Sie über Cisco Security-Lösungen wissen müssen, bereitgestellt wird, um Ihr Cisco Security-Geschäft zu entwickeln und auszubauen.

Engage
Ihr Einstieg bei Comstor

Develop
Entwickeln Ihrer Cisco Geschäftstätigkeiten und gemeinsame Planung

Grow
Ausbau Ihrer Kenntnissen in den Cisco Architekturen für ein stabiles Geschäftswachstum

Extend
Erschließen neuer Märkte und Geschäftsmodelle

Security Initiative

Comstor
Delivering Results Together
powered by WestconGroup

KONTAKT

Thomas Kind
Business Manager Security Solutions
Tel: +49 30 346 03 - 331
Mobil: +49 175 1500 918
E-Mail: thomas.kind@comstor.com

Comstor Deutschland
Comstor - Westcon Group Germany GmbH
Franklinstraße 28/29
10587 Berlin

www.de.comstor.com