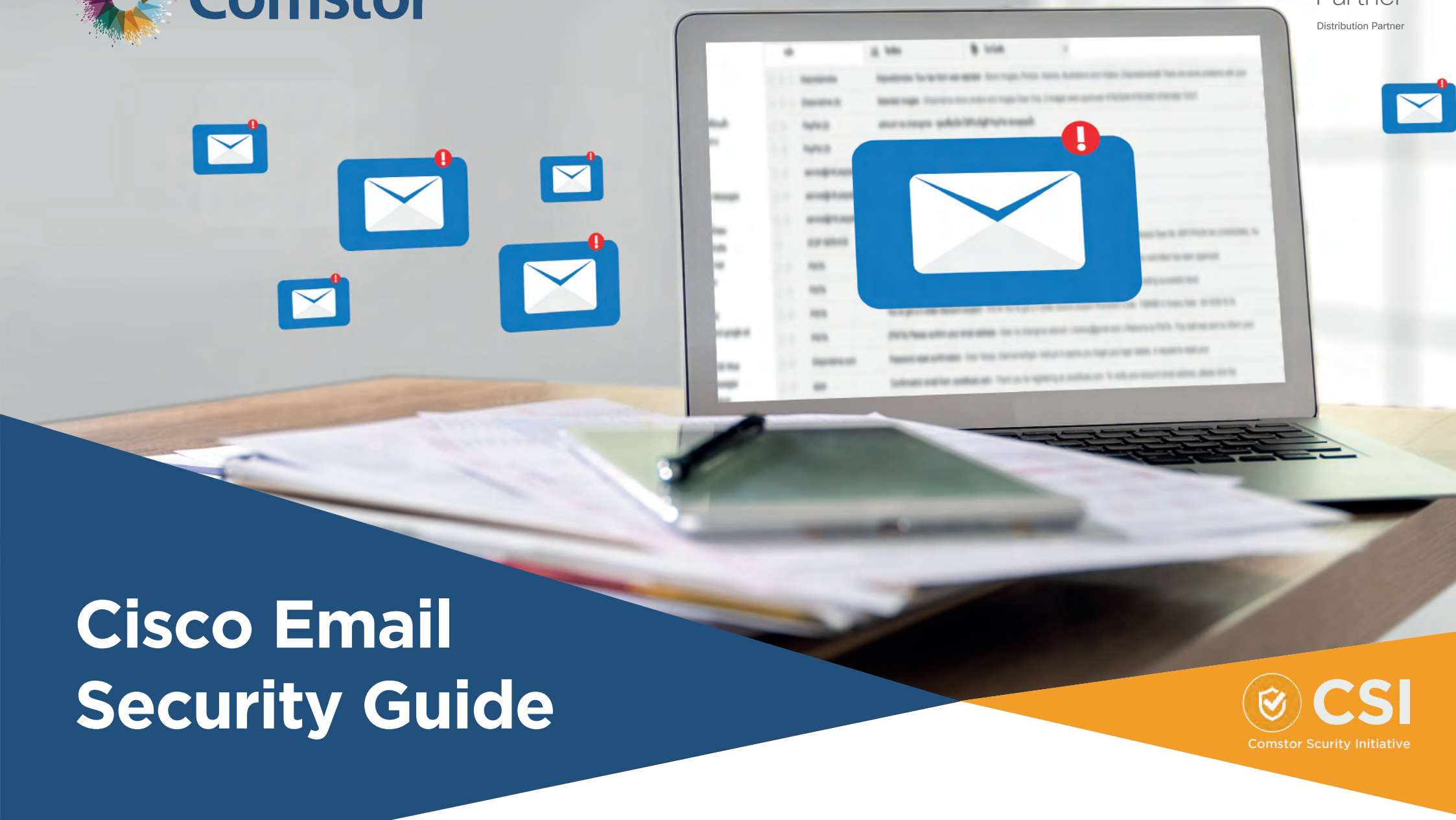
Comstor

Cisco Partner
Distribution Partner



Cisco Email Security Guide

CSI
Comstor Scurity Initiative

Cisco Email Security

E-Mails sind die wichtigste Art der Unternehmenskommunikation und der größte Bedrohungsvektor bei Cyberangriffen. Raffinierte Cyberkriminelle nutzen zunehmend E-Mails, um Ransomware und andere komplexe Malware schnell und effektiv einzuschleusen. Das Ziel dieser Cyberangriffe ist es, z. B. Geld zu erpressen oder das geistige Eigentum eines Unternehmens oder personenbezogene Daten der Mitarbeiter zu stehlen. Der zunehmende Einsatz von Cloud-Mailbox-Services wie Microsoft 365 öffnet zusätzlich kombinierten Angriffen Tür und Tor.

Die Cisco Email Security-Lösung bietet hochverfügbare E-Mail-Schutzebenen - auch für Cloud-basierte E-Mail-Lösungen wie Office 365 - gegen dynamische, sich rasch ändernde Bedrohungen, mit denen Unternehmen heute konfrontiert werden.

Mit Cisco AMP (Advanced Malware Protection) verfügt die Lösung über erweiterte Funktionen zum Schutz vor Spam und betrügerischen Absendern, schädlichen Dateien und potenziell gefährlichen URLs. Darüber hinaus umfasst Cisco Email Security Retrospective Security,

Cisco Email Security kombiniert mehrere Sicherheitsebenen zur Minderung des Risikos ausgehender Bedrohungen.

Cisco SecureX Plattform

Cisco Email Security ist Teil der Cisco Sicherheitsplattform SecureX, die für eine einheitliche Transparenz sorgt. SecureX ist ein plattformbasierter Ansatz zur Erfüllung der aktuellen und zukünftigen Sicherheitsanforderungen mit Lösungen, die sämtliche Bedrohungsvektoren und Eintrittspunkte abdecken. Die Sicherheit erhöht sich im gesamten Netzwerk, an den Endgeräten, in der Cloud und in den Anwendungen durch:

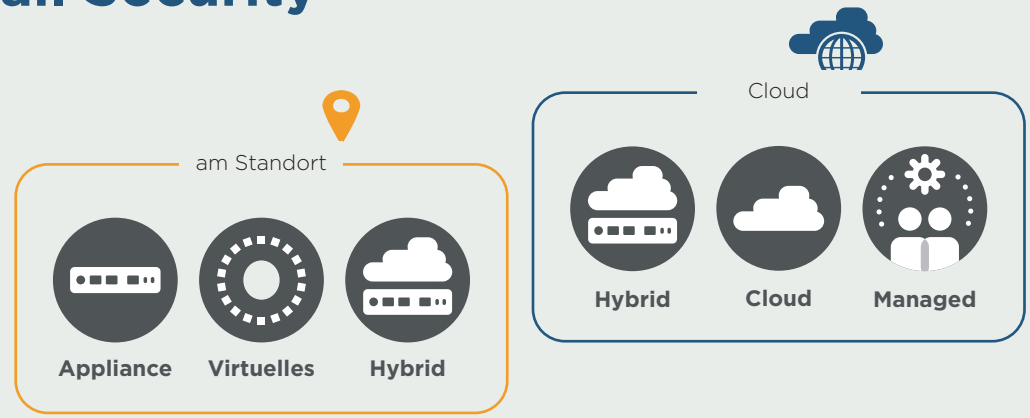
Vereinheitlichung der **Sichtbarkeit** über die gesamte Sicherheitsinfrastruktur, um schneller auf Bedrohungen reagieren zu können

Automatisierung kritischer Sicherheits-Workflows. Die Zusammenarbeit von SecOps, ITOps und NetOps ermöglicht eine Harmonisierung der Sicherheitsrichtlinien.

Komplexität reduzieren und Portfoliovorteile maximieren durch Integration weiterer Komponenten des Cisco Security Portfolios in die bestehende Infrastruktur.

Bereitstellungsoptionen für Cisco Email Security

Cisco Email Security kann vor Ort, in der Cloud oder als Hybridmodell bereitgestellt werden, wobei die Kunden jeweils dieselbe Codebasis mit den gleichen aktivierten Funktionen erhalten. Dank einfacher Einrichtung der Lösung und Automatisierung wird der Schutz innerhalb weniger Minuten gewährleistet. Abonnements sind ab einer Größenordnung von 100 Benutzern erhältlich.



Auswahl der Appliances

Unternehmensgröße	Email Security Appliance (ESA)	Virtuelle Appliance (ESAv) – Spezifikation (ESXi / KVM)	Management Appliance (SMA)	Virtuelle Appliance (SMAv) – Spezifikation (ESXi / KVM)
Evaluierung & Test		**C000v** (Evaluation only) • 200 GB HDD • 4 GB Memory • 1 CPU Kern		**M000v** (Evaluation only) • 250 GB HDD • 4 GB Memory • 1 CPU Kern
Kleine Unternehmen / Zweigstellen	• ESA-**C195**-K9 • Smart Net Total Care Services (SNTC) • CCS-PSU1-770AC= (**Redundant Power Supply** 770W für x95 Appliance)	**C100v** (bis 1.000 User) • 200 GB HDD • 6 GB Memory • 2 CPU Kerne	• SMA-**M195**-K9 • Smart Net Total Care Services (SNTC) • CCS-PSU1-770AC= (**Redundant Power Supply** 770W für x95 Appliance)	**M100v** (bis 1.000 User) • 250 GB HDD • 6 GB Memory • 2 CPU Kerne
Mittlere Unternehmen / Niederlassungen	• ESA-**C395**-K9 • Smart Net Total Care Services (SNTC)	**C300v** (bis 5.000 User) • 500 GB HDD • 8 GB Memory • 4 CPU Kern	• SMA-**M395**-K9 • Smart Net Total Care Services (SNTC)	**M300v** (bis 5.000 User) • 1.024 GB HDD • 8 GB Memory • 4 CPU Kerne
Großunternehmen und Service Provider	• ESA-**C695**-K9 / ESA-**C695F**-K9 (Fiber Interface) • Smart Net Total Care Services (SNTC)	**C600v** (User: Sizing erforderlich) • 500 GB HDD • 8 GB Memory • 8 CPU Kerne	• SMA-**M695**-K9 / SMA-**M695F**-K9 (Fiber Interface) • Smart Net Total Care Services (SNTC)	**M600v** (User: Sizing erforderlich) • 2.032 GB HDD • 8 GB Memory • 8 CPU Kerne

TIP

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

Um zentralisierte Email-Reports und Spam-Quarantänen sowie DLP Policies an einem einzigen Standort bereitzustellen, wird eine Management Appliance mit entsprechender Lizenz benötigt (Gilt nicht bei einem Cloud Deployment). Siehe SMA Seite 5 unten.

Bereitstellungsoptionen für Cisco Email Security

Cisco Email Security Bundles	Beschreibung	On-Prem Lizenzen für ESA oder ESAv	Cloud Lizenzen für CES	Hybrid Lizenzen für ESA / ESAv + CES
Inbound mit Advanced Malware Protection	**Schutz gegen Spam, Viren und zielgerichtete Attacken** Anti-Spam Scanning, Sophos Anti-Virus, Outbreak Filters, Forged Email Detection, Advanced Malware Protection (Reputation, Threat Grid Sandboxing) » 100 - 9.999 User, Sandbox-Limit von 200 Datei-Uploads pro Tag » 10K - 49.999 User, Sandbox-Limit von 2.000 Datei-Uploads pro Tag » 50K+ User, Sandbox-Limit von 6.000 Datei-Uploads pro Tag	EMAIL-SEC-SUB • ESA-ESI-AT-LIC	EMAIL-SEC-SUB • CES-ESSN-AMP-BNDL	EMAIL-SEC-SUB • H-ESA-ESI-AT-LIC • CES-ESSN-AMP-BNDL
Premium mit Advanced Malware Protection	**Schutz gegen Spam, Viren und zielgerichtete Attacken und Hilfe bei der Erfüllung von Compliance Anforderungen** Anti-Spam Scanning, Sophos Anti-Virus, Outbreak Filters, AMP (Reputation, Threat Grid Sandboxing) + Data Loss Prevention, Email Encryption (Cisco Registered Envelope Service) » 100 - 9.999 User, Sandbox-Limit von 200 Datei-Uploads pro Tag » 10K - 49.999 User, Sandbox-Limit von 2.000 Datei-Uploads pro Tag » 50K+ User, Sandbox-Limit von 6.000 Datei-Uploads pro Tag	EMAIL-SEC-SUB • ESA-ESP-AT-LIC	EMAIL-SEC-SUB • CES-PREM-AMP-BNDL	EMAIL-SEC-SUB • H-ESA-ESP-AT-LIC • CES-PREM-AMP-BNDL
Inbound	**Schutz gegen Spam, Viren und zielgerichtete Attacken** Anti-Spam Scanning, Sophos Anti-Virus, Outbreak Filters, Forged Email Detection	EMAIL-SEC-SUB • ESA-ESI-LIC	EMAIL-SEC-SUB • CES-ESSENTL-BNDL	EMAIL-SEC-SUB • H-ESA-ESI-LIC • CES-ESSENTL-BNDL
Outbound	**Hilfe bei der Erfüllung von Compliance Anforderungen** Data Loss Prevention, E-Mail Encryption (Cisco Registered Envelope Service)	EMAIL-SEC-SUB • ESA-ESO-LIC	EMAIL-SEC-SUB • CES-OUTBOUND-BNDL	EMAIL-SEC-SUB • H-ESA-ESO-LIC • CES-OUTBOUND-BNDL
Premium	**Schutz gegen Spam, Viren und zielgerichtete Attacken und Hilfe bei der Erfüllung von Compliance Anforderungen** Anti-Spam Scanning, Sophos Anti-Virus, Outbreak Filters, Data Loss Prevention, E-Mail Encryption (Cisco Registered Envelope Service)	EMAIL-SEC-SUB • ESA-ESP-LIC	EMAIL-SEC-SUB • CES-PREMIUM-BNDL	EMAIL-SEC-SUB • H-ESA-ESP-LIC • CES-PREMIUM-BNDL
Inbound O365	Anti-Spam Scanning, Virus Outbreak Filters, ohne Anti-Virus-Engine	–	EMAIL-SEC-SUB • CES-O365ESS-BNDL	–
Premium O365	Anti-Spam Scanning, Outbreak Filters, Data Loss Prevention, E-Mail Encryption (Cisco Registered Envelope Service), ohne Anti-Virus-Engine	–	EMAIL-SEC-SUB • CES-O365PREM-BNDL	–

TIP Die Anzahl der User entspricht der unique Mailboxen.

Auswahl zusätzlicher oder einzelner Features

Einzelne Features	Für Inbound Bundle	Für Premium Bundle	Für Outbound Bundle	Beschreibung	On-Prem Lizenzen für ESA oder ESAv	Cloud Lizenzen für CES	Hybrid Lizenzen für ESA / ESAv + CES
Advanced Malware Protection (AMP) Basic Add-On	optional	optional	–	Schutz vor fortgeschrittenen Bedrohungen wie z.B. individuell erstellter Malware. Erweiterung für Inbound und Premium. » 100 - 9.999 User, Sandbox-Limit von 200 Datei-Uploads pro Tag » 10K - 49.999 User, Sandbox-Limit von 2.000 Datei-Uploads pro Tag » 50K+ User, Sandbox-Limit von 6.000 Datei-Uploads pro Tag	EMAIL-SEC-SUB • ESA-AMP-LIC	EMAIL-SEC-SUB • CES-AMP	EMAIL-SEC-SUB • ESA-AMP-LIC • CES-AMP
Antispam	im Paket enthalten	im Paket enthalten	optional	Schutz vor unerwünschten Spam E-Mails, unerwünschten Massen- und Marketing E-Mails (auch bekannt als Graymail)	EMAIL-SEC-SUB • ESA-AS-LIC	–	–
Anti-Virus (Sophos)	im Paket enthalten	im Paket enthalten	optional	Leistungsstarker Schutz vor Virenangriffen per E-Mail.	EMAIL-SEC-SUB • ESA-SO-LIC	–	–
Data Loss Prevention (DLP, Add On für Inbound)	optional	im Paket enthalten	im Paket enthalten	DLP verhindert das Verlassen vertraulicher und sensibler Daten aus dem Unternehmensnetzwerk.	EMAIL-SEC-SUB • ESA-DLP-LIC	EMAIL-SEC-SUB • CES-DLP	EMAIL-SEC-SUB • ESA-DLP-LIC • CES-DLP
Encryption (Add On für Inbound)	optional	im Paket enthalten	im Paket enthalten	Sicheres und leistungsstarke E-Mail-Verschlüsselungssystem zur Erfüllung von Compliance Anforderungen	EMAIL-SEC-SUB • ESA-ENC-LIC	EMAIL-SEC-SUB • CES-ENCRYPTION	EMAIL-SEC-SUB • ESA-ENC-LIC • CES-ENCRYPTION
Graymail Safe-Unsubscribe (AddOn für Inbound)	optional	optional	–	Möglichkeit unerwünschte E-Mails abzubestellen, bei gleichzeitigem Schutz vor Bedrohungen oder Phishing-Attacken durch sichere „Unsubscribe“ Links.	EMAIL-SEC-SUB • ESA-GSU-LIC	EMAIL-SEC-SUB • CES-SAFEUS	EMAIL-SEC-SUB • ESA-GSU-LIC • CES-SAFEUS
Image Analyzer (Add On für Inbound)	optional	optional	–	Das Email Security Image Analyzer Add-On ermöglicht das Scannen nach nicht jugendfreien Inhalten in Bildern, die in E-Mails enthalten sind. Wird und oft zusammen mit DLP eingesetzt.	EMAIL-SEC-SUB • ESA-IA-LIC	EMAIL-SEC-SUB • CES-IMAGE	EMAIL-SEC-SUB • ESA-IA-LIC • CES-IMAGE
Intelligent Multi-Scan (AddOn für Inbound / Premium)	optional	optional	–	Intelligent Multi-Scan bietet zusätzliche Antispam-Klassifizierungsfunktionen zur Erhöhung der Spam-Erkennungsrate.	EMAIL-SEC-SUB • ESA-IMS-LIC	EMAIL-SEC-SUB • CES-IMS	EMAIL-SEC-SUB • ESA-IMS-LIC • CES-IMS
McAfee AntiVirus (AddOn zu Inbound und Premium)	optional	optional	–	Besserer Virenschutz durch zusätzliches Scannen mit der McAfee AV-Engine. Im Lieferumfang der Inbound bzw. Premium Bundles ist die Sophos AV-Engine.	EMAIL-SEC-SUB • ESA-MFE-LIC	EMAIL-SEC-SUB • CES-MCAFEE	EMAIL-SEC-SUB • ESA-MFE-LIC • CES-MCAFEE
Outbreak Filters	im Paket enthalten	im Paket enthalten	optional	Untersuchung ein- und ausgehender E-Mails auf deren Bedrohungspotential und Erstellung eines Threat-Scores mit temporärer Weiterleitung auf einen Quarantäne-Server.	EMAIL-SEC-SUB • ESA-OF-LIC	–	–
Die Cisco Security Management Appliance (SMA) vereinfacht die Administration von mehreren Cisco E-Mail Security Appliances. Mittels des flexiblen Management-Tools werden Änderungen und Einstellungen zentral an einer Stelle und nicht auf den einzelnen Geräten verwaltet. Spam E-Mails werden bspw. zentral in einer Spam Quarantäne gespeichert.							
E-Mail Security Management (on Prem)	optional	optional	–	Zentrales E-Mail Reporting + Message Tracking + zentralisierte Quarantäne für mehrere E-Mail Appliances.	EMAIL-SEC-SUB • SMA-EMGT-LIC	nicht erforderlich	EMAIL-SEC-SUB • SMA-EMGT-LIC

Ergänzende Services

Cisco Security Awareness

Cisco Security Awareness (CSA) ist ein Cloud-Service, der Kunden dabei unterstützt, automatisierte Sicherheitssimulationen und -schulungen für Endbenutzer durchzuführen und so die Einhaltung von Sicherheitsvorschriften zu erreichen. Es werden 40 verschiedene Sprachen unterstützt. Ein Trial für 100 Benutzer kann für 45 Tage angefordert werden.

Beschreibung	SKUs
Cisco Security Awareness Laufzeit 1, 3 oder 5 Jahre.	SA-SEC-SU • SA-SS-LIC • SA-SLT-LIC
Simulation only Dies ist vor allem für Kunden gedacht, die nur Quizze und Simulationen für Endbenutzer erstellen möchten, um zu testen, ob diese potentielle Spam-E-Mails, schadhafte Anhänge oder Links öffnen. Zu Compliance Zwecken werden Berichte bereitgestellt.	L-SA-SS-LIC=
Simulation + Training Select Dies ist für Kunden gedacht, die das gesamte Endbenutzer-Quiz und die Simulation automatisieren möchten, gefolgt von gezielten videobasierten Schulungen. Die Kunden erhalten die Möglichkeit, 12 beliebige Themen aus jeder Kategorie auszuwählen und sie ihren Endbenutzern zur Verfügung zu stellen.	L-SA-SLT-LIC=

Advanced Phishing

Cisco Advanced Phishing Protection (APP) ist ein Cloud-Service, der auf Täuschung basierende Angriffe wie Social Engineering, Business Email Compromise (BEC) und Betrüger identifiziert und stoppt. Verwendet wird eine Kombination aus Rapid DMARC, Advanced Display Name Protection und Lookalike Domain Erkennung.

Beschreibung	Für On-Prem (ESA / ESAv)	Für Cloud (CES)
Cisco Advanced Phishing Protection (CAPP) CAPP ist ein Cloud-Service, der Angriffe durch Identitätsbetrug über Social Engineering, Hochstapler und Business Email Compromise (BEC) verhindert. Einsatz idealerweise hinter dem Cisco E-Mail Security Gateway.		
Cisco Advanced Phishing Protection mit On-Prem Sensor Für Kunden mit lokalem E-Mail Gateway/Postfach. E-Mails bleiben On-Prem, nur Metadaten werden mit der Cloud ausgetauscht.	L-ESA-APP-LIC=	–
Cisco Advanced Phishing Protection mit Cloud Sensor (E-Mails gehen in die Cloud zur Advanced Phishing Protection) Für Kunden mit lokalem E-Mail Gateway/Postfach bzw. Cloud Email Security.	L-ESA-APPC-LIC=	L-CES-APPC-LIC=
Cisco Email Domain Protection und Cloud Adv Phishing Protection Service Einjähriger Service, der dem Kunden einen dedizierten Experten zur Verfügung stellt.	L-EML-DPAP-SVC=	L-EML-DPAP-SVC=

Domain Protection

Cisco Domain Protection (DMP) ist ein Cloud-Service, der dazu beiträgt, den Kunden-„Brand“ zu schützen, indem verhindert wird, Phishing-E-Mails über eine oder mehrere Kundendomains zu verschicken. Der Service automatisiert den Prozess der Implementierung des DMARC-Email-Authentifizierungsstandards, um Mitarbeiter, Kunden und Lieferanten besser vor Phishing-Angriffen mit Kundendomains zu schützen.

Beschreibung	Für On-Prem (ESA / ESAv)	Für Cloud (CES)
Cisco Domain Protection (DMP) Cloud-Service, der hilft, den Kunden „Brand“ zu schützen.		
Cisco Domain Protection Für Kunden mit lokalen Postfächern/E-Mail-Gateways bzw. Cloud Email Security	L-ESA-DMP-LIC=	L-CES-DMP-LIC=
Cisco Email Domain Protection und Cloud Adv Phishing Protection Service Einjähriger Service, der dem Kunden einen dedizierten Experten zur Verfügung stellt.	L-EML-DPAP-SVC=	L-EML-DPAP-SVC=

Hersteller Support

Smart Net Total Care - mehr als nur Garantie

- 24x7 Professionelle Unterstützung durch spezialisierte Techniker des Cisco Technical Assistance Center TAC
- Hardware-Austausch bis zu 2 Stunden alternativ mit Vor-Ort-Techniker verfügbar
- Software-Updates und Bug-Fixes des Betriebssystems (IOS)
- Sicherheits- und Produktalarm (Alert-Management-Workflow)
- Personalisierter Support über das Web oder mobile Anwendungen
- Voller Zugriff auf Software-Tools, Online Ressourcen und Online-Support Communities
- Service-Coverage-Management für die effiziente Verwaltung Ihrer Verträge
- Product-Lifecycle-Management für die schnelle Identifizierung Ihrer Produkte, die auslaufen oder nicht mehr unterstützt werden

Die Cisco Standardgarantie umfasst während der Garantiezeit nur Material- und Verarbeitungsfehler - mit einer Fehlerquote von 80% werden die meisten Netzwerkausfälle außerdem von Angestellten verursacht.

Reduzieren Sie Ausfallzeiten durch schnellen, kompetenten technischen Support, flexible Hardwareabdeckung und intelligente, proaktive Gerätediagnosen mit dem Cisco Smart Net Total Care-Service. Ihre IT-Mitarbeiter haben im Technical Assistance Center (TAC) jederzeit Zugang zu Experten von Cisco und genießen ein umfangreiches Angebot an Ressourcen, Tools und Schulungen.

Ihre Vorteile gegenüber einer Standardgarantie

Ihr Vorteil	Priorisierte Ersatzlieferung (innerhalb von 2 Stunden möglich)	24 x 7 x 365 Technische Unterstützung	Software Updates	Exklusiver Zugang zu Tools und Produkt-informationen	Automatisierte Vertrags- und Bestands-verwaltung	Laufzeit frei wählbar
Smart Net Total Care	✓	✓	✓	✓	✓	✓
Cisco Standard-garantie	✗	✗	✗	✗	✗	✗

Anhang

Wie viele User sollen lizensiert werden?
Die Anzahl der User entspricht der Anzahl der unique Mailboxen.

User Band
100-499 User
500-999 User
1000-4999 User
5000-9999 User
10000-24999 User
> 25.000 User

Comstor

Comstor Security Team

security.de@comstor.com
+49 30 346 03 331

Cisco Partner
Distribution Partner