DATENBLATT

FireEye Email Security Server Edition

Adaptiver, intelligenter, skalierbarer Schutz gegen E-Mail-Bedrohungen

HIGHLIGHTS

- Umfassender E-Mail-Schutz vor schädlichen Anhängen, URLs für den Diebstahl von Zugangsdaten sowie Spoofing-, Zero-Day- und mehrstufigen Angriffen
- Unterstützung von Analysen zum Abgleich mit Images der Betriebssysteme Microsoft Windows und Apple macOS X
- Ausführliche E-Mail-Analyse zur Erfassung versteckter Bedrohungen in passwortgeschützten Dateien, verschlüsselten Anhängen und URLs
- Bezug von Echtzeit-Bedrohungsdaten aus der FireEye DTI Cloud
- Bereitstellung von Kontextdaten, die die Priorisierung von Warnmeldungen und die Eindämmung von Bedrohungen erleichtern
- Implementierung in Ihrem Unternehmen, mit integriertem oder verteiltem MVX-Service

Abbildung 1: Integrierte Appliances für Email Security: EX 3500, EX 5500 und EX 8500

Überblick

Der größte Teil des eingehenden Datenverkehrs erreicht Unternehmen per E-Mail. Das macht E-Mail-Systeme verwundbar und damit zu einem Einfallstor für Hacker. Infolgedessen müssen Unternehmen eine steigende Anzahl E-Mail-basierter Bedrohungen abwehren. Dabei werden E-Mails meist eingesetzt, um mit Malware infizierte Dateianhänge in das Zielunternehmen einzuschleusen oder arglose Mitarbeiter zum Besuch von schädlichen Websites zu verleiten, die beispielsweise den Diebstahl von Zugangsdaten ermöglichen. Die Beliebtheit dieser Methode bei Cyberkriminellen ist nicht zuletzt darauf zurückzuführen, dass sich die schädlichen E-Mails genau an das jeweilige Zielunternehmen oder an die jeweilige Zielperson anpassen lassen.

Mit FireEye Email Security können Unternehmen schädliche E-Mails blockieren und das Risiko kostspieliger Sicherheitsverletzungen minimieren. Die Lösung wird unternehmensintern bereitgestellt und zeichnet sich unter anderem dadurch aus, dass sie Angriffe, die auf schädlichen URLs oder Anhängen basieren, äußerst zuverlässig erkennt, isoliert und sofort blockiert, noch bevor die Bedrohungen in die Infrastruktur des anvisierten Unternehmens gelangen. Unsere skalierbare Big-Data-Plattform setzt von Plug-ins erfasste Daten und Kontextinformationen aus diversen Quellen zueinander in Beziehung, um zu ermitteln, ob die in E-Mails enthaltenen URLs schädlich sind oder nicht. Mithilfe der signaturunabhängigen MVX-Engine (Multi-Vector Virtual Execution™) gleicht sie E-Mail-Anhänge

und Links zu URLs mit herunterladbaren Inhalten mit einer umfassenden Kreuzmatrix der Betriebssysteme, Anwendungen und Browser ab. Dadurch fallen bei der Bedrohungserkennung nur wenige nicht relevante Informationen an und es treten kaum Fehlalarme auf.

FireEye verfügt über detaillierte Bedrohungsdaten zu Hackern, die aus den von unseren Experten durchgeführten Bedrohungsuntersuchungen und aus Millionen von Sensoren stammen. Email Security nutzt diese Daten, um Warnmeldungen zu priorisieren und Bedrohungen in Echtzeit zu blockieren.

Darüber hinaus kann Email Security mit FireEye Network Security und Endpoint Security integriert werden, damit Sicherheitsteams einen umfassenderen Überblick erhalten und Maßnahmen gegen kombinierte Angriffe über mehrere Vektoren in Echtzeit koordinieren können.

Schutz vor E-Mail-basierten Bedrohungen

Cyberkriminelle recherchieren ihre Opfer mithilfe der unzähligen persönlichen Daten, die online frei verfügbar sind, bevor sie sich ihr Vertrauen mit Methoden des Social Engineering erschleichen. So können sie praktisch jeden dazu bringen, einen Link anzuklicken oder einen Anhang zu öffnen.

Typische Beispiele sind Spear-Phishing-Angriffe, E-Mails mit gefälschten Absendern und diverse Methoden zum Diebstahl von Anmeldedaten. Im Gegensatz zu den meisten herkömmlichen E-Mail-Sicherheitslösungen erkennt und blockiert FireEye Email Security diese Taktiken in Echtzeit. E-Mails werden analysiert und blockiert (in Quarantäne gesetzt), wenn neue oder komplexe Bedrohungen in Dateianhängen verschiedenster Art gefunden werden, unter anderem in:

- EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4 sowie ZIP-, RAR- und TNEF-Archiven
- passwortgeschützten und verschlüsselten Anhängen
- Anhängen, deren Passwort in Form einer Bilddatei übermittelt wird
- URLs, die in E-Mails, MS-Office-Dokumenten, PDF- und Archivdateien (ZIP, ALZIP, JAR) sowie anderen Dateiarten (UUencode, HTML) eingebettet sind
- über eine URL heruntergeladenen Dateien – und sogar FTP-Links
- verschleierten, gefälschten, verkürzten und dynamisch umgeleiteten URLs
- URLs für Anmeldedaten-Phishing und Typosquatting
- unbekannten Images der Betriebssysteme Microsoft Windows und Apple macOS X, Schwachstellen in Browsern und Anwendungen
- schädlichem Code in Spear-Phishing-E-Mails

Ransomware-Angriffe beginnen zwar mit einer E-Mail, aber vor der Verschlüsselung muss die Ransomware typischerweise eine Verbindung zu einem Command-and-Control-Server herstellen. Email Security erkennt und stoppt diese schwer erkennbaren, mehrstufigen Malware-Kampagnen.

Überlegene Bedrohungserkennung

Email Security hilft Unternehmen dabei, im normalen Internet-Datenverkehr versteckte, komplexe, gezielte und auf die Umgehung von Sicherheitsmaßnahmen ausgelegte Angriffe zu erkennen und zu blockieren und damit das Risiko kostspieliger Sicherheitsverletzungen zu senken. Angriffe werden unmittelbar nach der Aufdeckung gestoppt und analysiert. Dabei wird ein digitaler Fingerabdruck erstellt, damit sich derartige Gefahren in Zukunft schneller erkennen lassen.

Möglich wird dies durch die leistungsstarken Kernkomponenten von Email Security: Advanced URL Defense, die MVX-Engine und MalwareGuard. Diese Technologien nutzen maschinelle Lernverfahren und Analysefunktionen, um Angriffsmethoden zu erkennen, die herkömmliche, auf Signaturen oder Richtlinien basierende Sicherheitsmaßnahmen umgehen.

Ein wichtiger Bestandteil der URL-Sicherheitsfunktionen ist PhishVision, ein Algorithmus zur Klassifizierung von Abbildungen. Dieser erfasst und speichert Screenshots der Websites legitimer, aber häufig angegriffener Marken und vergleicht sie mithilfe von Deep-Learning-Verfahren mit den in E-Mails enthaltenen URLs. Ergänzend zu PhishVision wird das Plug-in Kraken eingesetzt, das Domains und Seiteninhalte analysiert, um Phishing-Angriffe zu erkennen und die maschinellen Lernverfahren zu verbessern. Ein weiteres innovatives Tool zur Erkennung schädlicher URLs ist Skyfeed, ein speziell für diesen Zweck erstelltes, vollständig automatisiertes System, das Informationen über Malware erfasst und speichert. Skyfeed wertet unter anderem Konten in sozialen Netzwerken, Blogs, Foren und Bedrohungsdaten-Feeds aus, um die fehlerhafte Klassifizierung schädlicher Inhalte zu vermeiden. Mit diesem mehrgleisigen Ansatz schützt Advanced URL Defense Unternehmen zuverlässig vor Spear-Phishing-Angriffen und dem Diebstahl von Anmeldedaten.

Dagegen handelt es sich bei MalwareGuard um ein selbstständig lernendes Hilfsprogramm, das Binärdateien analysiert und diesen jeweils eine Kennzahl zuweist, die über den Grad ihrer Verdächtigkeit Auskunft gibt. Jede über das Netzwerk übertragene ausführbare Windows-Datei (Portable Executable, PE) wird von MalwareGuard überprüft. Anschließend wird basierend auf der Kennzahl eine Einstufung vorgenommen und jede auf diese Weise erkannte Bedrohung mit einem Namen versehen.

Die MVX-Engine identifiziert Zero-Day-Exploits, Multi-Flow-Angriffe und andere gut getarnte Angriffe mithilfe einer dynamischen, signaturunabhängigen Analyse in einer sicheren, virtuellen Umgebung. Durch die Aufdeckung bisher vollkommen unbekannter Exploits und Malware-Varianten können Infektionen und Hackereinbrüche rasch unterbunden werden.

Erkennung von Umgehungstechniken

Im Controlled-Live-Modus bietet Email Security eine Funktion zur Abwehr von Angriffen an, die auf der Nutzung von Remote Objects basieren. Die MVX-Engine erkennt Binärdateien, die mehrfach zusätzliche Komponenten herunterladen. Sie lädt die angeforderten Remote Objects herunter und stellt sie für die Analyse bereit. Dadurch

kann die Aufdeckung mehrstufiger Malware-Downloads, raffinierter Spear-Phishing-Angriffe und der Einschleusung von Ransomware erheblich verbessert und die Zahl der Fehlalarme reduziert werden.

Zusätzlich bietet Email Security Schutz vor Angreifern, die versuchen, Technologien zur Identifizierung verdächtiger URLs zu umgehen. Zu diesem Zweck stellt die Lösung in Advanced URL Defense Mechanismen zur Enttarnung von Phishing-Websites bereit, die ständig weiterentwickelt werden. Darüber hinaus können individuell angepasste Guest Images genutzt werden, um Umgehungstaktiken auszuhebeln, die auf der Erkennung von Sandboxumgebungen basieren. Viele dieser Taktiken funktionieren nicht, wenn in der Sandbox eine Endpunkt-Domain, Aktivitäten eines Domainnutzers, Outlook-Daten und Daten zum Verlauf der Browsernutzung reproduziert werden. All das ist mit einem Guest Image möglich.

Aussagekräftige Warnmeldungen für eine wirksamere Bedrohungsabwehr

Email Security analysiert alle Anhänge und URLs, um komplexe Angriffe raffinierter Hacker zu identifizieren. Da die Lösung in Echtzeit mit Daten aus der gesamten FireEye-Installationsbasis aktualisiert wird, kann sie jederzeit Angaben zum mutmaßlichen Urheber einer Bedrohung und andere Kontextinformationen bereitstellen. Damit können Sie die wichtigsten Warnmeldungen identifizieren, rechtzeitig auf sie reagieren und komplexe E-Mail-basierte Angriffe abwehren. Email Security erkennt sowohl bekannte als auch unbekannte Bedrohungen und deckt auch Angriffe auf, bei denen keine Malware vewendet wird. Dabei generiert es nur wenige nicht relevante Informationen und Fehlalarme, sodass Sie Ihre Ressourcen gezielt für die Abwehr tatsächlicher Angriffe einsetzen und so Betriebskosten sparen können. Außerdem ermöglicht die Kategorisierung von Riskware eine genaue Unterscheidung zwischen kritischen Sicherheitsverletzungen und unerwünschten, aber weniger gefährlichen Aktivitäten (z. B. durch Adware und Spyware). Auf dieser Grundlage lassen sich die erforderlichen Gegenmaßnahmen nach Dringlichkeit priorisieren.

Schnelle Anpassung an die sich ständig ändernde Bedrohungslage

Mit Email Security kann Ihr Unternehmen seine Abwehrmaßnahmen gegen E-Mail-basierte Bedrohungen mithilfe des Echtzeitdatenfeeds aus der FireEye DTI-Cloud (Dynamic Threat Intelligence) kontinuierlich und proaktiv stärken. Unsere Lösung setzt alle uns vorliegenden Daten zu Angreifern, Geräten und Opfern zueinander in Beziehung und bietet Ihnen dadurch folgende Vorteile:

- Bereitstellung eines zeitnahen und umfassenden Überblicks über die Bedrohungen
- Identifizierung spezifischer Funktionen und Merkmale erkannter Malware und schädlicher Anhänge
- Bereitstellung von Kontextdaten, anhand derer Abwehrmaßnahmen priorisiert und beschleunigt werden können
- Ermittlung möglicher Identitäten und Motive der Hacker und Nachverfolgung ihrer Aktivitäten in Ihrem Unternehmen
- Modifikation aller in E-Mails enthaltenen verdächtigen URLs, um die Empfänger vor schädlichen Links zu schützen
- Rückwirkende Identifizierung von Spear-Phishing-Angriffen und Blockierung des Zugriffs auf Phishing-Websites durch Hinweise auf schädliche URLs

Integration in die Prozesse zur Bedrohungsabwehr

Email Security lässt sich nahtlos mit FireEye Helix und FireEye Central Management verzahnen.

- Als Teil der Sicherheitsplattform FireEye Helix bietet es einen detaillierten Überblick über die gesamte Infrastruktur. FireEye Helix reichert Warnmeldungen, die per Email oder von Drittanbietern eingehen, mit Bedrohungsdaten an, gibt Tipps für die Untersuchung von Vorfällen und ermöglicht den Abgleich der Prozesse am Endpunkt sowie die Automatisierung von Sicherheitsmaßnahmen. Mit diesen Features und Funktionen versetzt FireEye Helix Ihr Sicherheitsteam in die Lage, unbekannte Bedrohungen aufzudecken und fundierte Entscheidungen zu treffen.
- Central Management gleicht die Warnmeldungen von Email Security und Network Security miteinander ab, um umfassendere Kontextinformationen über den Angriff liefern zu können und die Erstellung von Abwehrregeln zu ermöglichen, die eine Ausbreitung verhindern.
- Durch rollenspezifisches Tagging kann Central Management darüber Auskunft geben, wem ein Angriff gilt.
- Außerdem unterstützt Central Management rollenbasierte Überprüfungs-, Eindämmungs- und Abwehrprozesse bei eingehenden Warnmeldungen.

Weitere Features und Funktionen

Individuelle Anpassung durch YARA-Regeln

FireEye Email Security unterstützt die Erstellung und das Testen eigener Regeln zur Überprüfung von E-Mail-Anhängen auf gezielte, unternehmensspezifische Bedrohungen.

Schutz vor Whaling-Angriffen

Email Security – Server Edition bietet die Möglichkeit, gefälschte E-Mails zu stoppen, die scheinbar von einem Mitglied der Unternehmensführung stammen (Business E-Mail Compromise, BEC). Mithilfe einer Richtlinie werden eingehende E-Mails blockiert, wenn die bei der Übertragung mitgelieferten Angaben zum Namen und zur E-Mail-Adresse des Absenders nicht mit den entsprechenden Daten aus einer genehmigten Whitelist übereinstimmen. Auf diese Weise lässt sich effektiv verhindern, dass wichtige Mitarbeiter Opfer eines Spoofing-Angriffs werden.

Nachrichtenwarteschlange und Management von Warnmeldungen und Quarantäne

Email Security – Server Edition bietet ein hohes Maß an Kontrolle für gescannte E-Mails. Im aktiven Schutzmodus können Nachrichten nachverfolgt und verwaltet werden, die sich in der MTA-Warteschlange befinden. Hier kann anhand von E-Mail-Attributen verifiziert werden, dass Nachrichten empfangen und analysiert wurden und am nächsten Netzwerk-Hop eingetroffen sind. Zugleich lassen sich Trends über ein intuitiv zu bedienendes Dashboard im Zeitverlauf verfolgen, während Zulassungs- und Sperrlisten eine individuelle Kontrolle der E-Mail-Verarbeitung ermöglichen. Darüber hinaus können Warnmeldungen anhand gemeinsamer Attribute gesucht und ausgewählt und ebenso wie Nachrichten im Quarantänebereich stapelweise bearbeitet werden.

Aktiver Schutzmodus oder reine Überwachung

Email Security kann E-Mails analysieren und Bedrohungen isolieren. Im reinen Überwachungsmodus muss eine transparente BCC-Regel eingerichtet werden, damit Email Security Kopien von E-Mails zur Analyse mithilfe der MVX-Engine erhält.

Flexible Bereitstellungsoptionen

Email Security – Server Edition bietet verschiedene Bereitstellungsoptionen für unterschiedliche Unternehmensanforderungen und -budgets:

- **Integrated Email Security:** eine All-in-one-Hardware-Appliance mit integriertem MVX-Dienst zur Sicherung des E-Mail-Eingangspunkts an einem Standort. Bei FireEye Email Security handelt es sich um eine einfach zu administrierende Lösung, die in weniger als 60 Minuten einsatzbereit ist. Dafür ist weder die Erstellung von Regeln und Richtlinien noch eine Anpassung der Konfigurationseinstellungen erforderlich.
- **Distributed Email Security:** erweiterbare Appliances mit zentral genutztem MVX-Dienst zur Sicherung von E-Mail-Eingangspunkten im Unternehmen.
- **Email Smart Nodes:** virtuelle Sensoren, die den E-Mail-Verkehr analysieren, um schädliche Inhalte zu identifizieren und zu blockieren sowie verdächtige E-Mails über eine verschlüsselte Verbindung an den MVX-Dienst für eine detaillierte Analyse weiterzuleiten.
- **MVX Smart Grid:** unternehmensintern installierter, zentraler und flexibler MVX-Dienst, der transparente Skalierbarkeit, integrierte N+1-Fehlertoleranz und automatisiertes Load Balancing bietet.

  Darüber hinaus fungiert das FireEye MVX Smart Grid als Puffer für integrierte Hardware-Appliances, der in Zeiten mit starkem E-Mail-Aufkommen zusätzliche Kapazitäten für die Erkennung und Analyse von in E-Mails versteckten Bedrohungen bereitstellt.
- **FireEye Cloud MVX:** abonnementbasierter MVX-Dienst, der eine datenschutzgerechte Überwachung des Datenverkehrs auf dem Email Smart Node ermöglicht. Nur verdächtige Objekte werden über eine verschlüsselte Verbindung an den MVX-Dienst weitergeleitet, wo sie später umgehend gelöscht werden, falls sie sich bei der Analyse als harmlos erweisen.

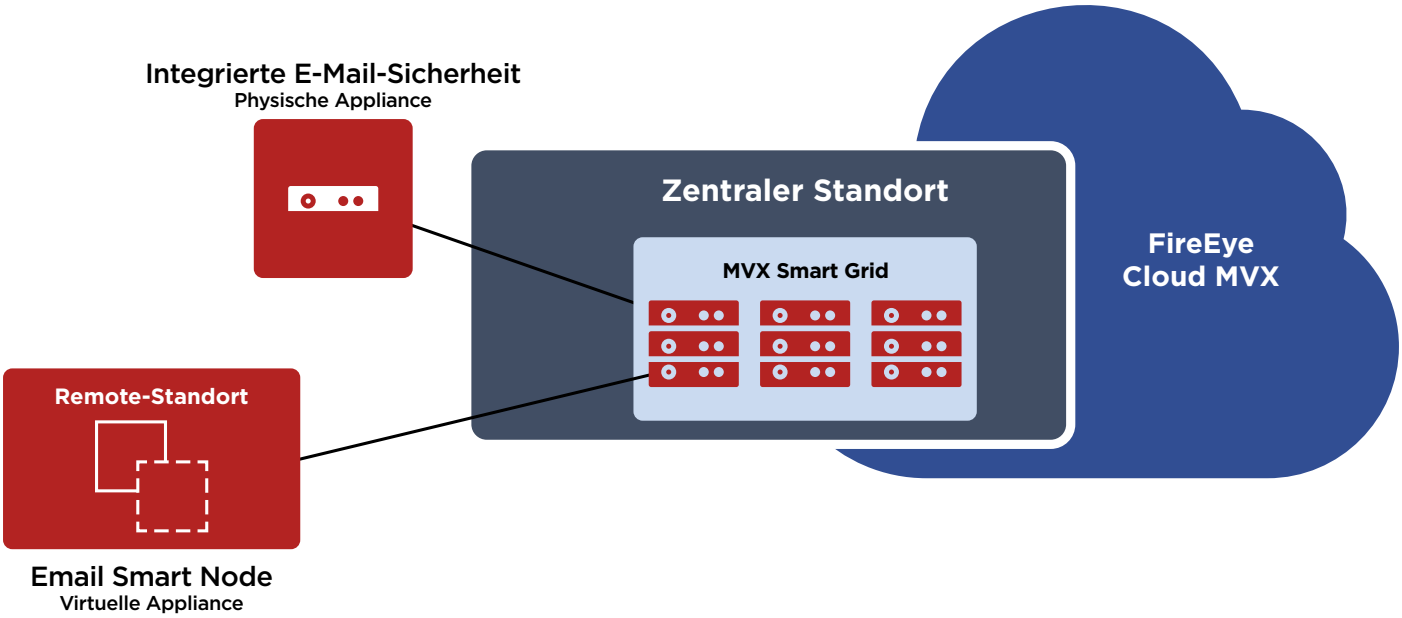

Abbildung 2: Bereitstellung von Email Security im verteilten Modus und im Burst-Modus

Tabelle 1: Technische Daten

	EX 3500	EX 5500	EX 8500
Leistung*	Bis zu 700 individuelle Anhänge/ Std.	Bis zu 1.800 individuelle Anhänge/Std.	Bis zu 2.650 individuelle Anhänge/Std.
Netzwerk-Ports	2 × 1 GigE BASE-T	2 × 1 GigE BASE-T	4 x SFP+ (unterstützt 10GigE Glasfaser, 10GigE Kupfer, 1GigE Kupfer); 2 × 1 GigE BASE-T
Managementports	2 × 1 GigE BASE-T	2 × 1 GigE BASE-T	2 × 1 GigE BASE-T
IPMI-Überwachung	Vorhanden	Vorhanden	Vorhanden
VGA-Port (Rückseite)	Vorhanden	Vorhanden	Vorhanden
USB-Ports	4 USB-Ports Typ A (Rückseite)	je 2 USB-Ports Typ A auf der Vorder- und Rückseite	je 2 USB-Ports Typ A auf der Vorder- und Rückseite
Serieller Port (Rückseite)	115.200 bit/s; keine Parität; 8 Bit; 1 Stoppbit	115.200 bit/s; keine Parität; 8 Bit; 1 Stoppbit	115.200 bit/s; keine Parität; 8 Bit; 1 Stoppbit
Speicherkapazität	4 HDD mit je 2 TB; RAID 10; 3,5 Zoll; FRU	4 HDD mit je 2 TB; RAID 10; 3,5 Zoll; FRU	4 HDD mit je 2 TB; RAID 10; 3,5 Zoll; FRU
Gehäuse	1 HE; passend für 19-Zoll-Rack	2 HE; passend für 19-Zoll-Rack	2 HE; passend für 19-Zoll-Rack
Abmessungen (B × T × H)	437 × 650 × 43,2 mm	438 × 620 × 88,4 mm	438 × 620 × 88,4 mm
Wechselstromanschluss	Redundant (1+1); 750 W bei 100-240 V; 9-4,5 A; 50-60 Hz; Eingang nach IEC 60320-C14; FRU	Redundant (1+1); 800 W bei 100–240 V; 9–4,5 A; 50–60 Hz; Eingang nach IEC 60320-C14; FRU	Redundant (1+1); 800 W bei 100–240 V; 9–4,5 A; 50–60 Hz; Eingang nach IEC 60320-C14; FRU
Gleichstromanschluss	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden
Max. Wärmeabstrahlung	245 W	456 W	530 W
Mittlere Betriebsdauer zwischen Ausfällen (MTBF)	54.200 h	57.401 h	53.742 h
Nettogewicht der Appliance/ Versandgewicht	13,6 kg / 18,6 kg	20,0 kg / 29,6 kg	20,2 kg / 29,8 kg
Erfüllte Sicherheitsstandards	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Erfüllte EMV-Standards	FCC Teil 15 ICES-003 Klasse A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 und V-3/2015	FCC Teil 15 ICES-003 Klasse A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 und V-3/2015	FCC Teil 15 ICES-003 Klasse A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 und V-3/2015
Sicherheitszertifizierungen	FIPS 140-2, CC NDPP V1.1	FIPS 140-2, CC NDPP V1.1	FIPS 140-2, CC NDPP V1.1
Erfüllte Umweltrichtlinien	RoHS-Richtlinie 2011/65/ EU; REACH; WEEE-Richtlinie 2012/19/EU	RoHS-Richtlinie 2011/65/ EU; REACH; WEEE-Richtlinie 2012/19/EU	RoHS-Richtlinie 2011/65/ EU; REACH; WEEE-Richtlinie 2012/19/EU
Betriebstemperatur	0 °C bis ca. 35 °C	0 °C bis ca. 35 °C	0 °C bis ca. 35 °C
Relative Luftfeuchtigkeit bei Betrieb	10 bis ca. 95% bei 40 °C, nicht kondensierend	10 bis ca. 95% bei 40 °C, nicht kondensierend	10 bis ca. 95% bei 40 °C, nicht kondensierend
Maximale Betriebshöhe	3.000 m	3.000 m	3.000 m

* Die tatsächlichen Leistungswerte sind von der Systemkonfiguration und dem verarbeiteten E-Mail-Verkehr abhängig. Es empfiehlt sich, die Größe der Appliance(s) basierend auf der Zahl der pro Stunde zu analysierenden individuellen Anhänge auszuwählen.

Tabelle 2: Technische Daten für FireEye MVX Smart Grid

	VX 5500	VX 12500
Unterstützte Betriebssysteme	Microsoft Windows Apple macOS X	Microsoft Windows Apple macOS X
Leistung*	Bis zu 480 individuelle Anhänge/Std.	Bis zu 3.780 individuelle Anhänge/Std.
Hochverfügbarkeit **	N+1	N+1
Managementports (Rückseite)	1 Port für 10/100/1000 Mbit/s BASE-T	1 Port für 10/100/1000 Mbit/s BASE-T
Cluster-Ports (Rückseite)	3 Ports für 10/100/1000 Mbit/s BASE-T	1 Port für 10/100/1000 Mbit/s BASE-T, 2 Ports für 10 Gbit/s BASE-T
IPMI-Port (Rückseite)	Vorhanden	Vorhanden
LCD-Anzeige und Tastenfeld auf Vorderseite	Nicht vorhanden	Vorhanden
VGA-Ports	Vorhanden	Vorhanden
USB-Ports (Rückseite)	4 USB-Ports Typ A	2 USB-Ports Typ A
Serieller Port (Rückseite)	115.200 bit/s; keine Parität; 8 Bit; 1 Stoppbit	115.200 bit/s; keine Parität; 8 Bit; 1 Stoppbit
Laufwerkskapazität	2 3,5-Zoll-SAS-Festplatten mit je 2 TB; RAID 1; im Betrieb austauschbar; FRU	4 3,5-Zoll-SAS3-Festplatten mit je 4 TB; RAID1; FRU
Gehäuse	1 HE; passend für 19-Zoll-Rack	2 HE; passend für 19-Zoll-Rack
Abmessungen (B × T × H)	437 × 650 × 43,2 mm	437 × 851 × 89 mm
Gleichstromanschluss	Nicht vorhanden	Nicht vorhanden
Wechselstromanschluss	Redundant (1+1) 750 W; 100–240 V; 8–3,8 A; 50–60 Hz; Eingang nach IEC 60320-C14; im Betrieb austauschbar; FRU	Redundant (1+1) 800 W: 100–127 V; 9,8–7 A; 1000 W: 220–240 V; 7–5 A; 50–60 Hz; FRU-Eingang nach IEC 60320-C14; FRU
Maximaler Stromverbrauch	285 W	760 W
Maximale thermische Verlustleistung	285 W	760 W
MTBF	54.200 h	38.836 h
Gewicht Appliance / Versandgewicht	15 kg / 21,8 kg	21 kg / 40,2 kg
Sicherheitszertifizierungen	FIPS 140-2 Level 1, CC NDPP v1.1	FIPS 140-2 Level 1, CC NDPP v1.1
Erfüllte Sicherheitsstandards	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

* Die tatsächlichen Leistungswerte sind von der Systemkonfiguration und dem verarbeiteten Datenverkehr abhängig.

** Mit der erforderlichen redundanten Hardwarekonfiguration

Tabelle 3: Technische Daten für den virtuellen Sensor von FireEye Email Security Smart Node

	EX 5500V
Unterstützte Betriebssysteme	Microsoft Windows, Apple macOS X
Leistung*	Bis zu 1.250 individuelle Anhänge/Std.
Ports für Netzwerküberwachung	2
Netzwerk-Managementports	2
CPU-Kerne	8
Speicher	16 GB
Laufwerkskapazität	384 GB
Netzwerkadapter	VMXNet 3, vNIC
Hypervisor-Unterstützung	VMWare ESXi 6.0 oder höher

* Die tatsächlichen Leistungswerte sind von der Systemkonfiguration und dem verarbeiteten Datenverkehr abhängig.

Mehr Informationen zu FireEye erhalten Sie unter: **www.FireEye.de.**

Telecom Liechtenstein AG
Schaanerstrasse 1
9490 Vaduz / Liechtenstein
security@telecom.li
+423 237 90 90

Über FL1

Als erster konvergenter Full-Service-Provider Liechtensteins ergänzt FL1 damit sein Portfolio sowie sein strategisches Geschäftsfeld um Managed Security Services der nächsten Generation. Im Mittelpunkt steht die zeitnahe Erkennung von Risiken für die Sicherheit der IT von Unternehmen und Behörden als Solution oder als Managed Service. Basis dafür ist eine hochmoderne, eigenentwickelte Technologie- plattform mit welcher Kunden ihr Cyber Defence Centre (CDC) aufbauen können oder die in Kombination mit Security-Analyseexperten, bewährten Prozessen und Best Practices als CDC as a Service zur Verfügung steht.