FORCEPOINT
POWERED BY Raytheon

Datasheet

Forcepoint URL Filtering

PROXYLOSER SCHUTZ VOR BEDROHUNGEN MIT SICHERHEITS-UPDATES NAHEZU IN ECHTZEIT

Forcepoint URL Filtering schützt Ihr Netzwerk und Ihre Ressourcen vor den neuesten Bedrohungen und ermöglicht eine Durchsetzung von Richtlinien für eine produktive Nutzung des Webs. Das System erhält Echtzeit-Sicherheits-Updates von der Forcepoint ThreatSeeker Intelligence. Hierbei handelt es sich um eine Sammlung von mehr als 900 Millionen angebundenen Endpunkten, die auf die Sicherheitsmaßnahmen der Forcepoint Advanced Classification Engine (ACE) zugreifen, um bis zu 5 Milliarden Anfragen pro Tag zu analysieren.

WARUM IST FORCEPOINT IHRE BESTE WAHL?

Forcepoint URL Filtering blockiert Bedrohungen aus dem Web, um die Anzahl der Infizierungen mit Malware und damit auch der Helpdesk-Anfragen zu reduzieren und wertvolle IT-Ressourcen freizusetzen. Mit über 120 Sicherheits- und Filter-Kategorien, Hunderten von Kontrollen für Web-Anwendungen und Protokolle und mehr als 60 individuell anpassbaren Berichten mit rollenbasiertem Zugriff bietet Forcepoint URL Filtering eine leicht zu implementierende und transparente Filter- und Sicherheitslösung, die die Komplexität eines Proxy-Gateways vermeidet.

ECHTZEIT-SICHERHEITS-UPDATES UND DETAILLIERTE RICHTLINIENKONTROLLEN

- Erhält Sicherheits-Updates aus der Forcepoint ThreatSeeker Intelligence fast in Echtzeit. Dies ist eines der weltweit größten Bedrohungsanalyse-Netzwerke, das unter anderem auch Facebook-Inhalte umfasst.
- Bietet branchenführende Richtlinienkontrollen für Sicherheit im Web, mehr als 120 Web-Sicherheits- und Inhaltskategorien sowie Zeitkontingente mit mehreren Authentifizierungsoptionen für Benutzer und Gruppen.
- Benutzerdefinierte Genehmigungs-/Ablehnungsfilter können vorübergehend oder dauerhaft eingesetzt werden und Sicherheitsdaten aus externen Quellen übernehmen.
- Bietet Kontrollen für virale Clips oder Unterhaltungs- und Überwachungsvideos, sowie Unterstützung für YouTube-Schulungsvideos.
- Liefert Hunderte von Kontrollen für Anwendungen und Protokolle sowie eine vollständige Überwachung sämtlicher Ports außerhalb von Proxy-Analysen.

INTEGRIERTES VERWALTUNGS- UND BERICHTSWESEN

- Die integrierte Forcepoint -Benutzeroberfläche vereinfacht die Bereitstellung und ermöglicht ein rollenbasiertes Reporting.
- Umfasst mehr als 60 vordefinierte Berichte, zahlreiche leicht anpassbare Reports, sowie administrative Warnmeldungen.
- Die TRITON Architecture unterstützt eine Erweiterung auf E-Mail-, Daten- oder mobile Sicherheitsprodukte, oder ein Upgrade auf Forcepoint Web Security.

BESTMÖGLICHER SCHUTZ OHNE PROXY

- Sicherheitsdaten aus der Forcepoint ThreatSeeker Intelligence
- Sicherheits-Updates in Echtzeit für aktuellen Schutz und neueste Bewertungen

REDUZIERTE KOMPLEXITÄT

- Transparente Implementierung über die bestehende Netzwerkinfrastruktur
- Implementierung als Appliance oder Software
- Eine einzige Benutzeroberfläche zur Verwaltung der Web-Sicherheit und zusätzlicher Forcepoint-Produkte für E-Mail-, Daten- oder mobile Sicherheit

VERBESSERTER SCHUTZ

- Reduzierung der Anzahl von Malware-Infizierungen und der Risiken eines Datendiebstahls oder einer Rufschädigung
- Reduzierung der Anzahl von Helpdesk-Anfragen und der für das Neuaufsetzen von Systemen benötigten Zeit
- Freisetzung von IT-Ressourcen zur Ermöglichung neuer geschäftlicher Abläufe

ERHÖHTE PRODUKTIVITÄT

- Branchenführende Richtlinienkontrollen, unter anderem mit Zeitkontingenten
- Mehr als 120 Web-Kategorien, einschließlich Videos, Produktivität und Bandbreite

INTUITIVES VERWALTUNGS- UND BERICHTSWESEN

- Ein Satz von vier anpassbaren Dashboards bietet einen umfassenden Überblick über Netzwerkaktivitäten und Bedrohungsniveaus
- Mehr als 60 vordefinierte Berichte für die Anzeige geschäftlicher und technischer Informationen
- Einfache Anpassung, Erstellung und Verteilung von Berichten

„Forcepoint hilft uns dabei, uns jeden Monat gegen Millionen von Online-Angriffen zu wehren und hat die Anzahl von Malware-Infizierungen deutlich gesenkt.“

— Sicherheitsbeauftragter, US-Gesundheitsministerium

Das ThreatSeeker-Netzwerk verwendet die Schutzmaßnahmen der ACE, um jeden Tag 3-5 Milliarden Anfragen auf der Basis unserer verlässlichen Security Labs-Expertise zu analysieren.

Forcepoint ThreatSeeker Intelligence

Die von den Forcepoint Security Labs verwaltete Forcepoint ThreatSeeker Intelligence liefert die zentralen kollektiven Sicherheitsdaten für alle von Forcepoint angebotenen Sicherheitsprodukte. Sie führt mehr als 900 Millionen Endpunkte zusammen und analysiert gemeinsam mit den Schutzmaßnahmen der Forcepoint ACE bis zu 5 Milliarden Anfragen pro Tag. Durch dieses umfangreiche Wissen über Sicherheitsbedrohungen ist die Forcepoint ThreatSeeker Intelligence in der Lage, Echtzeit-Sicherheits-Updates zu liefern, die fortgeschrittene Bedrohungen, Malware, Phishing-Angriffe, Köder und Betrugsversuche blockieren und die neuesten Web-Ratings bieten.

IHRE ANFORDERUNGEN	DIE FORCEPOINT-LÖSUNGEN
Einfache Installation und Verwaltung	Forcepoint Web Security bietet eine transparente, proxylose Implementierung und lässt sich leicht in Ihre bestehende Netzwerkinfrastruktur integrieren.
Echtzeit-Sicherheits-Updates für Schutz vor Bedrohungen	Forcepoint URL Filtering erhält Echtzeit-Sicherheits-Updates aus der Forcepoint ThreatSeeker Intelligence, um Schutz vor den neuesten fortgeschrittenen Bedrohungen sowie vor Malware, Phishing und Betrugsversuchen zu bieten.
Analyse, Verwaltung und Überwachung von Bedrohungsniveaus und Netzwerkaktivitäten	Forcepoint URL Filtering umfasst eine anwenderfreundliche, webbasierte Konsole und Dashboards, die einen vollständigen Überblick über aktuelle Bedrohungsniveaus, Netzwerkaktivitäten und die Durchsetzung von Sicherheitsrichtlinien bieten. Das Berichtswesen ist einfach und intuitiv.
Video-Kontrollen zum Schutz von Netzwerkressourcen sowie Genehmigungs-/ Ablehnungsfilter	Forcepoint URL Filtering ermöglicht das Abspielen von YouTube-Schulungsvideos und bietet Kontrollen für virale Clips oder Unterhaltungs- und Überwachungsvideos. Benutzerdefinierte Genehmigungs-/Ablehnungsfilter können für Sonderereignisse zeitlich beschränkt eingesetzt werden. Sie unterstützen Ausnahmen, um übermäßige Helpdesk-Anfragen zu vermeiden.
Überwachung von Netzwerkports mit Anwendungs- und Protokollkontrollen	Der integrierte Network-Agent bietet eine vollständige Port-Überwachung, einschließlich eines Monitorings des Datenverkehrs außerhalb von Proxy-Analysen. Zudem bietet er Kontrollen für Hunderte von Anwendungen und Protokollen.
Schutz von Remote- und Cloud-Benutzern	Ein optionales Remote-Filtermodul und/oder ein Forcepoint URL Filtering Cloud-Modul ermöglichen Remote-Nutzern den Zugang zum Web bei gleichzeitigem Schutz vor Bedrohungen und einer Durchsetzung von Richtlinien.
Echtzeitschutz vor fortgeschrittenen Bedrohungen	Bei einem Upgrade auf Forcepoint Web Security erhalten Sie Kontrollen für soziale Medien, Untersuchungen von SSL-Datenverkehr, Inline-Echtzeitsicherheit über die ACE und Data Loss Prevention (DLP) sowie ein Dashboard für fortgeschrittene Bedrohungen, das forensische Berichte liefert und versuchten Datendiebstahl bei Sicherheitsvorfällen erfasst.

KONTAKT

www.forcepoint.com/contact

ERFAHREN SIE MEHR

[DATASHEET_FORCEPOINT_URL_FILTERING_DE]-100011DE.030117