FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

Datenblatt

FORCEPOINT
Intrusion Prevention System

Forcepoint bietet das branchenweit sicherste* Intrusion Prevention System (IPS) zum Schutz von verteilten Unternehmensnetzwerken einschließlich Rechenzentren, Büros, Niederlassungen und der Cloud.

*NSS Labs NGIPS Test 2017

Die Netzwerksicherheitslösungen von Forcepoint bieten das sicherste Intrusion Prevention System der Branche. Das in unabhängigen Tests mit der Bestnote ausgezeichnete IPS von Forcepoint kann als eigenständiges Layer 2-IPS-Gerät oder als Teil einer vollständigen Layer 3-Firewall der nächsten Generation (Next Generation Firewall, NGFW) in physischen, virtuellen und Cloud-Umgebungen eingesetzt werden. Das IPS verhindert Umgehungen, Exploit-Angriffe und Malware, mit denen Angreifer in Unternehmensnetzwerke eindringen und sich dort ausbreiten.

Effektivität und hohe Geschwindigkeit dank einzigartiger Architektur

Forcepoint verwendet einen dynamischen, datenstrombasierten Überprüfungsansatz, der über die einfache Packet Inspection hinausgeht. Dabei werden die tatsächlichen Nutzlasten rekonstruiert und untersucht, um Umgehungsmethoden unwirksam zu machen, mit denen Exploit-Angriffe und Malware verschleiert werden sollen.

Zudem werden Angriffe, die sich in SSL/TLS-Datenverkehr verbergen, mithilfe einer detaillierten Hochgeschwindigkeitsentschlüsselung entlarvt. Forcepoint analysiert jeden Datenstrom und entschlüsselt dabei die verschiedenen Protokollschichten auf der Suche nach auffälligen oder manipulierten Protokollkonfigurationen, Metadaten und Headern.

Mithilfe innovativen Methoden werden dann die Übertragungsinhalte von Forcepoint auf Anzeichen für Exploit-Angriffe untersucht, die die Schwachstellen in vielen Systemtypen ausnutzen.
Im Gegensatz zu ausführlichen, musterbasierten Signaturmechanismen können derartige Angriffe dank des ausgefeilteren Ansatzes von Forcepoint in einem einzigen, prägnanten digitalen Fingerabdruck identifiziert werden. Fingerabdrücke werden mithilfe von High-Speed Deterministic Finite Automata (DFA) auf jeden Protokollkontext zugeschnitten. Dadurch können neue Fingerabdrücke nahezu ohne Beeinträchtigung der CPU-Ressourcen ergänzt werden.

Dank kontinuierlicher Updates Angreifern immer einen Schritt voraus

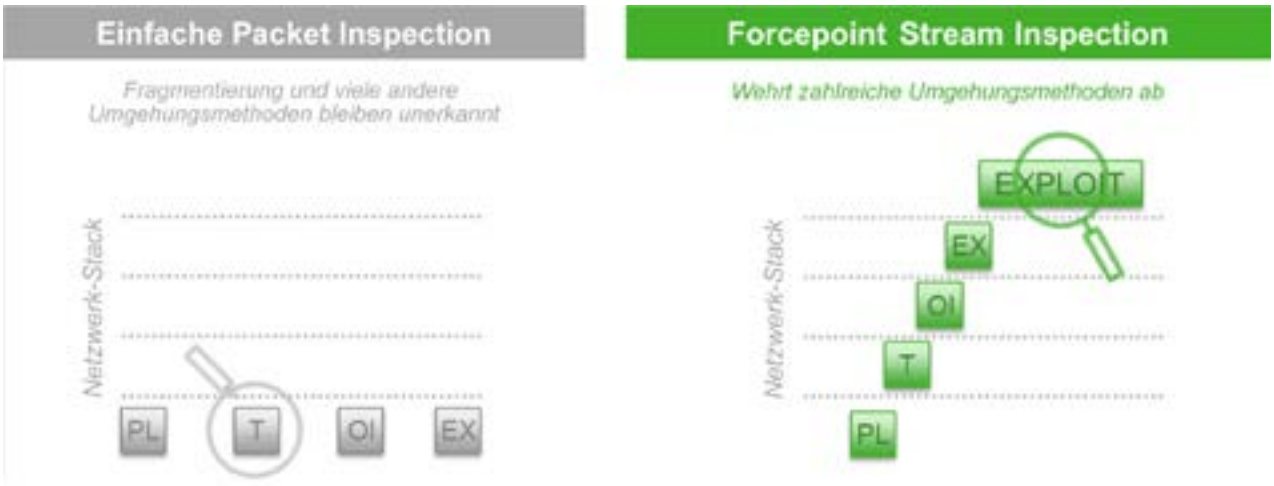
Das weltweit tätige Forschungsteam von Forcepoint ist ständig damit beschäftigt, Feeds mit Bedrohungsdaten, Berichte zu Sicherheitsrisiken aus unterschiedlichen Quellen und eine Vielzahl von Testsystemen zu untersuchen, um Exploit-Angriffe und Schwachstellen zu analysieren. Neue Fingerabdrücke werden nach Bedarf über unseren Cloud-Service veröffentlicht und von Forcepoint Netzwerksicherheitssystemen automatisch heruntergeladen. Durch diesen proaktiven Ansatz haben IT-Teams genug Zeit, um neu veröffentlichte Patches zu analysieren und entsprechende Maßnahmen zur Behebung zu implementieren, ohne einer unmittelbaren Gefahr ausgesetzt zu sein.

Schluss mit Zero-Days und unerwünschten Inhalten

Die Netzwerksicherheitsprodukte von Forcepoint bieten zudem mehrere Verteidigungsebenen vor zuvor unbekannten Angriffen und unerwünschten Inhalten. Übertragene Dateien durchlaufen ein strenges Reputations- und Malware-Scanning. Neue Bedrohungen, wie Zero-Day-Angriffe, können mit unserer fortschrittlichen Sandboxing-Technologie aufgedeckt werden. Forcepoint ist einer der Vorreiter auf dem Gebiet der Kategorisierung und Filterung von Websites und Inhalten. Unsere IPS-Geräte und Firewalls erleichtern es Unternehmen, Arbeitsplatzrichtlinien einzuhalten, die Offenlegung personenbezogener Daten zu beschränken und zu verhindern, dass Benutzer Websites mit gefährlichem Inhalt überhaupt erst besuchen.

Fail-Open-Resilienz

Die Appliances von Forcepoint unterstützen eine Reihe modularer Netzwerkkarten, einschließlich Fail-Open-Schnittstellen, die dafür sorgen, dass der Datenverkehr auch bei einem Leistungsabfall des IPS oder NGFW weiterhin übertragen wird.



FORCEPOINT KOMBINIERT EINE UMFASSENDE REKONSTRUKTION MIT HIGH-SPEED-EXPLOIT-FINGERPRINTING

Schutz für unterbrechungsfreie Geschäftsabläufe

Angreifern fällt es immer leichter, in Unternehmensnetzwerke, Anwendungen, Rechenzentren und Endpunkte einzudringen. Haben sie es einmal geschafft, können sie geistiges Eigentum, Kundendaten und andere vertrauliche Daten entwenden und so Ihr Unternehmen und Ihren Ruf unwiderruflich schädigen.

Bei Internetangriffen geht es nicht mehr nur darum, Systemschwachstellen auszunutzen. Zunehmend werden auch neue Methoden verwendet, um die Erkennung durch herkömmliche Netzwerksicherheitsgeräte zu umgehen, darunter auch viele Firewalls bekannter Marken.

Diese Umgehungsmethoden funktionieren auf mehreren Ebenen, um Exploit-Angriffe und Malware zu verschleiern und sie für die herkömmliche signaturbasierte Packet Inspection unsichtbar zu machen. Durch diese Umgehungen können sogar alte Angriffe, die jahrelang blockiert wurden, jetzt genutzt werden, um interne Systeme zu beschädigen.

Forcepoint verfolgt einen anderen Ansatz. Unsere branchenführende IPS-Engine ist für alle drei Ebenen des Netzwerkschutzes konzipiert. Sie verhindert Umgehungen, erkennt Exploit-Angriffe auf Schwachstellen und stoppt Malware. Die Engine kann transparent hinter bestehenden Firewalls eingesetzt werden, um ohne Betriebsbeeinträchtigung zusätzlichen Schutz zu bieten, oder sie kann als Teil einer vollständigen NGFW als All-in-One-Sicherheitslösung bereitgestellt werden.

Alle Netzwerksicherheitsprodukte von Forcepoint werden ständig aktualisiert, zentral verwaltet und können Sicherheitsrichtlinien und Dashboards in Ihrem gesamten Netzwerk nahtlos nutzen. Mit Forcepoint können Sie die zuverlässige, durchgängige und effiziente Sicherheit in Ihrem Unternehmen in sämtlichen Rechenzentren, Büros, Netzwerken, Niederlassungen und Cloud-Umgebungen sicherstellen.

Vorteile für Ihr Unternehmen

- **Weniger Sicherheitsverletzungen**
- **Mehr Sicherheit ohne Betriebsbeeinträchtigungen**
- **Geringere Gefährdung durch neue Schwachstellen, während IT-Teams neue Patches bereitstellen**
- **Sicherere Bereitstellung in Niederlassungen, Cloud-Umgebungen und Rechenzentren**
- **Niedrigere Gesamtbetriebskosten für Sicherheit und Netzwerkinfrastruktur**

Wichtigste Funktionen

- **Bereitstellung als Layer 2-IPS oder als Teil einer Layer 3-NGFW**
- **Datenstrom-Überprüfung, bei der die tatsächlichen Nutzlasten untersucht werden**
- **Vorreiter im Bereich Umgehungsschutz**
- **Hochgeschwindigkeitsentschlüsselung mit detaillierten Datenschutzkontrollen**
- **Erkennung von Protokollabweichungen und Missbrauch**
- **Exploit- und Malware-Erkennung über Hochgeschwindigkeits-DFA**
- **Denial of Service (DoS)-Erkennung**
- **Botnet-Schutz**
- **Zero-Day-Sandboxing über Cloud oder lokale Appliance**
- **Branchenführende URL-Filterfunktion**
- **Modulare Fail-Open-Netzwerkschnittstellen für Appliances**
- **Einheitliche Funktionen und Performance in allen Installationen**
- **Richtlinienbasierte, zentrale Verwaltung**
- **Schnelle Updates ohne Ausfallzeiten**

Forcepoint Intrusion Prevention System (IPS) – Technische Daten

UNTERSTÜTZTE PLATTFORMEN	
Appliances	Mehrere Serien modularer Appliances zur Bereitstellung in Rechenzentren, an Netzwerkrändern und in Niederlassungen
Cloud-Infrastruktur	Amazon Web Services, Microsoft Azure
Virtuelle Appliance	Auf x86 64 Bit basierende Systeme; VMware ESXi, VMware NSX, Microsoft Hyper-V und KVM-virtualisierte Umgebung
Bereitstellungsmodi	Eigenständiges IPS (Layer 2, mit optionalen Fail-Open-Netzwerkschnittstellenmodulen), als Teil der NGFW (Layer 3)
Virtueller Kontext	Virtualisierung, um logische Kontexte mit separaten Schnittstellen und Richtlinien zu trennen

ÜBERPRÜFUNG	
Mehrstufige Datenverkehrs-normalisierung/Umfassende Deep Inspection	• Rekonstruiert und analysiert tatsächliche Nutzlasten, um die Integrität von Datenströmen sicherzustellen • Löscht duplizierte, untergeordnete Segmente, die beim erneuten Zusammensetzen zu Unklarheiten führen könnten
Umgehungsschutz	Blockiert Fragmente außer der Reihe, überlappende Segmente, Protokollmanipulation, Verschleierung und Verschlüsselungstricks
Erkennung von dynamischem Kontext	Protokoll, Anwendung, Dateityp
Protokollspezifische Daten-verkehrsabwicklung/-prüfung	Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IP-in-IP, IPv6-Einkapselung, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, MSRPC, NetBIOS Datagram, OPC Classic, OPC UA, Oracle SQL Net, POP3, POP3S, RSH, RSTP, SIP, SMTP, SSH, SunRPC, NBT, SCCP, SMB, SMB2, SIP, TCP Proxy, TFTP, integrierte Prüfung mit Sidewinder Security Proxies
Detaillierte Entschlüsselung von SSL/TLS-Datenverkehr	• Hochleistungsentschlüsselung von HTTPS-Client- und Serverdatenströmen • Richtliniengesteuerte Kontrollen, um die Privatsphäre der Benutzer zu schützen und die Offenlegung von personenbezogenen Daten in Unternehmen zu beschränken • Gültigkeitsprüfung von TLS-Zertifikaten und Zertifizieren von Domain-basierten Ausnahmelisten
Erkennung von Exploits für Sicherheitslücken	• Protokollunabhängig, funktioniert mit jedem TCP/UDP-Protokoll mit Protokollierung von Umgehungen und Unregelmäßigkeiten • Virtuelles Patching für client- und serverseitige CVE-Schwachstellen • Intelligenter Fingerprinting-Ansatz, wodurch weniger Signaturen notwendig sind • High-Speed Deterministic Finite Automata (DFA) Matching Engine zur schnellen Erstellung neuer Fingerabdrücke • Kontinuierliche Updates von Fingerabdrücken über Forcepoint
Benutzerdefiniertes Fingerprinting	• Protokollunabhängiger Fingerprinting-Abgleich • Ausdrucksbasierte Fingerprinting-Sprache, die benutzerdefinierte Anwendungen unterstützt
Aufklärung	TCP/UDP/ICMP-Scan, Stealth- und Slow-Scan-Erkennung in IPv4 und IPv6
Botnet-Schutz	• Auf Entschlüsselung basierende Erkennung und sequenzielle Analyse der Nachrichtenlänge • Automatische Aktualisierung der URL-Kategorisierung, um Botnet-Websites zu blockieren oder Benutzer vor solchen Websites zu warnen
Korrelation	Lokale Korrelation, Protokollserver-Korrelation
DoS/DDoS-Schutz	• SYN/UDP-Flood-Erkennung mit gleichzeitiger Verbindungsbeschränkung, schnittstellenbasierte Protokollkomprimierung • Schutz vor langsamen HTTP-Abfragemethoden, halboffene Verbindungsbeschränkung • Trennung von Steuerebene und Datenebene
Blockierungsmethoden	Direktes Blockieren, Verbindungs-Reset, Blacklisting (lokal und verteilt), HTML-Antwort, HTTP-Umleitung
Datenverkehrserfassung	Automatische Datenverkehrserfassung/Auszüge von missbräuchlicher Verwendung
Automatische Updates	• Kontinuierliche dynamische Updates über Forcepoint Security Management Center (SMC) • Aktualisierung von virtuellen Patches und Erkennung und Vermeidung von neuen Bedrohungen

Forcepoint Intrusion Prevention System (IPS) – Technische Daten (Fortsetzung)

ERWEITERTE MALWARE-ERKENNUNG UND DATEIKONTROLLE	
Protokolle	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
Dateifilter	Richtlinienbasierte Dateifilter mit effizientem Einschränkungsprozess. Über 200 unterstützte Dateitypen in 19 Dateikategorien
Dateireputation	Cloud-basierte Hochgeschwindigkeitsprüfung der Malware-Reputation und Malware-Blockierung
Virenscanner für Dateien	Lokale Virenscanner-Engine*
Zero-Day-Sandboxing	Forcepoint Advanced Malware Detection ist sowohl als Cloud-Service als auch als lokaler Service verfügbar, wie er auch von Forcepoint Web Security, Forcepoint Email Security und Forcepoint CASB verwendet wird.

URL-FILTER	
URL-Kategorisierung	Mithilfe von Forcepoint ThreatSeeker Intelligence, wie bei Forcepoint Web Security und Forcepoint Email Security
Automatische Updates	Kontinuierliche Aktualisierung, wenn neue Websites analysiert werden
Durchsetzung kategoriebasierter Zugriffsrichtlinien	Die URL-Filterfunktion von Forcepoint NGFW ist als Add-On-Abonnement verfügbar.

VERWALTUNG UND ÜBERWACHUNG	
Verwaltungsschnittstellen	Zentrales Verwaltungssystem auf Unternehmensebene mit Protokollanalyse-, Überwachungs- und Reporting-Funktionen (weitere Details finden Sie im Datenblatt für Forcepoint Security Management Center)
SNMP-Überwachung	SNMPv1, SNMPv2c und SNMPv3
Datenverkehrserfassung	Tcpdump-Konsole, Remote-Erfassung mittels Forcepoint Security Management Center
Verwaltungskommunikation mit hoher Sicherheit	256-Bit-Sicherheit bei Engine-Verwaltungskommunikation
Sicherheitszertifikate	Common Criteria Network Devices Protection Profile mit Extended Package Stateful Traffic Filter Firewall, FIPS 140-2 Krypto-Zertifikat, CSPN by ANSSI, (First Level Security Certification USGv6)

*Der lokale Malware-Scan ist bei 110/115-Appliances nicht verfügbar.

KONTAKT
www.forcepoint.com/contact

[DATASHEET_FORCEPOINT_TEMPLATE_DE] XXXXXX.062817