Forcepoint

Datasheet

Forcepoint ONE Firewall

Secure all your internet traffic and safeguard against attacks designed to exploit vulnerable branch sites.

Key Benefits

Delivered as a service

- Distribute, update, and enforce new security policies and signatures in real-time.
- Implement automatic scaling (up or down) in a modern cloud architecture, driven by actual usage.
- Reduce cost and shift from high CapEx infrastructure to the cost-saving OpEX cloud architecture.

Increase security with industry-leading IPS capabilities

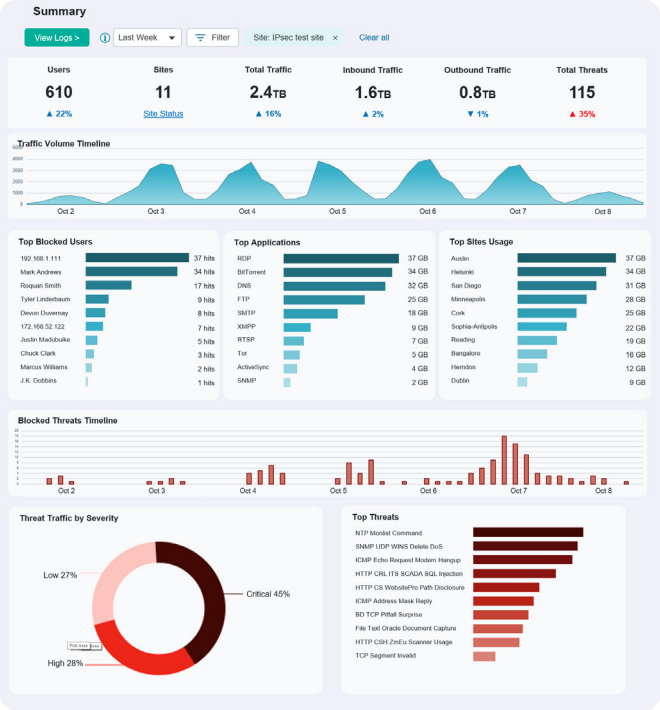
- View early warning signs of potential malicious activity, including zero-day threats and ransomware.
- Protect against Denial of Service (DoS) attacks. Identify known or suspected intrusions, including shell-code attacks.
- Prevent SSL attacks designed to exploit vulnerabilities aimed at leaking confidential information.

Dashboards and reporting

- Quickly spot threats with custom dashboards and reports, gain insights into the users or groups that encounter attacks most frequently.
- Reduce risk by easily identifying trends and patterns of threats.
- Simplify incident investigation by viewing events only associated with a specific incident.

Digital transformation is here: Data and applications reside in the cloud, and users access resources from anywhere, using both managed and unmanaged devices. Yet distributed organizations still rely on legacy firewalls to secure their networks. Cybercriminals are aware of this and are constantly crafting ways to attack the weakest link in the chain, which is often at the branch site.

Safeguard branch sites and remote offices with Forcepoint ONE Firewall. Ensure complete visibility, security and control over all internet traffic to eliminate networking blind spots. Gain peace of mind knowing your network is protected with industry-leading detection accuracy and evasion protection IPS features to protect against advanced threats, including zero-day attacks.



Complete traffic inspection

Forcepoint ONE Firewall delivers traffic inspection capabilities to safeguard against attacks meant to expose vulnerable branch and remote sites that operate with legacy firewalls. Forcepoint ONE Firewall, coupled with Forcepoint ONE SWG, ensures all ports and protocols are inspected. Secure and control all your internet traffic to mitigate security gaps and protect against unconventional port-targeted attacks.

Granular policy management

Forcepoint ONE Firewall gives administrators granular policy management capabilities to increase overall security. Administrators can specify rules based on user(s) and group(s), the service the policy rule governs, and the action to be taken when the policy rule is triggered. Administrators can also rearrange the priority of the policies from top to bottom and assign a default policy to be used in the absence of other policies. With Five- tuple policy control, admins can easily set rules based on protocol, source and destination IP addresses, and source and destination ports, allowing for precise control over network security and traffic. This level of precision enables organizations to establish detailed rules that ensure only authorized and secure communications occur.

Cloud deployment and management

Unlike the cumbersome, expensive and difficult-to-maintain physical appliance firewalls – Forcepoint ONE Firewall is "Delivered as a Service." This SaaS-based solution allows organizations to reduce or eliminate infrastructure and overhead costs associated with procuring, deploying and maintaining traditional physical firewalls at each branch location. With central management, administrators can quickly distribute and enforce the latest security updates and signatures in real time, improving overall security and reducing the risk of data breaches.

Based on reliable industry-leading IPS technology

Forcepoint ONE Firewall goes beyond tackling common network issues; it aalso quickly identifies and mitigates advanced cyber threats. From spotting Denial of Service (DoS) attacks to visibility into SSL attacks (such as Heartbleed), it helps administrators safeguard against attacks on unpatched servers and unmaintained infrastructures. Early warning signs of a network breach are critical to mitigate infiltration and prevent external and unauthorized control of internal resources from information leakage. That's why Forcepoint ONE Firewall detects botnet and anomalous traffic, both early indicators of potential malicious activity, including zero-day threats.

Strong reporting capabilities for informed decisions

Forcepoint ONE Firewall provides various dashboarding and reporting capabilities to ensure administrators are informed with the critical information required to make the right decisions. It offers Time Series charts to view trends and patterns of threats so admins can proactively take action and prevent repeated intrusions. Forcepoint ONE Firewall also provides the ability to see related events in logging to simplify incident investigation by only viewing events associated with a chosen incident. Administrators can generate detailed reports based on identified threats, including known and zero-day threats detected in downloads or uploads, along with insights into the users or groups that encountered them most frequently.

PLATFORMS	
Centralized Management	Enterprise-level centralized management system with log analysis, monitoring and reporting capabilities. See the Forcepoint Security Management Center datasheet for details.
NETWORK SECURITY FEATURES	
5-tuple Policy Control	Create policy based on users/groups, source sites or IP address lists, destination domains or IP address lists, source and destination ports, and protocols
Preconfigured Network Services and Protocols	Hundreds of predefined protocols and protocol agents
User-defined Protocols	Create user-defined protocols to govern internal application behavior
TRAFFIC INSPECTION	
Forcepoint ONE SWG Integration	Integration with Forcepoint ONE SWG for web protection
DNS	DNS threat prevention, protocol enforcement to prevent malicious attacks via DNS queries.
IPS AND THREAT PREVENTION CAPABILITIES	
Deep Packet Inspection	Inspect packet metadata and protocol behavior for suspicious traffic signature pattens
Extensive Catalog of Threat Situations	Guard against tens of thousands of threat situations continually updated via the cloud
Category-based Threat Protection	Enhance threat detection and simplify configuration management
Anomaly-based Detection	Provide early warning signs of potential malicious activity, including zero-day threats, by observing traffic prior to and following attacks
Signature-based Detection	App/protocol/service identification from fingerprinting
DoS Protection	Safeguard the network by identifying Denial of Service attacks, detect threats that attempt to crash unpatched servers and protect unmaintained infrastructures
Disclosure Attacks	Gain visibility into SSL threats attacks (like Heartbleed) designed to exploit vulnerabilities in servers that could leak confidential information, including passwords, encryption keys, user names, source code, directory, configuration, and file contents
Botnet Protection	Detect botnet traffic – an indicator the network has been compromised – and prevent external and unauthorized control of internal resources from data exfiltration
Malware / Antivirus	Detect and prevent threats from services known to demonstrate malicious or undesirable behavior, including spyware, adware and malware
Protocol Violations	Enforces strict compliance for a variety of protocols including TCP, HTTP, DNS, and others
Probes	Prevents scanning activity designed to gather intelligence and identify vulnerabilities
Malicious Routing	Attacks that attempt to misuse network protocols to avoid or bypass security filters