Advanced Threat Protection for HQ and Remote Sites

Improve Network Security for Office Locations with Forcepoint Next-Generation Firewall

Challenge

› Remote workers and HQ sites face increased exposure to sophisticated threats, including ransomware and data breaches, due to fragmented and complex security solutions.

Solution

› Forcepoint NGFW provides threat protection across all locations with an Intrusion Prevention System, deep packet inspection, threat intelligence and behavioral analytics, ensuring real-time detection and prevention.

Outcome

› Organizations gain increased network visibility and threat protection across their distributed environment, leading to improved security and business continuity.

Distributed sites are prime targets for cyberattacks that can compromise your sensitive data, disrupt business operations and harm your reputation. Forcepoint's Next-Generation Firewall (NGFW) offers a comprehensive security solution that provides advanced threat protection across both headquarters (HQ) and remote sites, ensuring continuous protection regardless of location.

As organizations embrace hybrid work environments, securing remote and HQ locations becomes more difficult. Traditional network security models are unsuitable to provide adequate visibility and protection across distributed systems, leaving critical assets vulnerable to advanced threats like ransomware, malware and unauthorized access attempts.

The Challenge: Evolving Cybersecurity Threats

Cybersecurity threats are continuously evolving, becoming more sophisticated and harder to detect. Common challenges faced by organizations include:

→ **Distributed Attack Surface:** As businesses embrace remote work and extend their operations to branch offices, securing a distributed network becomes critical.

→ **Advanced Persistent Threats (APTs):** Threat actors are using more advanced methods, such as multi-stage attacks and evasion techniques, to bypass traditional security defenses.

→ **Insider Threats:** Malicious or negligent insiders, either at the HQ or remote locations, pose significant risks to sensitive data and systems.

→ **Lack of Visibility:** Security teams often struggle with inadequate visibility into network traffic and the lack of centralized control over remote sites.

→ **Complex Security Management:** The growing number of security devices, systems and configurations can overwhelm security operations, increasing the potential for misconfiguration or overlooked vulnerabilities.

The Forcepoint NGFW Advantage

Forcepoint NGFW addresses these challenges with a comprehensive, adaptive security framework that combines technologies to protect both headquarters and remote sites. Its integrated approach delivers robust protection against a wide range of cyber threats, while ensuring ease of use and visibility across distributed environments.
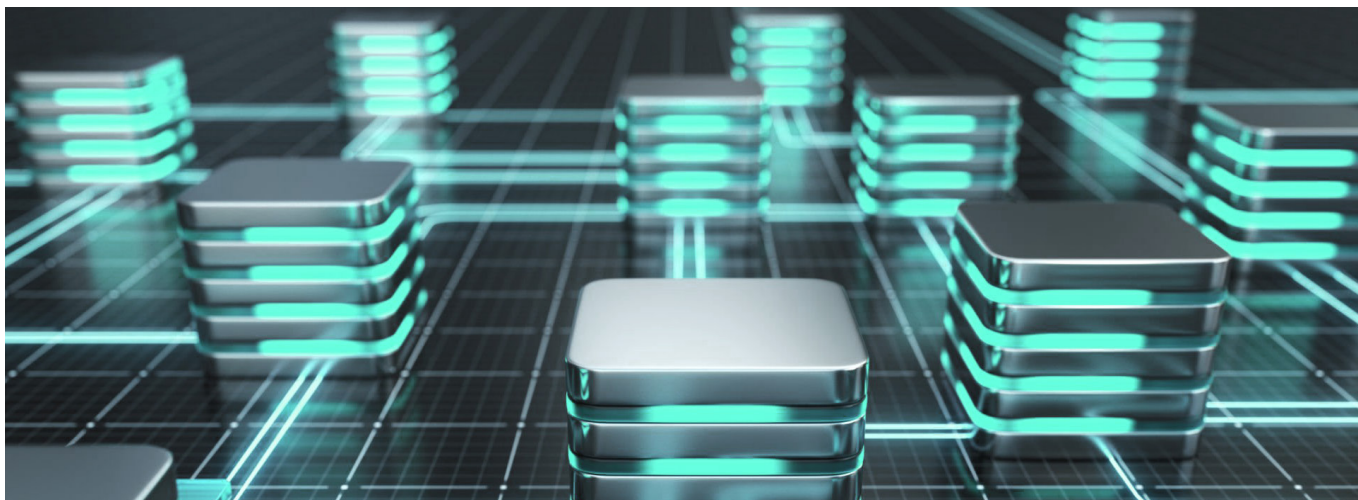
Key Capabilities

Advanced Threat Protection

Forcepoint NGFW includes advanced threat protection capabilities that detect and block modern, multi-stage cyberattacks. These features include:

→ **Intrusion Prevention System (IPS) with anti-evasion defense:** Achieve real-time detection and blocking of known and unknown attacks, including zero-day exploits. It stops out-of-order fragments, overlapping segments, protocol manipulation, obfuscation and encoding tricks.

→ **Multi-layer inspection:** By combining access control, application identification, deep inspection and file filtering, organizations can enhance security and system performance, ensuring robust threat detection and policy enforcement across the network, including remote sites.

→ **Endpoint Context Agent (ECA):** ECA enhances network security by providing detailed visibility into endpoint devices, users and applications, enabling better policy enforcement and threat detection.

→ **Advanced Malware Detection and Protection (AMDP):** Optional sandbox capability protects against malware by sending suspicious files to a virtual environment where they are analyzed for suspicious behavior before being executed on the network.

Seamless HQ and Remote Site Security

Forcepoint NGFW ensures that security is consistently applied across all locations, whether at HQ or remote sites, with the following features:

→ **Centralized Management:** Forcepoint Secure Management Console is a unified console for managing security policies, logs and alerts, providing complete visibility across the network from any location.

→ **Scalability:** Easily scale the deployment from a single HQ to hundreds of remote offices with centralized policy enforcement and distributed performance capabilities.

→ **Zero Trust Network:** Combine Forcepoint Endpoint Context Agent (ECA) with our VPN client to enable secure connectivity for remote workers, ensuring encrypted communications and secure access to corporate resources from anywhere.

Benefits of Forcepoint NGFW for HQ and Remote Sites

1. Comprehensive Threat Visibility & Control

Forcepoint NGFW offers a holistic view of network traffic, providing real-time monitoring, granular control and powerful analytics for detecting, preventing and responding to cyber threats across all sites.

2. Seamless Remote Work Security

As organizations continue to embrace hybrid work models, Forcepoint NGFW ensures remote employees can access corporate resources securely. The solution is designed to provide uninterrupted protection for employees working from various locations while reducing the risk of security breaches.

3. Simplified Security Management

The centralized management capabilities of Forcepoint NGFW simplify the deployment and ongoing maintenance of security policies. Security teams can create, modify and monitor policies across both HQ and remote sites from a single interface, streamlining operations and reducing complexity.

4. Reduced Total Cost of Ownership (TCO)

By consolidating multiple security functions, such as Nex-Gen Firewall, IPS and VPN into a single solution, Forcepoint NGFW reduces the need for multiple point solutions, lowering operational costs and complexity.

Don't let cyber risks prevent business growth

Forcepoint NGFW offers a robust, scalable and intelligent solution to secure both HQ and remote sites from the growing threat landscape. Its advanced threat protection capabilities, Zero Trust framework and centralized management make it the ideal solution for organizations looking to maintain strong security across their entire network, regardless of location. With Forcepoint, businesses can protect their assets, ensure regulatory compliance and confidently support a distributed workforce.

To learn more about Forcepoint NGFW and how it can help your organization, contact us today to **schedule a demo or a consultation.**

forcepoint.com/contact