

HP Network Security Services

Defend networks while streamlining data access

At-a-glance

With technology helping to eliminate traditional barriers to commerce, enterprise networks are increasingly more open. This allows a better flow of information, faster transactions, and more efficient work. But it also leaves your network vulnerable to increasingly sophisticated security threats that are targeting systems and endpoints across local or wide area networks. Perimeter-based defenses are not enough; yet protecting all points against every threat can result in security sprawl—an unwieldy set of products that are expensive, hard to manage, and often result in inconsistent, unreliable security.

HP offers an enterprise-wide, integrated network security solution

HP proactively defends your enterprise network, protecting daily operations, information assets, and intellectual capital. Our policy-driven approach and integrated services consistently manage risk to networks while streamlining appropriate information access and keeping your enterprise up and running.

Unlike point products, the HP integrated network security solution consistently manages the risks to enterprise networks and business systems. Applying our proven, globally consistent network security management approach, HP delivers a solution that is pivotal to securing enterprise data and enabling access to the information necessary for maintaining productivity.

HP Network Security Services includes threat prevention, traffic filtering, event detection/correlation, patch and policy management, and security auditing. This helps to dramatically reduce risks and exposure from internal and external threats such as viruses, worms, malware, and distributed denial of service attacks.

Leverage scale to mitigate risks and ensure access

To keep pace with your ever-changing business and security requirements, HP leverages our scale to ensure risk mitigation and proactive, real-time monitoring and problem resolution.

- HP works with you to create a custom network risk-mitigation strategy that incorporates your business goals and security policies, IT and network requirements, and network vulnerabilities.
- We design an integrated network solution aligned with your business processes and security policies, leveraging HP's cutting-edge network security technologies and proven best practices and processes.
- HP proactively analyzes the threat landscape and identifies emerging trends, enabling rapid and flexible response to the latest security vulnerabilities.
- HP monitors and protects your enterprise network 24x7, relying on our global team of network security specialists strategically placed within our Global Network Operation Centers.



Behind reliable, secure networks, there is HP

You can mitigate risks, meet compliance requirements, and maximize your ROI by leveraging our integrated solution—a package of products, services, and technologies designed to seamlessly work together—and through our consultative expertise that helps you blend existing IT elements to create a more efficient environment:

- Manage your current multivendor network security products through better accountability and a single point of contact.
- Enhance operational and network performance and reduce cost of ownership through HP economies of scale and global delivery infrastructure.
- Ensure network reliability and security that is resistant to disruption or failure, recovers rapidly, and is flexible and scalable.
- Maintain business continuity—even when a network is under attack—through improved detection and response to prioritized security threats, minimizing unplanned network downtime to less than 1%.
- Maximize business value, increase IT effectiveness, and control complexity of the networking infrastructure with HP network life cycle management.
- Mitigate risk during technology evolution through advanced wide-area and enterprise networks and services.
- Scale from simple equipment monitoring to comprehensive network security management and remote site support with dedicated resources.
- Address security audit and compliance requirements based on internal policies and external regulations.
- Minimize lost data and compromised systems from network-based attacks.

HP best practices

To ensure business process alignment and efficiencies within the network infrastructure, HP applies best practices using standardized, repeatable templates and processes and robust network and operational process management mapping to the following:

- Capability Model Maturity Integration (CMMI)
- Enhanced Telecom Operations Map (eTOM)
- Fault, Configuration, Accounting, Performance, Security (FCAPS)—ISO Telecommunications Management Network model and framework
- IT Infrastructure Library (ITIL®)

Enterprise leaders trust HP network security expertise

Leaders of some of the largest, most demanding companies and governments in the world trust HP because we offer better threat detection, superior analysis, and prioritized response to reduce network security risks to operations, data security, and compliance.

- We have more than 5,600 network professionals dedicated 24x7 to meeting the increasingly complex network security requirements of more than 1,000 network clients globally.
- The HP Zero Outage initiative continues to drive network performance improvement year over year, decreasing Sev 1 outages 42% in 2009.
- HP was ranked “Leader” in Gartner’s Magic Quadrant for Communication Outsourcing & Professional Services, Worldwide and North America evaluations.

For more information

Go to www.hp.com/enterprise/ito/networking

Features

- Managed Firewall—is the first line of defense between a corporate intranet and the public Internet.
- Network Intrusion Prevention—prevents security breaches and ensures network availability.
- Managed Remote Access—provides secure, authenticated connectivity to your corporate network for mobile and remote users.
- Managed Proxy Service—automatically establishes or terminates secure connections between Internet-enabled users and productivity-driving applications and information.
- Web Content Filtering—provides scalable access control for inappropriate Internet content.

Share with colleagues

