
MegaPath's Managed Security Services provide comprehensive, multi-layered security that protects your networks and information assets, while maintaining compliance with multiple regulatory needs.

Today, companies of all sizes are facing increasingly difficult odds in protecting their information assets while adhering to continuously evolving compliance requirements. Due to limited budgets, doing more with less has become the norm, and IT teams find it nearly impossible to keep pace.

MegaPath's Managed Security Services are delivered in a SaaS format, which means there is no hardware to acquire, no OEM support contracts to purchase, and services can be provisioned on demand in a matter of minutes—not weeks. Additionally, customers can choose between self-service or fully managed Service Level Agreements (SLAs).

Cloud Based + Premise Based = Defense-in-Depth

MegaPath's SaaS offerings incorporate comprehensive Unified Threat Management (UTM) security services that include Advanced Firewall, Intrusion Prevention, Antivirus, Web Filtering, Anti-spam, Application Control, and Data Leak Prevention. All UTM services can be fully implemented in the cloud, on premise, or in a hybrid configuration to deliver unprecedented, defense-in-depth security.

MegaPath Compliance and Secure Access

While MegaPath's comprehensive UTM services cover a broad range of common compliance requirements, we also offer SaaS versions of managed logging, vulnerability scanning, and security information management that can meet numerous regulatory needs—including PCI DSS, FFIEC / NCUA, HIPAA / HITECH, GLBA, and SOX.

MegaPath is among an elite handful of national providers who can offer a complete range of managed SaaS offerings that can also be fully integrated with access. Our range of access solutions—from DSL, cable, wireless, to our private MPLS network—offers the best-fit access technologies with built-in security and compliance.

Benefits:

- Reduce costs
- Improve security
- Simplify compliance
- Expert support
- 24 / 7 / 365 coverage
- Peace of mind
- One monthly bill

Components of Managed Security Services

MegaPath’s cloud-based and premise-based managed security services provide a comprehensive, multi-layered approach to security that is unmatched in the industry today. Our SaaS offerings work together as a security best practice to eliminate/reduce the risks associated with blended attacks, as well as coordinate security alerting, logging, reporting, compliance and response. Our suite of SaaS offerings include;

Advanced Firewall: Features deep packet inspection with up to 500 firewall policies, configurable by the customer via our secure Web portal; includes periodic and on-demand reporting

Intrusion Prevention: Features multi-layered and blended attack detection for both known and unknown threats with powerful anomaly detection functions to identify and stop zero-day threats; IPS supports all network types, including wireless IPS and rouge wireless detection

Anti-Virus/Anti-Malware: Provides comprehensive real-time network based anti-virus, anti-malware and anti-crimeware detection with both signature and rules-based blocking of known and zero-day attacks

Web Filtering: Manages employee Internet access with white lists/black lists and policy-based content filtering to reduce bandwidth consumption and enforce Internet use policies in real-time

Anti-Spam: Automatically detects spam; optionally tags or deletes spam based upon configurable policy rules before it can consume valuable bandwidth or email storage

Web Application Control: Provides more granular, precise control of specific applications—IM, chat, voice, or video on social media sites, such as Facebook® or MySpace®

Data Loss Prevention: Provides real-time detection and prevention of sensitive data being transferred outside of the organization—including credit card, healthcare, or financial data

Managed Logging: Performs cloud-based log collection, automated daily review, correlation, alerting, reporting and archive, coupled with real-time portal tools for enhanced security operations and compliance

Vulnerability Scanning: Performs on-demand scanning of internal and external IP addresses to identify and remediate vulnerabilities in real time; MegaPath certified quarterly scans for PCI compliance

Security Information Management: Performs portal-based workflow management and tracking required to demonstrate due diligence in meeting organizational security policies and compliance reporting

File Integrity Monitoring: Performs real-time monitoring of critical system or configuration files for unauthorized access or changes; supports Windows®-based POS and server systems

