



## Advantages of Managed Security Services

**Cloud services via MPLS networks  
for high security at low cost**

---

## Executive Summary

### Protecting Your Network and Information Assets

---

Today's distributed organizations are struggling with the increasing sophistication, proliferation, and severity of network security threats. Malware is a daily issue.

With security protection from MPLS-based Managed Security Services (MSS), companies can have cloud-based network protection around the clock against individual and blended threats without incurring the distraction, expense, and complexity of in-house systems and support staff.

Over the past decade, MPLS has evolved into the leading WAN VPN technology primarily because it enables fully managed, cost-effective, and comprehensive unified threat management. Such services have been well designed by managed services providers (MSPs) to meet current and future security challenges—including attack mitigation, anti-malware tools, and Web filtering.

The bottom-line opportunity is for better network security at a lower cost using cloud-based Managed Security Services from MPLS-based MSPs that deliver:

- Fully hosted, managed solutions with no customer premise equipment (CPE)
- Standards compliancy, such as PCI
- Proactive network monitoring
- Deep and broad security protection

---

## Today's Network Security Challenges

Malicious traffic—including viruses, spyware, worms, and service attacks—is malware, and it is a constant threat to a company's network, data, time, and employee productivity. Because it is nearly impossible to stop malware, and it is prolific on the Internet, malware is a constant threat to your computers, data, and critical applications. As these threats continue to grow in sophistication and severity, they can become a major organizational challenge.

Dedicated IT staff for any technical operations issues is in short supply. It is uncommon for companies with fewer than 50 employees to employ a dedicated IT staff person, and the average 100-employee company typically has two IT staffers. Even companies with up to 999 employees typically have no security specialists on staff. For all of these organizations, security threats present real problems, including:

- Complying with security, regulatory, and legislative initiatives
- Growing costs, complexity, and expertise needed to protect data assets
- Needing 24 / 7 / 365 proactive support from a dedicated technical staff

In addition, inappropriate Web surfing in the workplace is an unacceptable use of company resources that lowers productivity and puts pressure on network resources; it also creates potential legal liabilities.

---

## Managed Security Services in the Cloud

With protection from cloud-based Managed Security Services (MSS) via MPLS network-based MSPs, companies can get around-the-clock network protection against individual and blended threats without incurring the distraction, expense, and complexity of in-house systems or security staff. Cloud-based MSS is particularly effective for stopping malicious traffic before it consumes a network's last-mile circuit bandwidth, a job that can't be done with a premise-based solution alone.

---

Managed Security Services are hosted solutions that require no customer premise equipment (CPE), which relieves customer IT organizations of the burden of buying, deploying, and managing firewalls, anti-spam technology, and a host of associated security functions. MPLS networks offer more protection than premise-based solutions can provide alone, require no additional equipment or staff, and include:

- Managed firewalls that detect and block suspicious network traffic
- Proactive intrusion prevention against known and emerging threats
- Anti-virus/anti-spyware comprehensive real-time network protection
- Spam tracking that detects and manages spam on end-user desktops
- Web filtering for managing employee Internet access with white list / black list and content filtering

Managed Security Services increase company productivity by reducing wasted time and resources. MSS stops unwanted traffic before it enters the access circuit by blocking spam, network-based attacks, and bandwidth-consuming traffic.

---

## IT Staff Stats that Matter

33% of small business identified 'information security' as their top IT priority, and that figure increased to 48% amongst midsize companies (source: 2009 CDW Year-In-Review industry survey)

## Did You Know?

Mitigating a virus infection or outbreak requires 2.7 hours of IT staff time per security-related event. When that attack occurs in a non-hosted environment, fixing the same security event requires 14% more time.

---

## Role of the MPLS Network in Managed Security Services Delivery

### A Catalyst for Convergence

MegaPath owns and operates a fiber optic core network that has run MPLS since 1999. The MegaPath network serves over 20,000 customers and 70,000 endpoints with an MPLS-based Tier 1, all-optical IP network. MegaPath operates approximately 30 network points-of-presence (POPs), which are located in fault-tolerant, carrier-grade facilities. The POPs are connected to the network via multiple optical circuits (OCx) for complete redundancy.

All-optical switching technology allows coast-to-coast single hop networking for on-net traffic, which significantly reduces latency as traffic traverses the network. With a redundant path for every connection, traffic is instantaneously rerouted in the event of a network failure, ensuring uninterrupted, high-quality service.

The end result is a powerful, business-class MPLS core network that provides secure multi-site and remote access connections to empower today's distributed enterprises with converged IP data, voice, and video services.

With network connectivity from MegaPath that is available in a variety of access speeds—DSL, T1, business Ethernet—SMBs can select the right speed for the locations they serve. MegaPath has an unrivaled national broadband network footprint that ensures customers always get the right connection at the best price.

Furthermore, our network is protected at a global level from large-scale threats (including zero-day attacks) by a partnership with Fortinet®, a world leader in unified threat management.

---

## Managed Security Services: Protection in the Cloud

Managed Security Services (MSS) from MegaPath deliver comprehensive unified threat management through the network cloud. Built on the company's network of carrier-class gateways, MegaPath Managed Security works as a complete solution and as a complement to existing premise-based security equipment. Its multi-layer security approach safeguards networks and business-critical systems by blocking malicious traffic before it consumes a network's last-mile circuit bandwidth.

### A Fully Managed and Integrated Solution

---

Turnkey solutions should allow customers to protect their business assets, as well as meet regulatory requirements and legislative security initiatives. Any combination of MegaPath MSS can be seamlessly integrated to simplify and unify security management, as well as lower the cost of network security.

Multiple redundant network and security operations centers provide the capability and assurance for MSS services to proactively monitor customer networks. MegaPath MSS complies with selected industry-specific standards—such as PCI for payment card processing—and offers exceptional depth and breadth of security features.

MegaPath services reduce network complexity, and they provide easy and secure access to an increasingly mobile workforce. A unified approach delivers more protection than premise-based solutions can provide alone, and it requires no additional equipment or staff. MegaPath implements, hosts, and monitors solutions around the clock—all for one predictable monthly flat fee.

### Multi-Layer Security Approach

---

Look for a comprehensive multi-layer security approach that minimizes downtime from individual threats, reduces risks associated with blended threats, and coordinates security alerting, logging, and reporting. Service components should include:

- Managed firewall
- Proactive intrusion prevention
- Anti-virus/Anti-spyware
- Spam Tracker
- Web filtering

### Managed Firewall

---

A robust firewall is an imperative first line of defense against intrusions and other threats for any business network. The MegaPath Managed Firewall filters network traffic, allowing good traffic to pass through while blocking potentially harmful traffic. This cost-effective managed solution protects against unauthorized users, dangerous protocols, and common network layer attacks without impacting the network's performance.

MegaPath Managed Firewall is available in a Basic Firewall configuration for small businesses and branch offices, and is available in Advanced Firewall configurations for medium to large businesses. If a company already has an onsite firewall, MegaPath managed services can work in conjunction with the existing firewall and equipment, giving additional protection that a firewall alone doesn't provide.

## Intrusion Prevention

---

With the increased complexity and sophistication of today's security threats, a firewall is not enough to keep networks safe. The MegaPath Intrusion Prevention service constantly monitors network traffic for potential threats to network data. Leveraging a continually updated IPS signature database, MegaPath provides real-time, reliable protection from network and application attacks—such as worms, viruses, Trojans, DoS, DDoS, SQL injections, and other blended threats—without any degradation of network performance.

The Intrusion Prevention service blocks known attacks that don't violate protocol standards or behavioral rules, but do carry malicious content. It offers proactive protection against zero-day attacks and eliminates the window of vulnerability for new and emerging threats when signatures are not available.

## Spam Tracker

---

Detecting and managing spam is a constant problem for businesses. It's a burden to employees and can result in lost productivity and increased frustration. It also clogs email servers, slows network performance, and increases management costs associated with storing and maintaining unwanted email.

The MegaPath Spam Tracker service automatically detects and manages spam in real time on end user desktops and laptops. Once the spam is identified and tagged, it can be directed to a separate email folder, saving your employees' time and your business' money.

## Anti-Virus/Anti-Spyware

---

MegaPath Anti-Virus/Spyware service provides real-time protection against worms and spyware from inbound and outbound security threats. MegaPath leverages a continuously updated list of anti-virus signatures to provide a multi-layer defense from known viruses and new, unique outbreaks. We provide predictive defenses and complementary responsive techniques to stop threats as soon as they emerge on the Internet.

MegaPath Anti-Virus/Spyware service stops unwanted malware before it reaches an organization's network. It minimizes network disruptions caused by virus and worm outbreaks, and responds more effectively to fast-spreading attacks than traditional point and host security solutions. Even if an organization has deployed an anti-virus client, an extra layer of security provides better protection from malicious traffic.

## Web Filtering

---

MegaPath Web Filtering service is an easy way to enforce Internet usage policies and is continually updated to ensure policies include the latest threat protections. The service includes:

- Content Filtering: Blocks access to Internet sites by category content
- White List / Black List Filtering: Allows or denies access to selected Web sites

Separately or in tandem, these services help organizations achieve a balance between managing employee Internet access and enforcing Internet use policies. The result is improved employee productivity, decreased risk of legal liability from employee Internet activity, and optimal use of IT resources.

## Personal Protection Suite

---

MegaPath's Personal Protection Suite provides managed protection for a company's entire distributed workforce. It defends and protects all computers and corporate resources that connect to a company's network from malicious attacks with the following layers of fully managed security:

- Personal firewall with intrusion prevention/detection
- Virus prevention
- Spyware prevention
- Memory protection

The MegaPath Personal Protection Suite provides the security features and benefits of a fully managed service. There is no equipment to buy and only a nominal recurring fee. MegaPath provides installation, configuration, and deployment support, as well as ongoing management and maintenance, including automatic updates. This highly secure, fully managed, and integrated solution saves time, money, and IT resources while reducing the number of threats to your network.

## Implementation Methods

### MegaPath MSS Gateway

---

The MSS Gateway is based on the MegaPath MPLS network, using a security device as the Internet egress point (see diagram below). MegaPath configures the network to filter and scan the inbound and outbound Internet traffic. However, site-to-site traffic within the MPLS network is not scanned.

With MSS Gateway, customers can log on to the portal to view regular reports.

### MegaPath MSS Access

---

The MSS Access solution is based on the MegaPath on-net DSL, T1, or Bonded T1 service. During the provisioning process, MegaPath maps the customer's MSS order to the pre-defined module. Customers receive a welcome letter with information and credentials to access the customer portal. With MSS Access, customers log on to the portal to activate the service and manage its profiles for firewall rules and white list / black list.

If a customer adds MSS to an existing access service, MegaPath provisions MSS and sends a provisioning completion letter to the customer who follows the same process described above to use the service. Once defined, MegaPath monitors and manages the service 24 / 7 / 365. It is that easy.

Furthermore, customers may return to the portal any time to update profiles or generate on-demand reports. Reports are sent to the designated email address for viewing and storage.

## Managed Security Service Advantages

### Provides a Smart Investment in Cost and Risk Avoidance

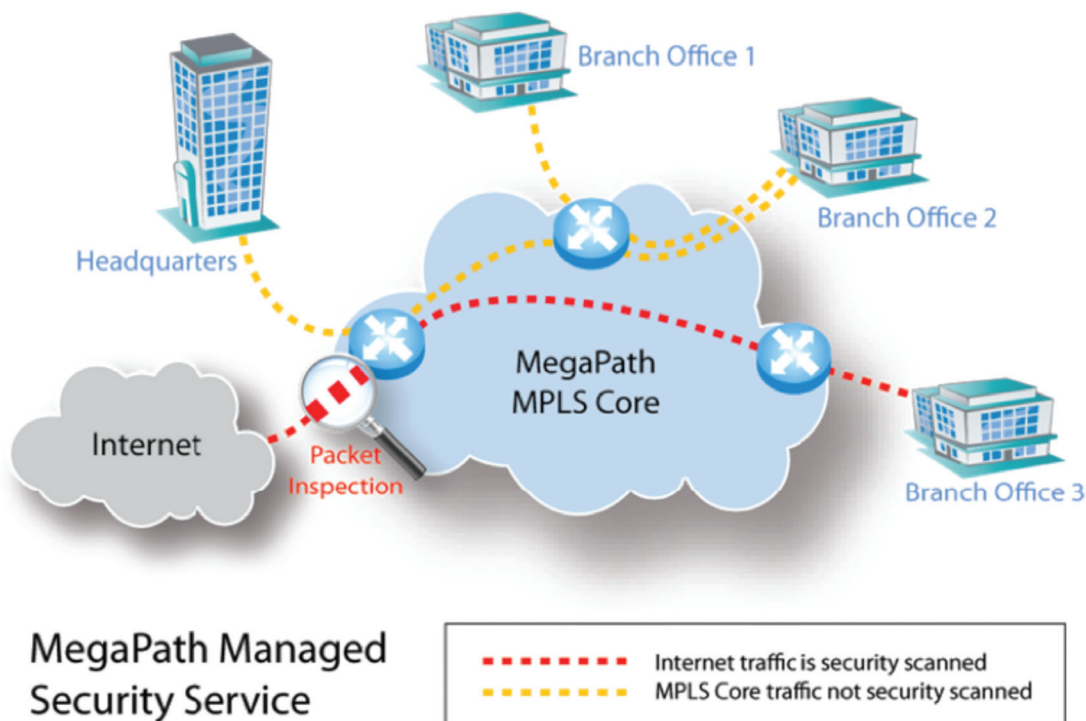
The MegaPath solution filters inbound and outbound Internet traffic at the network edge, thereby protecting all devices on the network, not just computers. It provides an extra layer of security—in addition to security programs that may be installed on individual computers—to protect companies from viruses, spyware, attacks, and visits to unauthorized Web sites.

### Reduces Wasted Time and Resources

MegaPath tags spam and proactively blocks network-based attacks, viruses, worms, and nonproductive Web surfing, providing detailed reports on all security-related network activity.

### Reduces Liability

Potential liability is reduced by preventing access to illegal and harmful Web sites.



## Saves Money

---

MegaPath eliminates the need for dedicated hardware and specialized security staff, while reducing the need for traditional security skill sets. By reducing bandwidth consumption, MegaPath Managed Security service can subsequently reduce required bandwidth, while increasing uptime and employee productivity.

### MegaPath Managed Security Services Benefits

- Turnkey deployment means no additional equipment or staff
- Reduces network complexity by eliminating multiple point solutions
- Lowers total cost of network ownership
- Protects business continuity, company assets, and brand reputation
- Helps maintain compliance with government regulations
- Improves network uptime and performance via 24 / 7 / 365 proactive monitoring and management
- Reduces threat gap via rapid threat solution discovery, development, and automatic updates
- Protects all devices on the network, not just computers
- Increases productivity by blocking spam and non-productive Web surfing
- Eliminates upgrading firewall firmware and anti-virus/intrusion subscriptions

## Notable Advantages

---

- Continually updated signature lists and databases provide aggressive threat identification and elimination
- Comprehensive on-demand reporting helps develop best practices and security policies

## Next Steps

---

Go to <http://www.megapath.com/managed-security/> to learn more about MegaPath Managed Security Services (MSS) solutions.