

O¹ Managed Security Services

Providing Better Security at a Lower Cost

O¹'s Managed Security Services provide continuous monitoring and management with best-in-class security services on a single platform. Our services span Firewall Management & Monitoring, Intrusion Detection & Prevention, Virtual Private Network Access, Anti-Virus, Web Content Filtering and SPAM Filtering.

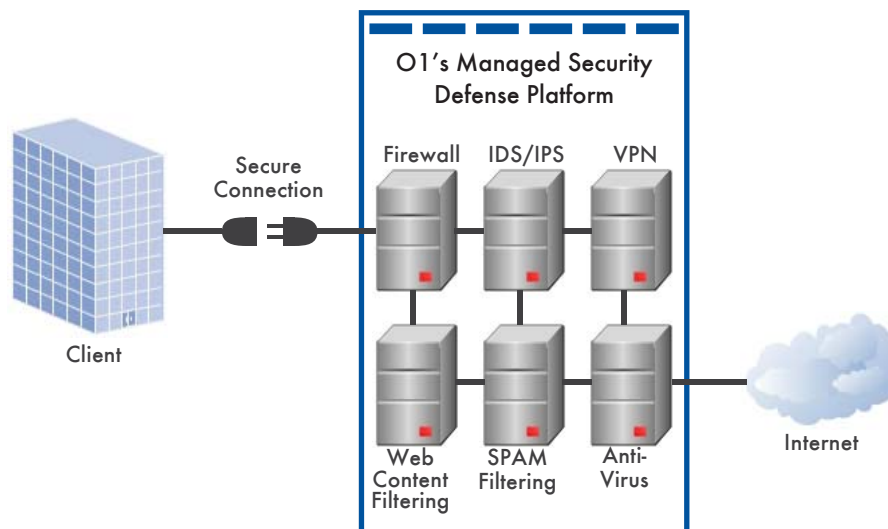
O¹'s innovative platform incorporates all essential security applications and services required to create a safe and clean communications environment. Deployed as an integrated or standalone solution, our Managed Security Services detect and eliminate today's threats as well as emerging blended threats. O¹'s solution lowers cost of ownership by integrating best-of-breed security applications in a single device.

Our device offers real-time network protection systems to support a multi-threat security environment. All inbound and outbound network traffic flows through the device to detect and eliminate content-based threats from email and web traffic such as viruses, worms, intrusions, and inappropriate web content – without degrading network performance.

» Complete Managed Services overview and feature descriptions listed on back

Features

- Real-time network protection system
- Complete scanning of all inbound and outbound network traffic
- Single, customized online system management portal
- Intuitive reporting features for regulatory requirements
- 24x7x365 security operations engineer support available
- Four (4) fully redundant data centers distributed across the nation.



01 Managed Security Services

OSP SERVICE	DESCRIPTION
MANAGED FIREWALL	Your first line of defense against threats aimed at your corporate network. Our service includes ongoing assessments of your firewall and DNS setup, firewall administration (including rule changes), maintenance of traffic flow and firewall reporting. With our service you can be confident that your firewalls are available, performing well and have not been compromised.
INTRUSION DETECTION & PREVENTION	Provides routing, encryption, authentication, and data integrity for secure connectivity across managed IP networks and the Internet. Our service connects remote users, branch offices, suppliers and customers with the cost and performance advantages of public IP networks and the security & control found in private networks.
VIRTUAL PRIVATE NETWORK	Provides the most advanced and complete monitored content security product available on the market today, providing the perfect balance between efficient content security and peace of mind. Our solution allows you to block and monitor all web traffic including sites that reduce productivity, non-business related sites, malicious sites, and sites that create excessive bandwidth utilization. We also use a Ratings Server Database containing millions of restricted web sites and updated continuously to block even the newest malicious sites.
WEB CONTENT FILTERING	Delivers a wealth of reliable and high performance features to detect, tag, quarantine and block SPAM messages and their malicious attachments. Our solution utilizes multiple SPAM detection methods combined with industry leading anti-virus scanning. Quick installation, low maintenance overhead and our 24x7x365 administration provides ease-of-use with a low cost of ownership.
SPAM FILTERING	Allows companies to scan all incoming IP traffic (Web and FTP) as well as inbound outbound email traffic for virus infection. Protecting the network at the point where information enters adds an additional layer of protection to traditional desktop and server-based anti-virus. Desktop virus defense alone cannot protect against viruses spreading in file sharing or peer-to-peer applications because they rely on a read/write operation to launch their scan. OSP Anti-Virus service blocks these memory based threats in addition to traditional malware. Most importantly, network administrators are relieved of the tedious task of updating virus patterns through the use of automatic updates.
ANTI-VIRUS	Allows companies to scan all incoming IP traffic (Web and FTP) as well as inbound/outbound email traffic for virus infection. Protecting the network at the point where information enters adds an additional layer of protection to traditional desktop and server-based anti-virus. Desktop virus defense alone cannot protect against viruses spreading in file sharing or peer-to-peer applications because they rely on a read/write operation to launch their scan. OSP Anti-Virus service blocks these memory based threats in addition to traditional malware. Most importantly, network administrators are relieved of the tedious task of updating virus patterns through the use of automatic updates.

*O1 Managed Security Services refers to security devices that combine multiple protections into a single device. These protections can be Firewall, Anti-Virus, Intrusion Prevention, SPAM Filtering, Virtual Private Network and Web Content Filtering. Not all devices provide all of these protections, and most come with different subscription services to select the features individually or in bundles.