

OneSecure

Managed Security Services



OneSecure
Managed Security
Services offers
Internet security
on demand to
protect you from
the dangers of the
Internet.

eSecurity is constantly evolving. The best way to achieve optimal protection is to layer your network with security services to thwart malicious attacks before they cause any harm. Here are the six basic layers of security that OneSecure managed security services provides:

- ▶ **Firewall:** The basic function of a firewall is to either lock or unlock ports to allow or prevent traffic into your network.
- ▶ **IPS:** Once you have determined which ports you need open and closed on the firewall, you need to monitor the open ports to ensure that malicious traffic is not allowed in the network. Our IPS system uses deep packet inspection to analyze network traffic and block packets known to match thousands of malicious code signatures. If the IPS system detects malicious activity, those packets are blocked from entering your network.
- ▶ **Gateway AV:** Hackers have become more serious in recent years by attaching malicious code to high traffic web sites. Once an unsuspecting visitor clicks on this web site, a virus, worm or other malicious code can be downloaded to the unsuspecting machine. Gateway AV thwarts these attacks by checking all HTTP, HTTPs, SMTP and FTP traffic for malicious code embedded within the traffic and blocks access to infected sites.
- ▶ **Web Content Filtering:** This service helps you implement company policies associated with preventing unauthorized web browsing.
- ▶ **SPAM Filtering:** This service passes all incoming email through a multi-layered SPAM filtering system that blocks or identifies/categorizes inbound SPAM. This processing takes place outside of your network, reducing network traffic and email server processing.
- ▶ **Virtual Private Network:** VPN allows individual employees, remote office locations, and/or suppliers to securely connect to your local area network.

Benefits of on demand internet security for your business

- ▶ Continuously Upgraded
- ▶ Limited Capex
- ▶ On Demand Reporting
- ▶ Avoid Technology Obsolescence
- ▶ Internet Usage Policy/Reporting
- ▶ Integrated Web Portal
- ▶ Protection of Your Assets
- ▶ Control over Your Network
- ▶ 24 x 7 x 365 Monitoring
- ▶ Easy to Use
- ▶ Maximize Employee Productivity
- ▶ Seamless Integration

Key features of Essential Security services

- ▶ Rock Solid Technology
- ▶ Battle Tested Platform
- ▶ Simple Installation
- ▶ Constantly Upgraded
- ▶ Simple Integrated Portal
- ▶ On Demand Reporting
- ▶ Monitored Security 24 x 7 x 365

OneSecure Customer Security Management Portal

1. Security Protection Rating:

Indicates at a glance how current security posture ranks against industry best practices.

2. Security Attack Trends:

Provides trending analysis of attacks against the network over the previous seven days.

3. Attack Log: Functions like an odometer recording total amount of traffic, attacks, viruses, web sites blocked and SPAM blocked since service inception.

4. Incident Alerts: View details of higher level attacks and how they were handled or need to be handled by the end user.

5. News:

Provides current information based on what the provider wants the end user to review.

6. Real Time Activity Detail

(last 7 days): Each individual square functions as a gauge for the indicated security services and delivers mini-reports on network security for the previous seven days.

7. Reporting: 30 reports showing all of your internet activity and attacks.

8. Support: Ability to submit online tickets for service changes and updates.

9. Subscribe: Ability to subscribe to additional services to increase your security rating.

10. Training: Online video describing how to use the portal to maximize your security posture.

11. Locations: If you have more than one location, you can view the activity at other offices within your company.

One integrated view for all your security services

Security Console

TelePacific COMMUNICATIONS

Dashboard Reporting Support Subscribe Training Logout Locations: Cooper City (Demp Device)

1 Security Protection Rating

2 Security Attack Trends

3 Attack Log (Since inception: 00/00/00)

FIREWALL	109,637,375 Traffic Allowed
IPS	1,605,719 Attacks Blocked
GATEWAY AV	389,749 Viruses Blocked
ANTI-SPAM	18,153 Viruses Blocked
DESKTOP AV	2,445 SPAM Blocked
WEB FILTER	329 Websites Blocked

4 Incident Alerts

Attack Name	Count
BufferOverflow.B	23
html.Access	2
Checksum.Bypass	15
Disclosure.SHTML	6
dos:Windows Ani.File.DoS.C	1

5 News

Microsoft security updates for August 2006
Microsoft August 2006 security update[s] affect Microsoft Windows and Microsoft Office.
Published: 8/8/2006

6 Real Time Activity Detail (Last 7 days)

Intrusion Defense

Firewall (Top Sites Analyzed)

Details	Count
Total Inbound Traffic	1,302,750
Total Outbound Traffic	17,528,342
Top Country	U.S.A.
Top Web Destination	www.google.com
Top Protocol	SMTP

IPS (Top Attacks Blocked)

Attack Type	Count
text_line_too_long	88
OpenSSLASN.1.Double.F	52
invalid_state-Pop Dec	10
bad-unknown	23
misc-activity	54

Core Security

Anti Virus

Gateway AV (Top Viruses Blocked)

Virus Name	Count
Worm.SomeFool.P	12
Trojan.Small-407	8
Worm.Dumanu.A	2
Worm.SomeFool.Gen-2	2
Worm.SomeFool.I	1

DesktopAV (Top Viruses Blocked)

Virus Name	Count
Eicar_test_file	5
EXPL_SSLICE.GEN	2
HTML_VMLFILL.I	1
HTML_test_file	2
EXP_SICE.G	1

Content Filtering

Web Filter (Top Websites Blocked)

Website Type	Count
Eicar_test_file	27
EXPL_SSLICE.GEN	21
HTML_VMLFILL.I	19
HTML_test_file	12
EXP_SICE.G	9

Anti SPAM (Top SPAM Blocked)

Spam Name	Count
Eicar_test_file	18
EXPL_SSLICE.GEN	4
HTML_VMLFILL.I	2
HTML_test_file	1
EXP_SICE.G	1

Supplementary

Data Backup (PageStatus)

Date	Status
Last Success Backup	6/30/07
Last Failed Backup	5/25/07
Size of Last Backup	2 GB
Total Storage Size	20GB

Web Monitoring (Page Status)

Web Page	Status
Avg Website Load Time	2.03 sec
Website Availability	100%
Home Page Defaced	No
Login Page Defaced	No
Service Page Defaced	No