



Managed Content Security

Email and web content threats and acceptable use of corporate resources continue as the number one concern of IT security staff. Risk to an organization's infrastructure, intellectual property and resources have always been a concern compliance frameworks are placing specific requirements on secure content management.

Managed Content Security Solutions

- Reduce your total cost of ownership (TCO) by eliminating the need for software or hardware at your site
- Ensure unlimited scalability and easy deployment across multiple sites
- Deploy tools that allow creation, enforcement and monitoring of policies
- Set targets for response times to alerts, validate, design and implement change requests
- Comprehensive management to free up internal expertise to focus on security projects
- Flexible multi-layered secure content management solution protecting email and Internet systems

TELEHOUSE Management Framework Value

- Leverage TELEHOUSE's best-of-breed monitoring technologies and proven implementation processes to provide rapid and effective management
- Gain visibility into your security environment
- Rely on expert analysts to improve the stability and availability of your environment

For more information visit www.TELEHOUSE.com

Email Content Management

Up to 90% of email server loads come from malicious SMTP traffic, with Directory Harvest Attacks (DHAs) and Denial of Service (DoS) attacks comprising as much as one-third of that load. Stopping these sophisticated attempts to acquire valid email addresses or damage your business requires constant diligence, the latest technologies, and extensive security expertise.

TELEHOUSE offers flexible solutions that provide multi-layered protection against spam, viruses, DHA, and DOS attacks.

- No hardware installation or maintenance
- Significant drop in mail server traffic and junk emails
- Extremely low latency
- Fast, easy installation and setup
- 100% anti-virus guarantees
- Spam, DoS and DHA prevention
- Phishing protection
- Policy violations and acceptable use
- End-to-end encryption management

Monitored Email Security Services

TELEHOUSE monitors your email security systems, analyzes the data continuously, and escalates problems to your designed staff.

Managed Email Security Services

TELEHOUSE monitors and manages your email security systems, analyzing the data continuously.

Hosted Email Security Services

This fully managed and hosted service delivers complete end-to-end optimized email security. Your staff can focus on your operations while you realize the benefits.

Web Content Management

With employee Web browsing and instant messaging comes potential problems that include access to unauthorized Web sites and the potential for malicious code, spyware, and other threats that could compromise your systems. TELEHOUSE offers flexible solutions for securing your web and instant messaging Internet communications.

- Web filtering
- Policy management by custom grouping, LDAP, and time-based policies
- Multiple virus and spyware engine scanning
- Proactive heuristics to identify unknown and zero-hour threats
- Selective adware access admission
- Monitoring, logging and usage reporting
- Real-time alerts for threats or attempted policy breaches
- Instant messaging (IM) control

Hosted Web Security Services

This fully managed and hosted service delivers complete end-to-end optimized Internet policy management and security. With all hardware and software hosted and managed by TELEHOUSE, you simply configure your systems to point to our hosting center.

- No hardware or software required at your site
- Flexible service options customized to your needs
- Simplified administration
- Fast, easy deployment
- Scalable to grow with your business
- Cost-effective and efficient



System Availability and Health Monitoring

TELEHOUSE monitors your security systems, with all monitored conditions brought to the customer’s attention or escalated. The Secure Operations Center (SOC), monitors each device. If a response is not available or if a variable exceeds pre-defined thresholds, an automatic alert is created and ticket generated.

The ticket is reviewed by an SOC analyst who then notifies the customer based on escalation procedures. If the customer has purchased a management solution (SecurePlatinum), the SOC analyst will identify the source of the problem and troubleshoot the issue until the root cause has been identified. The TELEHOUSE engineer will then take actions necessary to bring the device back to full functionality.

System Secure Web Portal

The Secure Web Portal provides “at a glance” dashboards showing the health of systems monitored or managed through TELEHOUSE.

Alerting and Escalation

Alerts sent from the managed system are logged, acknowledged, analyzed and then escalated by the SOC. Alerts that impact the

managed service delivery, the availability of the device or other monitored devices are escalated to the designated point of contact.

System Security Service Appliance (SSA)

TELEHOUSE’s worldwide service delivery infrastructure includes Security Operation Centers are strategically located in North America and Europe. As part of this architecture, TELEHOUSE has developed a Security Service Appliance (SSA).

The SSA is located onsite directly interfacing with the devices under management. The SSA provides a vital link in the secure monitoring and management of security systems by providing real-time log file analysis and alert creation, back up and restoration capabilities. The SSA also provides the platform for secure remote access. An Out-Of-Band connection ensures the SSA is reachable even when the primary Internet connection is not available. As events occur, the SSA provides a first step in the correlation process, reducing many associated events into a single multi-event message and ensuring bandwidth is not taken up with excess data being sent back to the security management centers for more comprehensive analysis.

TELEHOUSE Silver and Platinum Support Overview	SecureSilver Premium	SecurePlatinum Classic	SecurePlatinum Premium
→ 7/24 Service Availability	✓	✓	✓
→ Co-managed Service	✓	Option	Option*
→ System Availability Checks	✓	✓	✓
→ System Health Monitoring	✓	✓	✓
→ System Health Alerting & Escalation	✓	✓	✓
→ System Configuration Backup	✓	✓	✓
→ Reporting	✓	✓	✓
→ Web-based Customer Portal	✓	✓	✓
→ Extended Availability Monitoring	✓	✓	✓
→ Security Service Appliance	✓	✓	✓
→ Vulnerability Monitoring	✓	✓	✓
→ Rulebase Management	Option	✓	✓
→ Full Logfile Analysis (Security Event Monitoring)	✓		✓
→ Security Alerting & Escalation	✓		✓
→ Remote Equipment Management		Option	✓
→ Remote System Rebuilds		✓***	✓
→ Platform Management		✓	✓
→ Service Level Agreement *		*	✓*
→ Fully managed Service		✓	✓

* If Service purchased as co-managed Service, the Service Level Agreement is not available

***Full details on the service are available in the appropriate Contract Pack



Logfile Analysis

At the SecureSilver Premium and SecurePlatinum Premium level, TELEHOUSE monitors and analyzes log files for the devices under management. When log analysis is subject to internal compliance policy special procedures can be used to meet those requirements.

TELEHOUSE analyzes logs that record normal user access of web sites and other resources. These are logs that record the user name, web server accessed, web page viewed among other statistics. Generally tens to hundreds of megabytes in size, these access logs are normally stored on separate log and reporting servers.

Platform Management

TELEHOUSE looks after the day-to-day maintenance and management of the security system, performing software updates, configuration changes and configuration backups to keep the system running reliably and securely.

Policy Management

Policy Management allows calls to TELEHOUSE’s operations staff at any time to make configuration changes to security policy. TELEHOUSE will use its extensive network security expertise to validate, design and implement changes to your security policy. TELEHOUSE ensures that insecure changes are identified and avoided so that a robust security policy is maintained.

Reporting

A wealth of reporting options are provided via the Secure Web Portal. These reports provide information and details about alerts, system availability statistics and graphs, system resource usage, and policy modification events. Reporting parameters are flexible and report data can be downloaded in CSV format to allow tailored reporting.

Sample Report Types

Top Ten Destination Addresses (Webpages) accepted	Yes
Top Ten Destination Addresses (Webpages) dropped	Yes
Top Ten Source Addresses (Workstations) accepted	Yes
Top Ten Source Addresses (Workstations) dropped	Yes
Top Ten User - accepted	Yes
Top Ten User - dropped	Yes
Top Ten Content Types - accepted	Yes
Top Ten Content Types - dropped	Yes
Top Ten Mime -Types - accepted	Yes
Top Ten Mime -Types - dropped	Yes
Top Ten Viruses – dropped	Yes
Top Ten Protocols - accepted	Yes
Top Ten Protocols - dropped	Yes

Remote System Management and Rebuild

A catastrophic failure need not mean that communications are impacted for long. Once the hardware replacement has been provided—facilitated by TELEHOUSE—a remote system rebuild can commence. The SSA and out-of-band remote management kit are designed to allow for the restore the security device using the most recent configuration within a matter of hours.

System Configuration Backup

TELEHOUSE backs up the managed system configuration information on a daily basis for the purpose of system rebuilds.

ISIS

In addition to the wealth of standard reporting, our unique ISIS system allows fully configurable alerting around a series of business rules. This allows e-mail and SMS text message alerts of rule changes, logins and other interesting events based on time of day and type of activity, to be sent. ISIS offers advanced reporting and event correlation on a wide range of event types, making sure you are fully aware of the threat to your network at all times. About TELEHOUSE

Administrative Reports

- List of change requests *
- Change request search *
- List of trouble tickets
- Trouble ticket search

*For SecureSilver Premium only if the Policy Management Option has been purchased)

Service Delivery Reports

- Availability of monitored systems
- Alert reports
- Incident reports
- Traffic reports (Resource usage of managed systems)
- Review of incidents by type, e.g. policy changes, system access



"It is often easier to manage networks than people. Protect all aspects of your security posture with solid policies and procedures created by your trusted security expert, TELEHOUSE."

For more information visit
www.telehouse.com

Corporate Headquarters:
The Teleport - 7 Teleport Drive
Staten Island, New York 10311 USA

Phone: (718) 355.2500
Email: sales@TELEHOUSE.com

© 2009 by TELEHOUSE, Inc.. All rights reserved. TELEHOUSE reserves the right to change or modify any information contained herein without notice. Reproduction of this document in any form without prior written permission is strictly forbidden. All products or services referenced herein are the trademarks or service marks of their respective companies or organizations.

Certified to ISO/IEC27001:2005 Certificate number IS65890



Certified to ISO/IEC27001:2005
Certificate number IS65890