



Managed and Monitored Firewall Service

Superior Management and Monitoring of Security Devices

Axxera, a premier managed security services provider, offers you Managed and Monitored Firewall services through its Central Intelligence Technology platform. Central Intelligence provides comprehensive, outsourced monitoring and management for your organization's Firewalls, helping to detect and respond to the most sophisticated and malicious hacker attacks.

The Central Intelligence Managed and Monitored Firewall Service provides real-time security monitoring and 24x7 professional security analysis. The service offers complete outsourced management of supported Firewalls, including signature updates, system and software support, and upgrades

Central Intelligence alone offers the only true real-time Monitoring service in the Managed Security Services industry to protect your company's mission-critical information assets.

Redefining Security Monitoring

Unlike our competitors, Central Intelligence takes a holistic approach to security monitoring:

Aggregation of Data

The Central Intelligence technology platform aggregates log data and alerts through VPN connections to your security devices, including the leading commercially available firewalls, network-based IDSs, host-based IDSs, and other security applications.

Data Normalization

This data is then normalized across a distributed database architecture at Security Operations Centers (SOCs) where Security Analysts see an uninterrupted view of network activity.

Data Mining and Correlation

The Central Intelligence technology platform then mines the data for suspicious events using a variety of expert systems and anomaly-based advanced query sets, correlates them to other signs of attack, and presents them to Security Analysts.

Expert Analysis

Security Analysts in the SOCs interpret this data in real-time, using advanced query and analysis tools. Analysts then categorize attacks by analyzing malicious activity according to many different criteria, including source, destination, direction and distinguishing factors.

• Real Time Security Monitoring

- o Real-time ticket information and status
- o Real-time security device log and alert data
- o Real-time analysis, commentary and recommendations of security events by security analysts

• Managed Security Services

- o **Managed and Monitored Firewall Service**
- o **Managed and Monitored Network-Based IDS Service**
- o **Security Monitoring Service for Host-Based IDS**
- o **Digital Evidence**
- o **Predictive/Proactive Security Service**
- o **Enterprise Security Reporting**

• Reporting and Analysis

- o Security Statistics
- o Changes, upgrades, maintenance report
- o Malicious activity and other significant events report
- o Forensic investigation
- o Digital Evidence Analysis
- o Online data storage

• Service Delivery

- o 24 x 7 x 365 expert support through Security Operations Center
- o Real time and proactive action
- o Remote management through secure communication channels

• Tiered Services Options

- o Scale as you need
- o Low overhead costs

They then prioritize the results according to a constantly evolving threat model, customized to your needs.

Fast, Professional Response

Working closely with the client, Security Analysts take action to help defend against intrusions before a crippling loss of information can occur.

Services Overview

Central Intelligence provides the following as part of the Managed and Monitored Firewall Service:

Gold

The Central Intelligence Gold Service level includes the following features:

- 24x7 Support center coverage
- Next-generation security monitoring
- Standard configuration management, emergency configuration management and security support available 24x7x365
- Monitoring and management of infrastructure firewalls 24x7x365
- Real-time automated proactive protection against attacks
- Predictive protection based on real-time global IP reputation (botnets) intelligence
- Forensic investigation of attacker for trending and analysis
- 4.5 GB of online log data storage per device with the option to purchase additional online storage
- Access to the Axxera central intelligence portal for real-time security analysis

Platinum

The Central Intelligence Platinum Service level includes the following features features:

- 24x7 Support center coverage
- Next-generation security monitoring
- Standard configuration management, emergency configuration management and security support available 24x7x365
- Monitoring and management of infrastructure firewalls 24x7x365
- Real-time automated firewall proactive protection against attacks
- Predictive protection based on real-time global IP reputation intelligence
- Forensic investigation of attacker for trending and analysis
- Primary Security Analyst assigned to your account to analyze repetitive cyber attacks
- Proactive security incident management with root cause analysis
- Proactive security architecture problem review
- Proactive firewall patch management based on current exploits
- 30 standard policy changes per month and 12 emergency policy changes per year per device
- 4.5 GB of online log data storage per device with the option to purchase additional online storage
- Access to the Axxera Central Intelligence portal for real-time security analysis

Axxera Service Description

	Gold	Platinum
→ 24x7 Support Center coverage	✓	✓
→ Event correlation and validation with Central Intelligence technology	✓	✓
→ Central Intelligence portal (system health, forensic investigation, security reporting)	✓	✓
→ Ticket tracking, communication, notification and escalation management	✓	✓
→ Operational Steps with validation and notification steps	✓	✓
→ Security Incident management (detection, classification, notification, recording, and closure)	✓	✓
→ Project management for installation	✓	✓
→ Provide real-time proactive security incident response	✓	✓
→ Provide real-time proactive security incident mitigation	✓	✓
→ Provide real-time forensic investigation on attacker for pattern analysis	✓	✓
→ Provide real-time Intelligence based Protection from bad reputation ip address	✓	✓
→ Provide real-time security incident dashboard graphs	✓	✓
→ Provide real-time security forensic investigation dashboard graphs	✓	✓
→ Monitor availability and response for firewall and IDS	✓	✓
→ Operational Steps with validation, troubleshooting, resolution and escalation steps	✓	✓
→ Incident resolution based on manual or automated procedures (blocking attacks, ports, or internal hosts)	✓	✓
→ Primary Security Analyst assigned to every account for incident investigation, diagnosis, and control		✓
→ Proactive security architecture problem identification		✓
→ Configuration identification, status, verification and audit		✓
→ Patch analysis and management		✓
→ Analyze repetitive critical cyber attacks and suggest corrective actions		✓
→ Update and manage IDS signatures for the latest attack patterns		✓
→ Analyze IDS signature updates and suggest classification changes		✓
→ Suggest changes to optimize security for new applications		✓
→ Analyze digital evidence and suggest forwarding to law enforcement		✓
→ Project management resource assigned for installation and on-going account maintenance		✓
→ Complete security problem management with incident root cause analysis, when appropriate		✓
→ Enterprise account management with complete understanding of architecture		✓
→ Change management coordination, review, risk assessment and justification		✓
→ Release management planning, deployment and acceptance		✓
→ Monitor ticket activity (24 hour report) and work to reduce false-positive and non-critical items		✓
→ Streamline resolution procedures to reduce resolution times of security tickets		✓
→ Configuration management (identification, planning, control and optimization)		✓
→ Perform changes to optimize firewall and IDS		✓
→ Install and apply fixes to security vulnerabilities according to industry standards		✓
→ Install latest anti-virus data files (any applicable software fees to be paid by customer)		✓

Policy Changes

Policy changes to Central Intelligence managed firewalls are defined as client requests to alter the rule set that defines what traffic can pass through the firewall. These requested changes can take the form of:

- Adding, deleting or changing what services are allowed through the firewall

Policy Change Definition

A single Policy Change consists of one of the following:

- Up to 15 additions, deletions or changes to the service rules of one firewall or high availability firewall pair at one time

The following are not considered Policy Changes:

- Modifications to the network topology around or into the device
- Substantial changes to the feature set
- The integration of complementary products to the firewall

There are two types of Policy Changes: Standard Policy Changes and Emergency Policy Changes.

Standard Policy Changes

All Managed Firewall packages include a given number of Standard Policy Changes per device. The following rules apply to Standard Policy Changes:

- Clients are limited to one Standard Policy Change per day.
- Clients are permitted to make a certain number of Standard Policy Changes in any given month, as outlined in their service description.
- Standard Policy Changes are queued.
- Central Intelligence guarantees that Standard Policy Changes will be completed within 24 hours of the request being received.

Emergency Policy Changes

All Managed Firewall packages allow the client to purchase Emergency Policy Changes per device. The following rules apply to Emergency Policy Changes:

- There is no daily limit on the number of Emergency Policy Changes
- Emergency Policy Changes are worked continuously by the SOCs from the time they are received until completion
- Central Intelligence guarantees that Emergency Policy Changes will be completed within 12 hours of the request being received.

Service Enhancements

The following enhancements to the Central Intelligence Managed and Monitored Firewall Service are available:

Security Help Desk

While the Central Intelligence Managed and Monitored Firewall / IDS Services includes basic functionality support, Central Intelligence has developed a Security Help Desk to assist clients with installation difficulties and configuration problems with your Network.

Through the SOCs, Central Intelligence offers comprehensive 24x7 support at additional charge.

Security Help Desk support is intended for use by a client IT staff point of contact to address any Network / Security concerns, installation and configuration issues.

The Central Intelligence Security Help Desk functions on a token redemption basis. One token provides for a single help desk support call of up to one hour in length.

Online Data Storage

All Managed and Monitored Firewall Service packages include a fixed amount of online data storage per device. This amount of data storage represents 3 to 6 months of firewall log data for a typical Central Intelligence client. If a client's device generates a greater-than-average amount of data, Central Intelligence recommends that the client purchase additional online data storage. While all data is backed up on tape, once the amount of online data storage is exceeded, the oldest material is purged from the online data store. Clients can purchase additional storage at their discretion for a one-time setup fee and an incremental monthly fee.

Network Deployment

Central Intelligence offers special packages for the monitoring and management of IDSs when deployed in conjunction with our Managed and Monitored Firewall Service. For more information, see the Managed and Monitored Network-Based IDS Service document.

Service Level Agreements

Central Intelligence provides industry-leading Service Level Agreements (SLAs) in support of the Managed and Monitored Firewall Service. The SLAs include uptime, service guarantees and penalties if guarantees are not met.

Additional Security Offerings

Central Intelligence offers a full suite of information security services to suit your needs. For additional information about the Central Intelligence Real-Time Managed Security Services, see the following documents:

- Managed and Monitored Network-Based IDS Service
- Host-Based IDS Monitoring Service
- Digital Evidence
- Predictive/Proactive Services
- Enterprise Security Reporting

Protect Your Network with the Central Intelligence Managed and Monitored Firewall Service

With real-time information protection and industry-leading security professional services, Central Intelligence provides the most advanced information security available today. Find out how the Central Intelligence Managed and Monitored Firewall Service can give your network the security you need.

About Axxera

Founded in 2007, Axxera is uniquely positioned to safeguard the electronic presence of today's corporations. Our founders pioneered the security industry by designing, and building security infrastructure worldwide. Axxera has helped secure hundreds of global organizations, and e-businesses.

Axxera Managed Security Services delivers the expertise, tools and infrastructure you need to secure your information assets from Internet attacks 24/7/365, often at a fraction of the cost of in-house security resources. Access to the Axxera Portal a secure Web-based management tool, provides a single interface to easily monitor the security of your overall infrastructure of managed and unmanaged security devices.

Axxera's proprietary technology platform enables detailed processing of every event on your network. Our processing model gives expert analysts at Axxera's Security Operations Centers the advanced tools they need to provide real-time analysis and protection.

Axxera Headquarters

2 Park Plaza	Phone: 949.502.4930
Suite 200	Fax: 949.861.9229
Irvine, CA. 92614	Email: info@axxera.com
	Web: www.axxera.com

Sales Offices

3109 Colebrook Lane	590 Madison Avenue
Dublin, CA. 94568	New York City, NY. 10022

Axxera International Center

1st Floor, Lakshmi Towers - B
Plot No. 17, Nagarjuna Hills
Hyderabad, Andhra Pradesh, India.
Pin - 500082