

## fact sheet: security solutions

# Verizon Security Solutions

### Security Infrastructure Monitoring and Management

Comprehensive managed security services deliver world-class, cost-effective infrastructure protection solutions.

An effective program of incident detection, response and reporting is a continuous process—not a one-time solution—and requires a team of experts to support this ongoing process.

As a leading provider of incident prevention, detection, response and reporting solutions for government agencies, Verizon Security Solutions is well-qualified to help state and local governments develop effective programs.

Verizon infrastructure security monitoring and management services support not only the deployment of effective firewall and intrusion detection/protection solutions, but the ongoing management of security devices, helping to ensure they are operational, properly configured, and up-to-date. **Verizon Security Solutions** has the proven expertise, processes and technology to provide your organization with an effective incident detection, prevention, response, and reporting program.

### Cloud to Core Visibility and Insight

At Verizon Business, we continue to extend the breadth of backbone intelligence sources and focus on improved depth of visibility into customer networks, which can help transform threat data into security insight, intelligence, and action—all in the context of your organization.

- **Gather data from the enterprise core.** Verizon's security infrastructure gathers data and normalizes and consolidates it into information relevant to your agency
- **Integrate cross-enterprise intelligence.** With several thousand customers, including a number of cabinet-level government agencies and some of the largest corporations in the world, we incorporate insight from many devices in countries around the world for broad and early threat intelligence.
- **Global vision—the key to early detection.** Verizon operates one of the world's largest IP networks. Continuous, in-depth monitoring activity such as fraud correlation, Internet outage correlation, and dark space analysis helps Verizon detect emerging security events—in many cases before they threaten your agency.
- **Actionable intelligence.** Verizon's managed security services platform, correlates data and uses statistical modeling to detect anomalous activity, develops rules to highlight alerts (worms vs. false positives), and also features sophisticated visualization tools for fast investigative analysis.

### Broad Device Support Options

Verizon Business offers 24x7 monitoring and management of security infrastructure, including a broad selection of best-of-breed firewalls, intrusion detection and intrusion prevention devices, and routers. The infrastructure monitoring and management services are backed by Verizon's customized Service Level Agreements (SLA).

#### features

- 200+ dedicated security professionals
- Managed and Professional Security Solutions
- 24x7 SOC locations
- Integrated visibility from the Internet cloud to the enterprise core
- Managed security services platform

#### benefits

- Proven ability in threat discovery
- Flexible solutions to meet diverse business needs
- Early threat detection through combined global intelligence
- Integrated, proactive approach to mitigating risks
- Secure customer interface with real-time, actionable reports

## **Government Cleared Facility and Staff**

**Verizon Security Solutions** personnel and facilities have been cleared for the processing of classified information by multiple federal agencies. The **Verizon Security Operations Center (SOC)** is equipped with a Cyber Warning Information Network (CWIN) facility, providing an additional means of early warning, and an out-of-band channel to communicate with federal authorities and other major providers of Internet infrastructure in the event of a major Internet outage.

Our systems are staffed and monitored by cleared, trained security professionals who respond to alerts and alarms. Second-level analysts provide in-depth support and review batch data, looking for historical trends and anomalous activity.

## **Customer Alerts of Security Events and Device Status**

Verizon monitors networks from its sophisticated SOC to provide prompt alerts of security events and device status. The SOC utilizes state-of-the-art physical and data security technologies, combined with proven processes and procedures to help customers protect their data both in storage and in transit.

Device loss of service is reported via automated alerting. When a potential security event is detected, Verizon Business enacts the appropriate response based on customizable alert and escalation procedures, as well as established customer service level agreements. Alarm and log data generated by monitored devices is collected and securely delivered through Finium, our managed security service platform. This data is then managed in a three-stage process that:

- Identifies all alarms
- Investigates all events
- Responds to all incidents

## **On-line Security Collaboration and Reporting Environment**

Verizon customers have access to dynamic activity data alongside standard reporting on historical trends and statistics via the secure web console. With secure, remote access to this pertinent information, your staff and Verizon personnel can efficiently collaborate to respond to incidents and resolve issues.

Reporting includes:

- Device activity
- Status of policy change requests
- Policy of firewall configurations
- Overview of device availability issues
- Problems and assistance requests
- Daily analysis of device operations
- Key statistics

Device logs are also monitored, and security events such as port scans are identified, analyzed and escalated as required. Logs are archived, and analysis results as well as raw log data are available through the secure Finium web console reporting function.

## **Lifecycle Security Device Management**

Device management services can provide lifecycle support for security devices managed by Verizon Business. This includes:

- Maintenance
- Upgrades of the security application
- Upgrades of the operating systems
- Device policy updates
- Device replacement

## security solutions

An important component in device management is the application of patches to operating systems, applications and platforms. Verizon Business identifies new security threats and corresponding patches and upgrades, using comprehensive vulnerability information. Customers are promptly informed of any potentially critical security vulnerability that is discovered. Verizon Business tests patches before implementation to evaluate effectiveness and impact on overall system reliability.

### Major Device Upgrades

Verizon Business also performs major device upgrades in order to help maintain security effectiveness. Upgrade plans are agreed upon with the customer before implementation. When appropriate, Verizon Business will evaluate customer security configurations, and resulting changes are agreed upon and implemented.

### Verizon Security Solutions

Founded by former government security experts, **Verizon Security Solutions** has taken a leadership role in the development of the management disciplines and processes needed to achieve success in information assurance. Verizon Business provides comprehensive expertise in helping government entities plan and measure their security programs, establish and monitor compliance, and improve security infrastructure operations. That's why today Verizon Business is a leading security services provider to the U.S. Federal Government.

### Contact Us

For more information on **Verizon Security Solutions**, contact your Verizon Business account manager at [www.gov-edu-security@verizonbusiness.com](mailto:www.gov-edu-security@verizonbusiness.com).

Visit our website at  
[www.verizonbusiness.com](http://www.verizonbusiness.com)  
to learn more about  
Verizon Business's  
products suite.