

Cisco Remote Management Services for Security



Innovation: Many Take Advantage of It, Some Strive for It, Cisco Delivers It.

Cisco Remote Management Services (RMS) for Security provide around the clock remote management, monitoring, and remediation for today's networks against sophisticated attacks, vulnerabilities, and malware. They relieve the burden of routine, reactive, and proactive security management tasks and allow the customer's IT staff to focus on more strategic business initiatives.

Cisco RMS for Security includes a dedicated team of highly skilled security experts acting as an extension of the customer's IT organization. Utilizing a proven, co-managed methodology and process based on ITIL®, the Cisco team delivers trusted solutions to help enable business continuity. Our customers retain ultimate control of their own network security devices, and they have complete visibility into network health and the status of our work through the innovative Cisco RMS for Security web portal.

Two Distinct Services to Fit Your Unique Organizational Needs

Cisco RMS for Security delivers two service offerings that can help your organization meet the needs of managing and maintaining the security technologies deployed on your network, while mitigating threats and vulnerabilities before they can affect business continuity.

Management Support

The Cisco RMS for Security platform delivers a breadth of security management services, thereby providing a comprehensive coverage of Cisco security devices. With this comprehensive coverage, our Cisco Remote Management Services for Security engineers and analysts can co-manage more of our customers' Cisco security deployment and solutions, thereby helping to provide efficacy, business continuity, and ultimately, productivity. The Cisco Remote Management Services for Security includes incident, problem, change, release, and configuration management support for the following:

- Cisco Firewall
- Cisco Intrusion Prevention System
- Cisco VPN

... can help your organization meet the needs of managing and maintaining the security technologies deployed on your network, while mitigating threats and vulnerabilities before they can affect business continuity.

- Cisco IOS® Security
- Cisco ACS
- Cisco ACE Web Application Firewall
- Cisco ACE Application Control Engine
- Cisco Security Configuration Engine
- Cisco Security MARS
- Cisco Security Manager

In addition, the Cisco RMS for Security platform is designed to aggregate and correlate primary data sources, including network protocols such as syslog and NetFlow to provide a more comprehensive view of our customer's network.

The Cisco RMS for Security platform is designed to deliver truly robust monitoring and management capabilities that enable Cisco ROS to deliver a more holistic managed security solution, thereby protecting our customers from network attacks and emerging threats.

Multivendor Monitoring Support

Networks evolve over time. Therefore, technology choices are made for various reasons, and typically, most networks are heterogeneous environments, including products from various security vendors. The Cisco RMS for Security platform delivers to our customers a more diverse coverage of their network security deployment by monitoring security products from the most popular vendors. These include:

- Cisco Security devices
- Checkpoint
- Juniper
- IBM/ISS
- TippingPoint

This ability to provide monitoring of multivendor products, as well as Cisco devices, provides our customers a more robust service, by which more of the network is monitored, and malicious activity is thwarted before it can affect business continuity. With the addition of multivendor monitoring services, our customers benefit from the convenience and expertise of one company providing their remote security monitoring solution. Additionally, while our platform allows for the immediate monitoring of vendors listed above, we will have the flexibility to grow this list as our customers' business needs dictate.

Actionable, Multitiered Correlation and Intelligence

In order to meet the security challenges that face today's IT departments, Cisco RMS for Security delivers actionable intelligence based off of aggregated and correlated data. Without a specialized, global perspective of risks and attacks, the ability to reduce those risks and protect networks, data, and business continuity is diminished. Therefore, Cisco RMS for Security and its SOC experts are part of a cohesive ecosystem of teams, products, and technology, working in concert to deliver real-world solutions for our customer's individual security deployments. This multidynamic security perspective is achieved through the following collaborative sources:

Cisco Security Intelligence Operations

Cisco Security Intelligence Operations are a centralized security operations center, which consists of data and teams working together to deliver ready-to-use intelligence and real-world solutions for

The Cisco RMS for Security platform delivers to our customers a more diverse coverage of their network security deployment by monitoring security products from the most popular vendors.

security risks as they occur on a global basis. This intelligence is gathered and investigated through a host of technology and teams. These security intelligence data streams include:

- Cisco STAT team: A team dedicated to testing vulnerabilities within Cisco equipment
- Cisco applied intelligence team: A team that develops white papers and rules for mitigating vulnerabilities and security risks utilizing Cisco technology
- Cisco IPS signature development team: The team of engineers who develop and test the signatures for Cisco's intrusion prevention technology
- Cisco seekers: A research team that analyzes hostile network activity as it appears globally and then delivers to our customers solutions to mitigate malicious attacks. This team is involved in ongoing botnet research, web browser exploit discovery, zero day server exploit discovery, SensorBase data analysis, ongoing malware analysis, and open proxy attack vector analysis.
- IntelliShield: A team of engineers who investigate and deliver vendor-neutral threat intelligence and means to mitigate malicious attacks.
- SenderBase and SensorBase: Market-leading technology within both the Cisco IronPort mail security devices as well as the Cisco IPS security technologies that detects and alarms on global threats in real time and reports them, automatically, back to the Cisco Global Threat Operations Center, thereby allowing protection globally, from threats seen in their infancy, locally.
- Cisco's Product Security Incident Response Team (PSIRT): A dedicated global team that manages the receipt, investigation, and public reporting of security vulnerability-related information, related to Cisco products and networks.
- ROS Security Operations Center: The team of security engineers and analysts who deliver the Cisco RMS for Security services. This team of security experts encompass the delivery arm of the overall Cisco Threat Operations Center.



Multitiered Correlation Capabilities

Through the ecosystem of intelligence gained from the Cisco Global Threat Operations Center, the Cisco RMS for Security SOC and its platform are able to deliver powerful aggregation and correlation capabilities that help ensure accuracy in identifying and mitigating current threats and attacks. Correlation is based on a multidimensional engine in which rules are created, modified, and refined based on evolving security threats and attacks, as well as the global intelligence described above. These correlation engines include:

- Rules-based correlation: Single-state or multistate rules that are fired based on a series of conditions, time periods, and rules that reduce the number of benign alarms, enabling rapid response to legitimate attacks.
- Vulnerability correlation: Used to incorporate vulnerability data to reduce false positives and identify potential threats targeted at high-value assets.
- Statistical correlation: Provides the ability to analyze network behavior and identify threats based on severity and anomalous event patterns.
- Historical correlation: Provides the capability to identify patterns of repeating and automated slow attacks, which can be concealed within millions of raw security events.

Customer-Site Data Collection

As part of the Cisco RMS for Security platform, we have made sure that all data is collected prior to correlation and analysis from all managed sources. Therefore, depending on the design and network traffic patterns of the customer's security architecture, and as part of our monitoring and management services, some customers might receive at least one ROS Management Application Platform (MAP) 3050 appliance. The MAP 3050 appliances are an extension of the Cisco ROS Data Communication Network (DCN) and are deployed on the customer's premises to aggregate, correlate, compress, and forward security event data back to the Cisco ROS DCN. In addition, a Cisco ROS VPN termination router will also be deployed on the customer's premises to facilitate management and monitoring network connectivity. Our goal is to establish a thorough view of network traffic while protecting our customers' data.

As you can see, the Cisco RMS for Security is an ecosystem of security intelligence that increases the overall efficiency and accuracy of security incident investigation, classification, and notification.

Cisco RMS Web Portal

The Cisco RMS for Security web portal provides a unique capability for our customers, by which they have around the clock access to their managed security service and the Cisco SOC engineers monitoring their network. In effect, the Cisco RMS for Security web portal allows our customers the ability to "look over our shoulder" at the events and alarms that are generated from their managed service, as well as the reporting and actions being taken by Cisco RMS for Security engineers and analysts. As a function of the Cisco RMS for Security web portal, a suite of security reports are available that can be used by either an executive or security engineer to garner information needed to observe security incident trends as well as take concise action to remediate a threat. The web portal reporting function provides a real-time view of the current security risks as well as the devices from which they were generated. These reports are as follows:

The web portal reporting function provides a real-time view of the current security risks as well as the devices from which they were generated.

- Intrusion Prevention Blocked Attack Reports
 - Top Blocked Attacks by Signature
 - Top Blocked Attacks by Sensor
 - Top Source Blocked Attacks
 - Top Destination Blocked Attacks
 - IPS Signature Categories
- Intrusion Prevention Summary Reports
 - Top Fired Signatures/Signature Severity
 - Top Attacker Source
 - Top Attacked Destinations
 - Signature Severity Summary by Sensor
 - Top Fired Signatures Severity
- Firewall Summary Report
 - Total Denied Packets
 - Top Denied Source Addresses
 - Top Denied Destination Addresses
 - Top Denied Protocols
 - Top Denies by Access Control Policy

- Authentication Failure Reports
 - Top Source Address Failed Attempts
 - Top Destination Address Failed Authentication Attempts
 - Top Authentication Failures by Device
 - Top Username Failed Attempts
- Bandwidth Summary Reports
 - Top Applications
 - Top Source/Destination

Through the delivery of this comprehensive list of available reports, Cisco RMS for Security helps ensure that the intelligence our customers receive as part of their managed service is actionable while continuing to meet current and future security needs.

Cisco is continuing to deliver on our promise of excellence. Through the innovation of technology, service delivery, and customer satisfaction, Cisco RMS for Security is once again differentiating Cisco from the competition and providing your organization world-class functionality.

For more information regarding Cisco Remote Managed Services for Security, visit www.cisco.com/en/US/products/ps6192/serv_category_home.html#~sec.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco.Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)