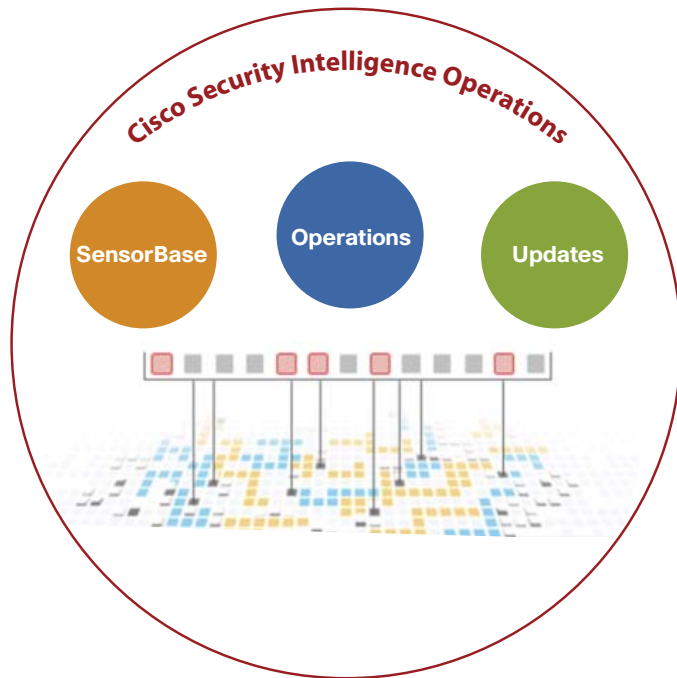


## What Is the Value of Cisco Security Intelligence Operations?

Cisco® Security Intelligence Operations (SIO) is a cloud-based service that connects global threat information, reputation-based services, and sophisticated analysis to Cisco network security devices to provide stronger protection with faster response times (Figure 1).

Figure 1 Cisco Security Intelligence Operations



## What Problems Does It Help Solve?

It has become an increasing challenge to manage and secure today's distributed and agile networks. Cloud computing and the sharing of data are threatening security norms. Online criminals are continuing to exploit the user's trust in consumer applications and devices, increasing the risk to organizations and employees.

Traditional security has relied on layering products and using multiple filters. However, as threats become more sophisticated, these filters have to look deeper into network and application-layer traffic, with the result that filters and layering alone are not thwarting attacks. The latest generation of malware spreads quickly, has global targets,

and uses multiple vectors to propagate. What's more, each attack is different. To combat today's threats, security systems need to look around more pervasively and respond quickly. Cisco has designed Security Intelligence Operations (SIO) to cope with this constantly evolving environment and provide unrivalled protection.

## Cisco SIO Overview

Cisco SIO uses three components to enhance the filters already available in Cisco devices:

- Cisco SensorBase: The world's largest threat-monitoring network that captures global threat telemetry data from an exhaustive footprint of Cisco devices and services
- Cisco Threat Operations Center: A global team of security analysts and automated systems that extract actionable intelligence
- Dynamic updates: Real-time updates automatically delivered to security devices, along with best-practice recommendations and other content dedicated to helping customers track threats, analyze intelligence, and ultimately improve their organization's overall security posture

## Proactive Threat Intelligence

Cisco SIO dynamically collects the broadest depth and breadth of threat information through a real-time threat-monitoring network, Cisco SensorBase. SensorBase includes:

- More than 700,000 (and growing) globally deployed Cisco intrusion prevention system (IPS), email security, web security, firewall devices
- Cisco IntelliShield, a historical threat database of 40,000 vulnerabilities and 3300 tuned IPS signatures
- More than 600 third-party threat intelligence sources, which track over 500 third-party data feeds and 100 security news feeds around the clock

More than 1000 threat collection servers process 500 GB of data a day. The Cisco Threat Operations Center processes this global, real-time threat intelligence and incorporates it into the security services available on Cisco security devices.

## Threat Operations Center

The operations arm of Cisco SIO is a combination of people and automated algorithms that process Cisco SensorBase data in real time. These teams create machine-generated and manually generated rules for protection against new and dynamic threats.



The Threat Operations Center teams consist of more than 500 people dedicated to 24/7 threat research, analysis, and quality assurance every day of the year, in five global locations. The threat operations teams not only research Internet threats, but also collaborate across Cisco to build and maintain engineering security products and to provide outreach that helps combat cybercrime.

## Global Threat Correlation

Cisco Global Threat Correlation is a sophisticated, automated security capability that correlates SensorBase data, such as reputation, known exploits, or anomalous behaviors, to halt attacks more effectively, accurately, and quickly. Whereas traditional network security systems examine only the packet contents, Global Threat Correlation performs a full-context analysis to better understand traffic. The Global Threat Correlation engine considers all of the following variables:

- Who: The “reputation” of who sent the packet. The Reputation Filter blocks the worst offenders, stopping 10 to 15 percent of attacks, and assigns an appropriate reputation status to suspected attacks.
- What: The packet contents compared to exploit, virus, or vulnerability signatures.
- Where: The geographic and industry-specific trends in the sources of traffic.
- How: The propagation and mutation methods.

Global Threat Correlation uses these parameters to continuously develop, test, and publish new rule sets that are used by Cisco security devices.

## Dynamic Updates

Cisco SIO’s dynamic updates deliver current and complete security information to Cisco customers and devices. Threat mitigation data is provided through:

- Automatic rule updates for Cisco products, such as firewall, web, IPS, or email devices delivered every 3 to 5 minutes
- Cisco IntelliShield Alert Manager Service
- Security best-practice recommendations and community outreach services

In addition to dynamic updates, Cisco’s security intelligence is used in many dimensions for the benefit for the general public, end customers, enterprises, and even governments. Through this full security lifecycle approach to understanding and combating threats, you gain the knowledge required to make educated decisions that increase your security posture while helping to ensure that your network is automatically protected from the latest attacks.

## What Are the Benefits of Cisco Security Intelligence Operations?

- Optimize operational efficiency with more effective filters and fewer false positives
- Increase compliance posture and protect brand reputation
- Gain visibility into the latest threat landscape
- Protect against new and emerging threats with market-leading network security devices, including Cisco IronPort® Web Security Appliances, Cisco IPS, and Cisco Adaptive Security Appliances

## Why Cisco?

As blended, cross-protocol threats continue to increase globally, the security industry has recognized that products must be flexible and respond faster. The Cisco Security Intelligence Operations solution enhances the ability to identify, analyze, and mitigate today’s threats. Cisco is committed to providing complete security solutions that are integrated, timely, and effective—securing borderless networks for organizations worldwide.

## More Information

Cisco Security Intelligence Operations Portal: <http://www.cisco.com/go/sio>

Cisco SIO To Go iPhone Application: <http://www.cisco.com/go/siotogo>

Cisco Security Blog: <http://blogs.cisco.com/security>