How Cisco Protects the Enterprise: A Cisco-on-Cisco Overview

With the SolarWinds Orion platform supply chain attack impacting so many organizations around the globe, customers have approached Cisco to learn how we have protected ourselves, including our internal incident response. This high-level document provides an overview of what we do to protect the Cisco Enterprise and how we safeguard our customers in an environment of ever-increasing cyber risk.

Protecting the Enterprise

Defending Cisco starts by securing our global Enterprise – a workforce of 125,000 across 170 countries – supported by 40,000 routers, 26,000 remote office connections, 2500 IT applications, 1350 engineering labs, and 500 cloud applications.

Every day this massive and complex data system produces 47 terabytes of data, 50 billion netflow records, 20 billion DNS queries, and 200 million web transactions.

Cisco Incident Response

Cisco has a dedicated Security and Trust Organization that is focused on three priorities: (1) defending our Enterprise business operations, (2) securing our offers and supply chain, and (3) earning customer trust through trustworthy practices, including incident response.

Our Incident Response Command reports directly to the Chief Cybersecurity and Trust Officer and provides centralized coordination for Cisco's overall incident response.

Our Computer Security Incident Response Team (CSIRT) is a global team of information security professionals responsible for the 24/7 monitoring, investigation, and response to cybersecurity incidents for Cisco-owned businesses.

CSIRT engages in proactive threat assessment, mitigation planning, incident detection, trending, and analysis as well as the development of our cybersecurity architecture. This team includes Analysts (first-level support), Investigators (senior security professionals), Threat Intelligence Analysts (who gather and maintain information), and Engineers (who maintain, test, and develop solutions).

Working alongside CSIRT during the SolarWinds Orion platform supply chain breach and other such attacks, is our Product Security Incident Response Team (PSIRT), responsible for Cisco solution security and Cisco Talos Incidence Response, delivering threat intelligence to provide faster emergency support.

Cisco Cybersecurity Architecture

Cisco uses a robust cybersecurity architecture for governing policy and standards across five key functional areas: (1) security operations and monitoring, (2) identity and access, (3) security across applications, data, and infrastructure, (4) compliance monitoring, and (5) Security Information and Event Management (SIEM).

Visibility

A fundamental component in protecting the Cisco Enterprise is through network and endpoint-based security monitoring to improve real-time and retrospective threat visibility. Some examples of the types of network and endpoint tools we use include:

- **Netflow** – We collect netflow traffic in and out of Cisco, including information from our internal data centers. Netflow data is generated not only from the network devices in the network but from the endpoints themselves. We use Cisco Secure Cloud Analytics (Stealthwatch) to collect and monitor this data. Any signs of abnormal or malicious activity generate alerts that are captured as telemetry data sources for our central SIEM and inform how we respond via our Information Security Playbook (see Procedures below).
- **DNS** – We collect and store DNS requests made from endpoints within Cisco. We have two main sources for collecting DNS data, a level 2 passive DNS capture of requests, and our enterprise instantiation of Cisco Umbrella. We use Cisco Umbrella to manage endpoints to log DNS requests, block access to malicious domains as well as collect and store data for historical analysis. In addition to passive DNS collection, we maintain and use an internal DNS Response Policy Zone (RPZ) for blocking DNS resolution to known malicious hosts and sites, effectively turning a recursive DNS server into a DNS firewall.
- **Cisco Secure Endpoint (formerly AMP for Endpoints)** – Cisco-managed devices have Cisco Secure Endpoint installed and their logs provide visibility to endpoint activity. These logs are kept for retrospective analysis and are essential during zero-day attacks, by identifying all affected applications, processes, and systems to pinpoint patient zero as well as the method and point of entry.
- **Endpoint and Network Device Logging** – Logs from Cisco endpoints are collected along with data from host intrusion prevention tools, both natively from the OS itself and through tools that see the processes running and versions of software installed. Other sources of visibility include network intrusion detection systems, email scanning, web proxy logs, and the use of Threatgrid for dynamic analysis.

Procedures

The CSIRT Security Operations Center (SOC) focuses on reducing the risk of business loss resulting from cybersecurity incidents. To ensure consistency and adherence to procedure, CSIRT SOC utilizes the Information Security Playbook, a dynamic resource for identifying threats, detecting issues, and detailing plays and reports to address alarms and events. CSIRT Analysts rely heavily on the Playbook to address issues, while actively maintaining and contributing to plays. The Playbook is also critical for executing against our SIEM and for CSIRT Investigators as they use the data collected to inspect cases and hunt for new threats in the network.

Defending Cisco is how we safeguard our customers

The Cisco cybersecurity architecture and governance model aims to ensure that we have consistent policies and standards to assess and manage security risk across operations, applications, data, and infrastructure. We believe our pervasive security and zero trust architecture mindset allow us to pivot faster and with greater confidence, to defend Cisco and safeguard our customers.

Customer Resources

How can we find out if we've been breached?	Cisco Talos Incidence Response Service offers a variety of emergency IR services that include scoping, incident command, environment hardening, tool deployment, digital forensics and analysis, intelligence gathering, containment options, and strategic/tactical recommendations.
We need to understand our existing network posture and best practice recommendation.	Cisco Security Infrastructure Advisory Services help customers detect vulnerabilities in their IT infrastructure, network architecture, and configuration. Cisco Zero Trust Strategy Service provides customers with a quick start to their Zero Trust initiative by supporting the development of a three-year strategy for progressing towards a Zero Trust state.
We need network remediation and hardening support.	Cisco Network Security Implementation Service integrates Cisco Security technologies into multivendor environments, including supporting migrations from other solutions and legacy products while optimizing existing technologies to strengthen a customer's security profile.
We want to be better prepared for future events with an effective cybersecurity program.	Cisco Security Attack and Penetration Advisory Service looks at key areas of customer security defenses through the lens of an advanced adversary to determine vulnerability and resistance of networks, personnel, and physical facilities. Cisco Cybersecurity Maturity Program Assessment (CMPA) helps customers understand their current security posture by benchmarking and determining the maturity of their overall program, policies, standards, procedures, security controls, and risk.

How to stay informed

- Cisco Official Security Event Response including a detailed Q&A.
- Cisco Talos Threat Advisory posts on the SolarWinds Supply Chain Attack and the theft of FireEye Offensive Security Tools.
- Talos blog or Talos on Twitter for the latest updates.
- SolarWinds Security Advisory and the FireEye Announcement for full explanations.
- Visit the Trust Center to keep apprised of Cisco security and trust thought leadership and innovation.