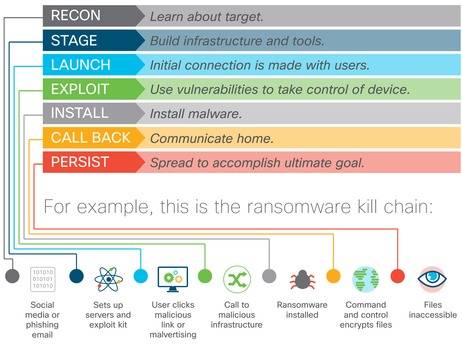
Protection across the kill chain with Cisco Security

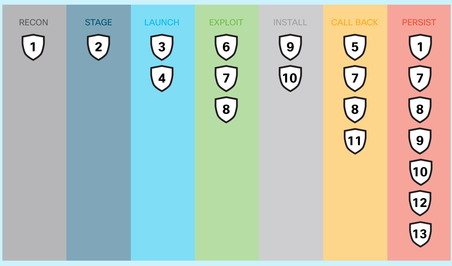
The Cisco Security portfolio protects effectively across the kill chain with solutions that are simple, open, and automated.

Most cyber attacks follow this general flow:



For example, this is the ransomware kill chain:

The Cisco cybersecurity portfolio acts across the entire kill chain.



1. Cisco Stealthwatch identifies reconnaissance activity.
2. Cisco Talos provides industry-leading global threat telemetry and can identify where attacks are staged in the wild.
3. Cisco Email Security blocks malicious emails.
4. Cisco Web Security blocks malicious content in http and https traffic.
5. Cisco Umbrella software blocks command and control traffic at the DNS layer and over any port and protocol.
6. Cisco FirePOWER Next-Generation IPS (NGIPS) blocks exploits with industry-leading threat efficacy.
7. Cisco FirePOWER NGFW and Meraki MX can block command-and-control traffic and unauthorized access to applications and critical assets.
8. Cisco AnyConnect Secure Mobility Client applies NGFW protection to the off-premises user.
9. Cisco Advanced Malware Protection (AMP) for Endpoints blocks malicious files and provides one-click remediation.
10. AMP Threat Grid feeds dynamic malware analysis to the AMP solution to determine if a file is malicious.
11. Cisco Cognitive Threat Analytics identifies breaches through behavioral analysis of command-and-control http and https traffic.
12. Cisco Identity Services Engine (ISE) and Cisco TrustSec technology provide granular access and identity control.
13. Cisco Cloudlock can block unauthorized access to cloud applications and the data within them.

The Cisco Security portfolio is also simple, open, and automated to make you more effective.

Simplify your workflow.

- Manage AMP and Cisco Email Security from the same interface.
- Deploy Cisco Umbrella globally in less than 5 minutes.

Openly share intel across products and third parties.

- Cisco has more than 120 security partners.
- Talos updates products with global threat telemetry in real time.

Automatically respond.

- Automatically remove a malicious file from all email inboxes.
- Automatically block a malicious destination in Umbrella based on threat intel from AMP Threat Grid.

Be more effective.

Cisco's total time to detection is **14 hours**, versus the industry average of **100–200 days**.

Cisco 2017 Annual Cybersecurity Report

Visit cisco.com/go/security to learn more >