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.

Cisco Stealthwatch identifies reconnaissance activity.
Cisco AnyConnect Secure Mobility Client applies NGFW protection to the off-premises user.
Cisco Advanced Malware Protection (AMP) blocks malicious files and provides one-click remediation.
AMP Threat Grid feeds dynamic malware analysis to the AMP solution to determine if a file is malicious.
Cisco Cognitive Threat Analytics identifies breaches through behavioral analysis of command-and-control http and https traffic.
Cisco Identity Services Engine (ISE) and Cisco TrustSec technology provide granular access and identity control.
Cisco Cloudlock can block unauthorized access to cloud applications and the data within them.
Cisco Talos provides industry-leading global threat telemetry and can identify where attacks are staged in the wild.
Cisco Email Security blocks malicious emails.
Cisco Umbrella software blocks malicious content to help prevent malware.
Cisco Web Security blocks applications meant to harm users and data.
Cisco FirePOWER Next-Generation IPS (NGIPS) blocks exploits with industry-leading threat efficacy.
Cisco FirePOWER NGFW and Meraki MX can block command-and-control traffic and unauthorized access to applications and critical assets.
Cisco Umbrella software blocks malicious content to help prevent malware.
Cisco Web Security blocks applications meant to harm users and data.
Cisco FirePOWER Next-Generation IPS (NGIPS) blocks exploits with industry-leading threat efficacy.
Cisco FirePOWER NGFW and Meraki MX can block command-and-control traffic and unauthorized access to applications and critical assets.
Cisco Umbrella software blocks malicious content to help prevent malware.
Cisco Web Security blocks applications meant to harm users and data.
Cisco FirePOWER Next-Generation IPS (NGIPS) blocks exploits with industry-leading threat efficacy.
Cisco FirePOWER NGFW and Meraki MX can block command-and-control traffic and unauthorized access to applications and critical assets.
Cisco Umbrella software blocks malicious content to help prevent malware.
Cisco Web Security blocks applications meant to harm users and data.
Cisco FirePOWER Next-Generation IPS (NGIPS) blocks exploits with industry-leading threat efficacy.
Cisco FirePOWER NGFW and Meraki MX can block command-and-control traffic and unauthorized access to applications and critical assets.
Cisco Umbrella software blocks malicious content to help prevent malware.
Cisco Web Security blocks applications meant to harm users and data.
Cisco FirePOWER Next-Generation IPS (NGIPS) blocks exploits with industry-leading threat efficacy.
Cisco FirePOWER NGFW and Meraki MX can block command-and-control traffic and unauthorized access to applications and critical assets.
Cisco Umbrella software blocks malicious content to help prevent malware.
Cisco Web Security blocks applications meant to harm users and data.
Cisco FirePOWER Next-Generation IPS (NGIPS) blocks exploits with industry-leading threat efficacy.
Cisco FirePOWER NGFW and Meraki MX can block command-and-control traffic and unauthorized access to applications and critical assets.
Cisco Umbrella software blocks malicious content to help prevent malware.
Cisco Web Security blocks applications meant to harm users and data.
Cisco FirePOWER Next-Generation IPS (NGIPS) blocks exploits with industry-leading threat efficacy.
Cisco FirePOWER NGFW and Meraki MX can block command-and-control traffic and unauthorized access to applications and critical assets.
Cisco Umbrella software blocks malicious content to help prevent malware.
Cisco Web Security blocks applications meant to harm users and data.
Cisco FirePOWER Next-Generation IPS (NGIPS) blocks exploits with industry-leading threat efficacy.
Cisco FirePOWER NGFW and Meraki MX can block command-and-control traffic and unauthorized access to applications and critical assets.
Cisco Umbrella software blocks malicious content to help prevent malware.
Cisco Web Security blocks applications meant to harm users and data.
Cisco FirePOWER Next-Generation IPS (NGIPS) blocks exploits with industry-leading threat efficacy.
Cisco FirePOWER NGFW and Meraki MX can block command-and-control traffic and unauthorized access to applications and critical assets.
Cisco Umbrella software blocks malicious content to help prevent malware.
Cisco Web Security blocks applications meant to harm users and data.
Cisco FirePOWER Next-Generation IPS (NGIPS) blocks exploits with industry-leading threat efficacy.
Cisco FirePOWER NGFW and Meraki MX can block command-and-control traffic and unauthorized access to applications and critical assets.
Cisco Umbrella software blocks malicious content to help prevent malware.
Cisco Web Security blocks applications meant to harm users and data.