Compare Industry Next-Generation Firewalls (NGFWs)

Data Valid as of October 2018

	Cisco	Palo Alto Networks	Fortinet	Check Point Software Technologies
Security Features				
Continuous analysis and retrospective detection	✓ Cisco Firepower employs continuous analysis, beyond the event horizon (point-in-time) and can retrospectively detect, alert, track, analyze, and remediate advanced malware that may at first appear clean or that evades initial defenses and is later identified as malicious.	Limited Point-in-time only. (Point-in-time analysis indicates that a verdict is made on the disposition of a file at the moment it is first seen. If a file morphs or begins acting maliciously later, there are no controls in place to keep track of what happened or where the malware ended up.)	Limited Point-in-time only. (Point-in-time analysis indicates that a verdict is made on the disposition of a file at the moment it is first seen. If a file morphs or begins acting maliciously later, there are no controls in place to keep track of what happened or where the malware ended up.)	Limited Point-in-time only. (Point-in-time analysis indicates that a verdict is made on the disposition of a file at the moment it is first seen. If a file morphs or begins acting maliciously later, there are no controls in place to keep track of what happened or where the malware ended up.)
Network file trajectory	Continuous Cisco maps how hosts transfer files, including malware files, across your network. It can see if a file transfer was blocked or the file was quarantined. This provides a means to scope, provide outbreak controls, and identify patient zero.	✗ Trajectory dependent on continuous analysis.	✗ Trajectory dependent on continuous analysis.	✗ Trajectory dependent on continuous analysis.
Impact assessment	✓ Cisco Firepower correlates all intrusion events to an impact of the attack, telling the operator what needs immediate attention. The assessment relies on information from passive device discovery, including OS, client and server applications, vulnerabilites, file processing, and connection events, etc.	Limited Impact is measured only against threat severity. No host profile information to determine if host is actually vulnerable to threat.	Limited Impact is measured only against threat severity. No host profile information to determine if host is actually vulnerable to threat.	Limited Impact is measured only against threat severity. No host profile information to determine if host is actually vulnerable to threat.
Security automation and adaptive threat management	✓ Cisco automatically adapts defenses to dynamic changes in the network, in files, or with hosts. The automation covers key defense elements such as NGIPS rule tuning and network firewall policy.	Limited All policies require administrator interaction. Policies are limited to basic tuning. False positives are manually identified and mitigated.	Limited All policies require administrator interaction. Policies are limited to basic tuning. False positives are manually identified and mitigated.	Limited Policies require administrator interaction.

	Cisco	Palo Alto Networks	Fortinet	Check Point Software Technologies
Security Features (continued)				
Behavioral indicators of compromise (IoCs)	✓ Cisco Firepower considers file behavior and the reputation of sites, and correlates network and endpoint activity using >1000 behavioral indicators. It provides billions of malware artifacts for unmatched scale and coverage from global threats.	Limited Standard, nonbehavioral IoCs are available in separate product.	Limited IoCs are based upon threat severity, not behavior.	Limited IoCs are based upon threat severity, not behavior.
User, network, and endpoint awareness	✓ Cisco Firepower provides full contextual threat analysis and protection, with awareness into users, user history on every machine, mobile devices, client-side applications, operating systems, virtual machine-to-machine communications, vulnerabilities, threats, and URLs.	Limited User awareness only.	Limited User awareness only unless separate endpoint software is used.	Limited User awareness only unless separate endpoint software is used.
NGIPS	Next-gen Next-generation IPS with real-time contextual awareness and network mapping.	Signature-based	Signature-based	Signature-based
Integrated advanced threat protection	✓ Built-in, dynamic sandboxing capabilities (AMP-ThreatGrid), detects evasive and sandbox-aware malware, actionable event correlations, >1000 behavioral IoCs, billions of malware artifacts, and easy-to-understand threat scores.	Limited Sandbox available as cloud subscription or on-premises appliance.	Limited Sandbox available as cloud subscription or on-premises appliance.	Limited Sandbox available as cloud subscription or on-premises appliance.
Malware remediation	✓ Intelligent automation from Cisco AMP for Networks allows you to quickly understand, scope, and contain an active attack even after it happens.	Limited No root cause or trajectory results in an unknown threat scope. Remediation is a manual process during post-breach incident response.	Limited No root cause or trajectory results in an unknown threat scope. Remediation is a manual process during post-breach incident response.	Limited No root cause or trajectory results in an unknown threat scope. Remediation is a manual process during post-breach incident response.

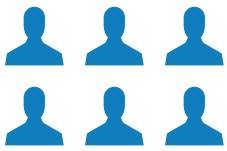
DID YOU KNOW?

"Attacks like WannaCry and Nyetya exposed how unprepared many businesses are to the evolution of malware."

(source: 2018 Cisco Annual Cybersecurity Report)

Learn more

	Cisco	Palo Alto Networks	Fortinet	Check Point Software Technologies
Threat Intelligence (Talos)				
Unique malware samples per day	1.5 million	10s of thousands	10s of thousands	10s of thousands
Threats blocked per day	19.7 billion Excludes email	Not reported	Not reported	Not reported
Email messages scanned per day	600 billion Of the 600B scanned, more than 85% are spam.	Not reported	6 million	Not reported
Web requests monitored per day	16 billion Web requests monitored by WSA/CWS per day. For perspective, Google processes 3.5 billion searches per day.	Not reported	35 million	Not reported
Automated intelligence feeds	✓ Security intelligence feeds are updated every 2 hours, adjustable to 5-minute intervals.	✓	✓	✓



DID YOU KNOW?

Cisco Talos consists of over 250 researchers, making it one of the largest threat intelligence organizations in the world.

See what they do

	Cisco	Palo Alto Networks	Fortinet	Check Point Software Technologies
Operational Capabilities				
Scanning architecture	Single pass	Single pass	ASIC	Multipass
Software-defined segmentation	✓ Cisco TrustSec and ACI provision security services separated from workload and deployment (physical, virtual, cloud). Security group tags (SGTs) segment software in the network.	✗	✗	✗
Automatic threat containment	✓ Cisco Rapid Threat Containment automates quarantine actions by the Cisco Identity Services Engine.	✗	✗	✗
Operations and management	Excellent Combined security and network operations. One console or HA pair of consoles provides all updates, patching, reporting, and threat information.	Limited Single UI for NGFW management. Additional UIs for malware, endpoint, or any other platform features.	Limited Single UI for NGFW management. Additional product and UI for logging and events. Additional product and UI for sandboxing.	Excellent Single manager of managers for each individual function of NGFW, ATP, etc.

	Cisco	Palo Alto Networks	Fortinet	Check Point Software Technologies
Operational Capabilities (continued)				
Deployment models	Typical Appliance, virtual instance (VMware), and public cloud (AWS and Azure)	Typical Appliance, virtual instance (VMware), and public cloud (AWS and Azure)	Typical Appliance, virtual instance (VMware), and public cloud (AWS and Azure)	Typical Appliance, virtual instance (VMware), and public cloud (AWS and Azure)
eStreamer API	✓ Cisco Firepower can stream event data and host-profile information to client applications, SIEM and SOC platforms, enhancing your actionable intelligence.	✗	✗	✗
Remediation API	✓ Cisco Firepower can work in conjunction with third-party products. It can change an asset's VLAN or access controls, or even open a ticket with the help desk.	✗	✗	✗
Host API	✓ Other systems such as inventory, vulnerability & asset management, and Nmap can feed data into the Cisco Firepower platform.	✗	✗	✗

DID YOU KNOW?

"More than half of all attacks resulted in financial damages of more than US $500,000"

(source: 2018 Cisco Annual Cybersecurity Report)

Don't become a statistic

	Cisco	Palo Alto Networks	Fortinet	Check Point Software Technologies
Critical Infrastructure (ICS/SCADA)				
Hardened and ruggedized versions available	✓	✗ Must run VM version of NGFW on a separate server; includes loading and managing a supported hypervisor.	✓	✓
Base feature set	NGFW, AMP, NGIPS, threat intelligence NGFW includes application visibility, URL filtering, IPS, antivirus, user identity. Firepower also includes all key security enhancements mentioned above, such as NGIPS, Advanced Malware Protection (AMP), retrospection, impact analysis, etc.	NGFW only	NGFW only	NGFW only

	Cisco	Palo Alto Networks	Fortinet	Check Point Software Technologies
Critical Infrastructure (ICS/SCADA) (continued)				
SCADA rules	~250 ~250 rules based on Snort. Talos provides rules geared toward ICS industry. Third-party rules can be imported. Customers can build rules.	~100	~300	~180
Modbus, DNP, CIP pre-processors	✓ Modbus, DNP3, and BACnet. SCADA protocols are available through the Firepower system.	✓ Modbus, DNP3, OPC, ICCP, IEC 61850	✓ Modbus, DNP3, BACNet, MMS, OPC, Profinet, ICCP, IEC.60870.5.104, IEC.61850	✓ Modbus, DNP3, BACNet, MMS, OPC, Profinet, ICCP, IEC.60870.5.104, IEC.61850
Service Provider				
Carrier-class certification	✓ NEBS Level 3	✗	✓ NEBS Level 3	✓
Carrier-class features	✓ GTP v2, CG-NAT, Diameter, SCTP, SIP-signaling firewall	✗	✓ GTP v2, CG-NAT, Diameter, SCTP, SIP-signaling firewall	✓ GTP v2, CG-NAT, Diameter, SCTP, SIP-signaling firewall
Third-party services stitching	✓ Third-party and native containers can be seamlessly stitched together to run with Firepower Threat Defense.	✗	✗	✗
True DDoS	✓ Radware DefensePro vDOS container is integrated directly into the NGFW system (Cisco Firepower 9300).	✗	Limited Requires separate product.	Limited Requires separate product.

To learn more about the Cisco Next Generation Firewall (NGFW), visit www.cisco.com/go/ngfw