Ransomware Defense Competitive Cheat Sheet

Security. No Excuse.

Cisco® ASA with FirePOWER™ Services combines the security benefits of the Cisco Adaptive Security Appliance (ASA) firewall platform with industry-leading FirePOWER threat prevention to provide comprehensive protection from advanced threats.

Cisco ASA with FirePOWER Services – Competitor Highlights

Attribute	CheckPoint (CKPT)	Fortinet (FTNT)	Palo Alto Networks (PANW)	Cisco	Highlight/Benefit
Contextual awareness	✗	✗	✗	✔	Cisco ASA with FirePOWER Services is the only threat-centric solution that can see beyond the packet and provide contextual threat analysis and protection. It achieves this by correlating full-stack endpoint visibility with applications, OS, Vulnerabilities, device information, users associated with security events and more, Allowing for very high-efficacy and extremely accurate detection and prevention. Our competitors have no visibility beyond the packet and correlate no context to relate the packet to. This limits your customer's ability to optimise defenses with automation.
Visibility	✓	✓	✓	✔	Only Cisco has full-stack visibility from physical layer to application layer and from attacker to target. The more we see, the more we can correlate information, make intelligent analysis and take action, either with automation or manually. CheckPoint and Fortinet are limited to applications, URLs, users and agents. Palo Alto Networks is limited to applications, URLs, users and light content.
Threat intelligence	✓	✗	⊖	✔	Cisco FirePOWER Next-Generation Intrusion Prevention System (NGIPS) and Advanced Malware Protection (AMP) lead the pack in overall security effectiveness with 99.5% overall, according to an NSS Labs report[1] released in 2015. CheckPoint's overall security effectiveness was 96.4%. Fortinet's (1500D) next-generation firewall (NGFW) security effectiveness was 99.2%. Palo Alto Network's overall security effectiveness was 98%.

✔ Full Coverage ✓ Partial/Incomplete ⊖ Some Coverage ✗ Not Available

[1] Next Generation Firewall Product Analysis Published September 2014, NSS Labs

Ransomware Defense Competitive Cheat Sheet

Security. No Excuse.

Attribute	CheckPoint (CKPT)	Fortinet (FTNT)	Palo Alto Networks (PANW)	Cisco	Highlight/Benefit
Collective security intelligence	✗	✓	✓	✔	Collective Security Intelligence (CSI) ecosystem, led by the Talos Security Intelligence and Research Group, brings vast resources to provide real-time protection for customers against the latest known and unknown advanced threats. Cisco CSI delivers security protection and services through leading full coverage some coverage security researchers, infrastructure and partnerships.
Security automation and adaptability	✗	✗	✗	✔	Cisco automatically adapts defenses to dynamic changes in the network, in files, or with hosts, maintaining high levels of protection without the need for administrator intervention. Impact flags automatically alert security analysts to the most critical events, reducing wasted time and effort. Our competitors are not dynamic in their response to an attack and require some level of human intervention.
Continuous analysis with retrospective security	✗	✗	✗	✔	Retrospective security in the "after" phase of the attack continuum uses big data analytics to continue to investigate unclassified data beyond the event horizon, which defines the initial "point-in-time" disposition of an object as clean, unknown, or malicious. Using this continuous analysis and global security intelligence, Cisco can track, analyse and remediate advanced malware that uses new technologies to evade initial defenses but is later identified as malicious. No other vendor has this capability and other vendors can only make a determination based upon a specific point in time.
Single management platform	✗	✗	✗	✔	The new Cisco ASA with FirePOWER Services meets the varying needs of customers. The unified, on-box manager allows complete local system management of NGFWs, the Cisco FirePOWER NGIPS and AMP technologies. Cisco FireSIGHT® Management Center combines all of the management functions of the NGFW, NGIPS and AMP on a system-wide basis, into a single, hierarchical manager, including: advanced threat and malware defenses, sophisticated policy management and comprehensive event and information management with correlated security information and event management (SIEM) reporting. In addition, incident control systems, vulnerability management, network and data forensics and system-wide remediation are available in the Cisco FireSIGHT Management Center. Its increased accuracy and visibility reduces false positives, therefore improving operational efficiency and significantly lowering TCO.

✔ Full Coverage   ✓ Partial/Incomplete   − Some Coverage   ✗ Not Available

Ransomware Defense Competitive Cheat Sheet

Security.
No Excuse.

CheckPoint

Product Overview: UTM-1 Edge appliances, Power-1 appliances, Integrated Appliance Solutions (IAS), software blades and ThreatCloud

Cisco Value Differentiators

- Offers the only adaptive, threat-focused NGFW in the industry
- Offers a complete security and advanced threat solution in a single box
- Automatically adapts defense to dynamic changes in the network
- Only vendor to provide full-stack threat visibility from physical layer to application layer, from attacker to target
- Industry's leading IPS detection technologies and AMP effectiveness as proven by NSS Labs
- Only vendor with enough context to accurately and dynamically adapt security controls to a changing network and send out impact flags to alert the SecOps team to what threats are most critical
- Highest catch rate against malware URLs in the industry
- Includes total network visibility
- Only Cisco integrates and delivers NGFW services, NGIPS and AMP in the core product without the need for a separate client agent* or to add another product to the NGFW

Strengths

- Recognised as a firewall market leader in the Gartner Magic Quadrant
- Number two network security vendor
- Rich NGFW and firewall capabilities
- Customised and packaged feature offerings (software blades)
- Superior management compared to most vendors—highly regarded by industry as its best feature

*A client agent (AMP) may be added to further enhance local active response and remediation on the endpoint if desired.

Weaknesses

CheckPoint

- Missed out on the opportunities presented by market transitions to reach customers' security challenges such as advanced persistent threats (APTs), NGFW, endpoint security and mobile solutions
- Performance drops significantly as more features are enabled; most boxes sold are oversubscribed because of price and inflated numbers
- Very few customers turn on CheckPoint IPS because of overall box performance impact
- CheckPoint Threat Extraction isn't practical; it removes executable content from all files, regardless of intent

Visibility and Threat Context

- No visibility beyond the packet and no related threat context, limiting customers' ability to optimise defenses with automation or to provide an assessment of which events are critical and require immediate attention
- Has no client for endpoint visibility and therefore cannot determine if threats are relevant or false positive

Point-In-Time Analysis

- Only performs point-in-time detection and analysis, where verdicts are handed out when the packet is first seen

After an Attack

- Lacks continuous analysis, which means that any attacks that get through will run rampant on the network and no one will be able to determine the scope of the outbreak, the root cause, or provide an adaptive response

Ransomware Defense Competitive Cheat Sheet

Security.
No Excuse.

Fortinet

Product Overview: Unified Threat Management (UTM), Advanced Threat Protection: FortiSandbox, FortiAnalyzer and FortiManager

Cisco Value Differentiators

- Cisco FireSIGHT Management Center provides central management of Cisco ASA with FirePOWER Services
- World's most proven firewall; number one in global market share[2]
- Superior performance with services simplifying cost and complexity with fewer devices to deploy and manage
- Offers full-featured, enterprise-class security
- More effective at blocking known and zero-day threats
- Supports both interface-based and zone-based security in Layer 3 firewall
- Only Cisco integrates and delivers NGFW services, NGIPS and AMP in the core product without the need for a separate client agent* or to add another product to the NGFW

Strengths

- UTM mindshare leader[3]
- Application-specific integrated circuit (ASIC), high-performance architecture
- Low cost: Less than 50% of comparable offerings
- Broad breadth of NGFW and UTM security offerings
- Performance is normally understated; systems are fast and accurate; will drop fewer packets than any other competitor at scale.[4]

Weaknesses

FortASIC

- New features run on x86 processors until included into an ASIC
- ASIC gap is typically18 months
- New features and integration suffer greatly, especially when integrated with ASIC-based features, which brings the overall system performance down

Visibility and Threat Context

- No visibility beyond the packet and no related threat context, limiting customer's ability to optimise defenses with automation or to provide an assessment of which events are critical and require immediate attention

Point-In-Time Analysis

- Only performs point-in-time detection and analysis, where verdicts are handed out when the packet is first seen

After an Attack

- Lacks continuous analysis, which means that any attacks that get through will run rampant on the network and no one will be able to determine the scope of the outbreak, the root cause, or provide an adaptive response

*A client agent (AMP) may be added to further enhance local active response and remediation on the endpoint if desired.

[2] Infonetics: https://cisco.jiveon.com/docs/DOC-1053153 (Page 9)

[3] Gartner UTM MQ: http://www.gartner.com/reprints/vol-3?id=1-2M0PNV1&ct=150827&st=sb

[4] NSS Labs 2014 NGFW–(Latency), Meircom Cisco NGFW and Internal Testing

cisco

Ransomware Defense Competitive Cheat Sheet

Security.
No Excuse.

Palo Alto Networks

Product Overview: NGFW solutions, including the new PA-200 and PA 500, virtualised firewall and WildFire advanced malware protection

Cisco Value Differentiators

- Offers the only adaptive, threat-focused NGFW in the industry
- Offers a complete security and advanced threat solution in a single box
- Automatically adapts defense to dynamic changes in the network
- Only vendor to provide full-stack threat visibility from physical layer to application layer, from attacker to target
- Industry's leading IPS detection technologies and AMP effectiveness as proven by NSS Labs
- Only vendor with enough context to accurately and dynamically adapt security controls to a changing network and send out impact flags to alert the SecOps team to what threats are most critical
- Highest catch rate against malware URLs in the industry
- Only Cisco integrates and delivers NGFW services, NGIPS and AMP in the core product without the need for a separate client agent* or to add another product to the NGFW

Strengths

- NGFW mindshare leader[4]
- Very strong NGFW capabilities, rich reporting and simplified management
- Broad range of firewalls with decent performance and application-access controls

Weaknesses

Prevention

- Focuses purely on prevention and claims that this is 100% effective
- If the NGFW was 100% effective, as claimed, there would be no need for the TRAPS agent
- TRAPS endpoint is a Microsoft Windows-only agent and can only gather forensic information during an attack
- TRAPS endpoint doesn't allow customer to know who attacked them or why

Visibility and Threat Context

- No visibility beyond the packet and no related threat context, limiting customer's ability to optimise defenses with automation or to provide an assessment of which events are critical and require immediate attention

Point-In-Time Analysis

- Only performs point-in-time detection and analysis, where verdicts are handed out when the packet is first seen

After an Attack

- Lacks continuous analysis, which means that any attacks that get through will run rampant on the network and no one will be able to determine the scope of the outbreak, the root cause, or provide an adaptive response
- When an attack does get through, customers won't have the ability to do anything about it

*A client agent (AMP) may be added to further enhance local active response and remediation on the endpoint if desired.

[4] https://cisco.jiveon.com/docs/DOC-1053153 (Slide 21) and www.paloaltonetworks.com

For more information, refer to the Cisco ASA with FirePOWER Services At-a-Glance and Call Guide (Midmarket) or visit www.cisco.com/go/asa