Malware Defense With Cisco Secure Firewall

Contents

Product overview

Today's attacks are stealthy and evasive, designed to bypass traditional perimeter defenses like firewalls, antivirus software, and intrusion prevention systems. Having an industry-leading perimeter defense is a key part of any security strategy, but these tools will never be 100 percent effective. Fighting malware effectively today requires new approaches, strategies, and advanced threat capabilities. Malware Defense with Cisco® Secure Firewall delivers network-based advanced malware protection that goes beyond point-in-time detection to protect your organization across the entire attack continuum—before, during, and after an attack. Malware Defense detects, blocks, tracks, and contains malware threats across multiple threat vectors within a single system. It also provides the visibility and control necessary to protect your organization against highly sophisticated, targeted, zero day, and persistent advanced malware threats. To active Malware Defense, purchase the Malware Defense licence for Cisco Secure Firewall.

With Malware Defense, you can:

- **Trust protection that moves beyond point-in-time:** Malware Defense goes beyond point-in-time detection to analyze files and traffic continuously. This capability helps enable retrospective security, the ability to look back in time and trace processes, file activities, and communications. You can understand the full extent of an infection, establish root causes, and perform remediation. The result: more effective, efficient, and pervasive protection for your organization.
- **Limit policy-violating files and more:** Tracking data that comes through the web, email, or other attack vectors, Malware Defense automatically recognizes files and applications. It then performs broad-based filtering of files using the application and file control policies that you set.
- **Detect and block exploit attempts:** With an inline deployment, the Cisco solution can detect and block client-side exploit attempts. You're also protected against vulnerability exploit attempts aimed at Adobe Acrobat, Java, Flash, and other commonly targeted client applications.
- **Identify, block, and analyze malicious files:** The system blocks malicious files from their target system and analyzes files with an unknown disposition. If no disposition is returned, the suspect file will automatically be submitted to Cisco Secure Malware Analytics (formerly Threat Grid) for further analysis.
- **Go beyond just sandboxing:** Malware Defense includes built-in sandboxing capabilities, but with the integration of Secure Malware Analytics, malware analysis and threat intelligence are taken to a whole new level. Secure Malware Analytics provides more than 700 unique behavioral indicators to analyze the actions of a file and help you understand what malware is doing, or attempting to do, and how large a threat it poses to your organization. You get easy-to-understand threat scores and billions of malware artifacts at your disposal for exceptional scale and coverage from global threats.
- **Analyze files and traffic continuously:** Determining that an observed file is malicious triggers retrospective alerts from Malware Defense, even if the file traversed the network hours or days in the past, so you can still take action and mitigate damage.
- **Correlate discrete events into coordinated attacks:** Malware Defense illustrates the risk associated with an ongoing attack. It provides automated and prioritized lists of potentially compromised devices with combined security event data from multiple event sources.
- **Track malware's spread and communications:** With the file trajectory feature of Malware Defense, you can track a file's transmission across the network. Each file in the file trajectory view has an associated trajectory map with a visual display of the file's transfers over time as well as additional information about the file.

- **Contain malware to prevent loss and outbreaks:** Blocking advanced threats and malware communications with a simple policy update is easy with Malware Defense. With custom detection lists, you are empowered to act whenever you want, without waiting for a vendor-supplied update to take action.

Effective security requires more than detection

Point-in-time detection alone will never be 100 percent effective. It takes only one threat that evades detection to compromise your environment. Using targeted context-aware malware, sophisticated attackers have the resources, expertise, and persistence to outsmart point-in-time defenses and compromise any organization at any time. Furthermore, point-in-time detection is completely blind to the scope and depth of a breach after it happens, rendering organizations incapable of stopping an outbreak from spreading or preventing a similar attack from happening again.

Malware Defense is the only network-based system that goes beyond point-in-time detection and uses an integrated set of controls and continuous analysis capabilities to detect, confirm, track, analyze, and remediate threats to protect you across the entire advanced malware attack continuum—before, during, and after an attack. Before an attack, Malware Defense prevents known malware, as well as policy-violating file types and communications, from entering your network—thereby reducing your attack surface. During an attack, exploit attempts and malicious files and traffic are detected and blocked.

After an attack, recognizing that preemptive detection and blocking methods are not 100 percent effective, Malware Defense system continues to analyze files and network traffic for stealthy threats that may have evaded initial detection. If new Indications of Compromise (IoCs) arise, the system automatically correlates multiple sources of security event data like retrospective malware alerts, intrusion events, and malware callback attempts into a single prioritized view. So now, in the event of an attack, this intelligent automation allows you to quickly and efficiently understand, scope, and contain an active attack even after it happens. This reduces the critical discovery-to-containment period and allows you to stop the spread of malware before it can cause damage.

Malware Defense also reduces the number of actionable events you deal with on a daily basis and provides actionable insights so you can spend your time addressing the high-risk advanced malware threats that matter most.

Furthermore, Malware Defense integrates with Cisco Secure Endpoint to increase security effectiveness across multiple control points. With AMP in more places, you get more eyes watching more attack vectors, continuously monitoring for malicious behavior across the extended network. Using continuous analysis, retrospective security, and multisource Indications of Compromise (IoCs), you can identify stealthy attacks that manage to traverse from the network to the endpoint, or enter through your email or web gateways, and correlate those events for faster response, and achieve greater visibility and control.

Unmatched security intelligence and malware analysis

Malware Defense is built on big data and exceptional security intelligence. The Cisco Talos® Security Intelligence and Research Group and the Secure Malware Analytics threat intelligence feeds represent the industry's largest collection of real-time threat intelligence with the broadest visibility, the largest footprint, and the ability to put it into action across multiple security platforms. This data is then pushed from the cloud to the Malware Defense system, providing you the latest threat intelligence at all times.

Organizations benefit from a large collection of real-time threat intelligence, including:

- 1.5 million incoming malware samples per day
- 13 billion web requests
- 1.6 million global sensors
- Team of more than 250 engineers, technicians, and researchers
- 100 terabytes of data per day
- 24-hour operations

Malware Defense automatically correlates files, behavior, telemetry data, and activity against this robust, context-rich knowledge base to block threats trying to infiltrate the network. It provides security teams with a greater awareness of threats within the network and allows for faster and easier incident response.

The integration of our Secure Malware Analytics sandboxing technology into Malware Defense also provides over 700 unique behavioral indicators that evaluate the actions of a file submission, not just its structure. You gain insight to unknown malware, including the associated HTTP and DNS traffic, the TCP/IP streams, the processes that it's affecting, and registry activity.

Secure Malware Analytics also provides users with context-rich, actionable content everyday—more than 8 million samples are analyzed each month, resulting in billions of artifacts. And finally, highly accurate content feeds, delivered in standard formats to seamlessly integrate with existing security technologies, enable organizations to generate context-rich intelligence specific to their organization.

Limit policy-violating files and more

Malware Defense lets you define the types of files that are allowed through the system. Whether files arrive from the web, email, or other attack vectors, the system automatically recognizes files and applications. It then performs a broad-based filtering of files using the application and file control policy that you set (see Figure 1). These policies can apply to inbound and outbound files, allowing you to control files downloaded and uploaded, and it addresses both external and internal threat actors.

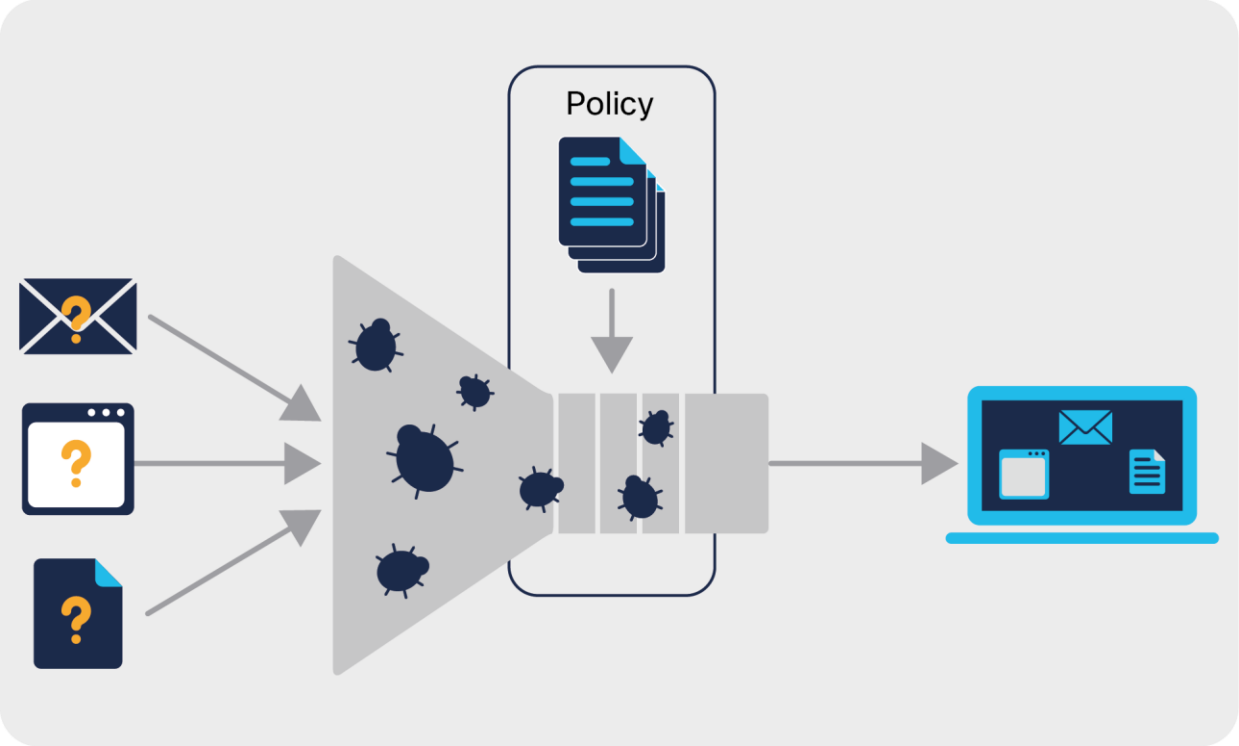

Figure 1.
Limit policy-violating files

The system also includes global security intelligence feeds that dynamically block connections that are known to be malicious. An optional URL filtering license allows you to block attempts to download files from websites and domains categorized as malicious.

Detect and block exploit attempts

Capabilities of Malware Defense license complement those of the Cisco Secure Firewall IPS license (formerly NGIPS). When the system is deployed in line, it detects and blocks client-side exploit attempts that can lead to malicious file downloads, commonly referred to as drive-by attacks. Cisco IPS can also protect against other vulnerability exploit attempts aimed at web browsers, Adobe Acrobat, Java, Flash, and other commonly targeted client applications. Acting as early as possible in the attack chain, the system attempts to limit collateral damage and avoid costly cleanup efforts.

Detect, block, and analyze malicious files

Malware Defense uses the Cisco Talos cloud to obtain real-time file dispositions across multiple attack vectors, like web and email. Known malicious files are blocked from reaching their target system. Files with an unknown disposition are automatically submitted to the Secure Malware Analytics dynamic analysis engine. A threat score is computed for analyzed files, and a detailed threat report from Secure Malware Analytics is available in the management console to aid in decision making. Files of any type can optionally be saved to the system and safely retrieved to enable further analysis manually.

Continuously analyze files and traffic

Typical network-based antimalware systems inspect malware only at the point in time when it traverses the network device. Since no detection technology is 100 percent effective and advanced malware can disguise itself to evade first-line defenses, you often lose visibility after the initial inspection is performed.

Cisco solves this challenge by using big data analytics for continuous analysis in addition to point-in-time detection. This continued analysis can result in a malicious verdict after the malware is first inspected and allowed to pass through the device. Continuous analysis is a key enabler of retrospective security (Figure 2).

Retrospective alerts from Malware Defense tell you when an observed file is determined to be malicious, even if the file traversed the network hours or days in the past, allowing you to take action and mitigate the damage.

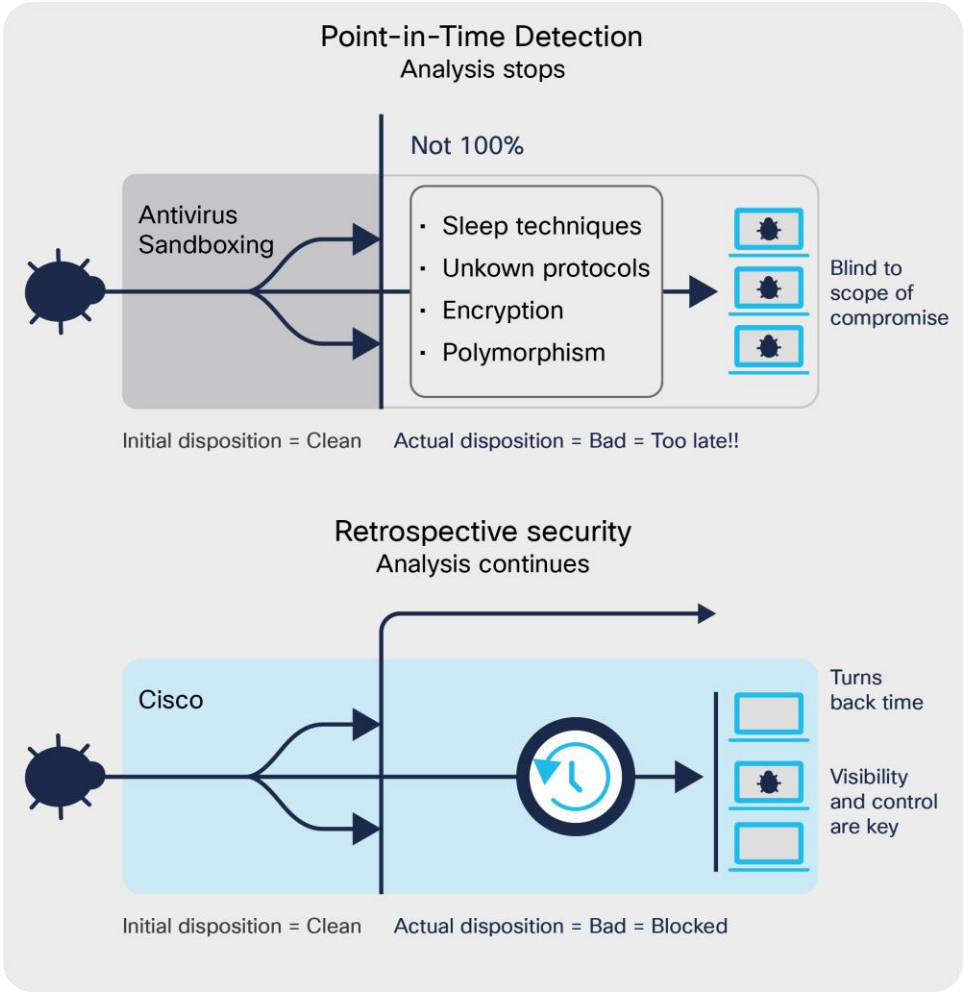

Figure 2.
Point-in-time detection compared with continuous analysis and retrospective security

Correlate discrete events into coordinated attacks

The capability of Malware Defense license leverages Cisco Firewall Management Center (Figure 3), Cisco's discovery and awareness technology. It collects information about hosts, operating systems, applications, users, files, networks, geolocation information, and vulnerabilities. Malware Defense combines these discrete but related events into an aggregate view called IoCs in the Firewall Management Center.

Figure 3.
Cisco Firewall Management Center

This view provides an automated and prioritized list of potentially compromised devices, with combined security event data from multiple event sources to illustrate the risk associated with an ongoing attack (Figure 4). With this added contextual data, you can make more informed decisions and determine the best course of action.

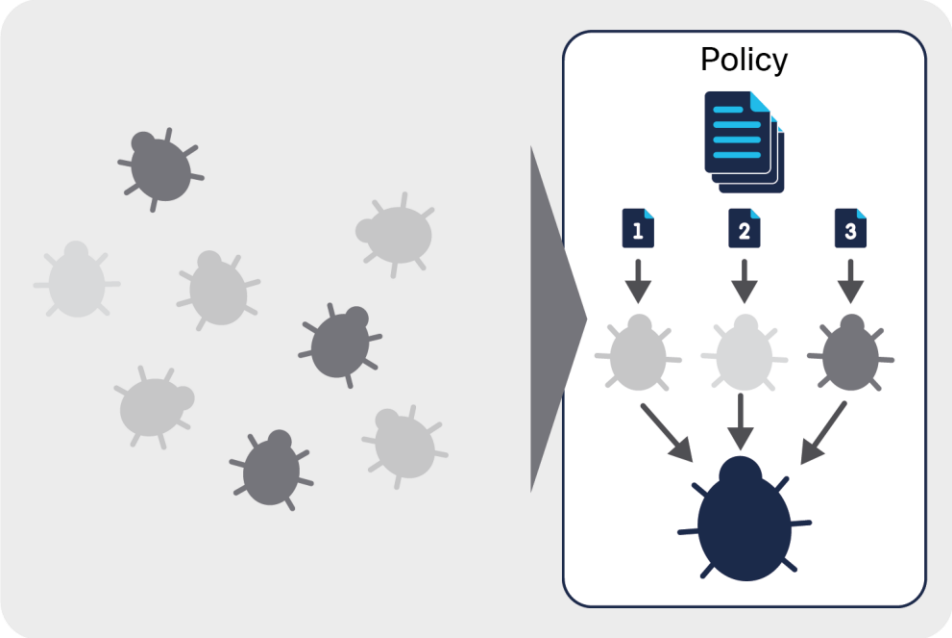

Figure 4.
Event correlation

Track malware's spread and communications

Malware Defense uses a file trajectory feature to allow you to track a file's transmission across the network. Each file in the file trajectory view has an associated trajectory map, which contains a visual display of the file's transfers over time as well as additional information about the file.

File trajectory is essential to determining the impact and scope of a potential infection. Essential Firewall Management Center data is included with the view to aid decision making. Contextual information like the target system and the users of that system, as well as protocol and communication attempts, are all available to better understand the risk associated with the file.

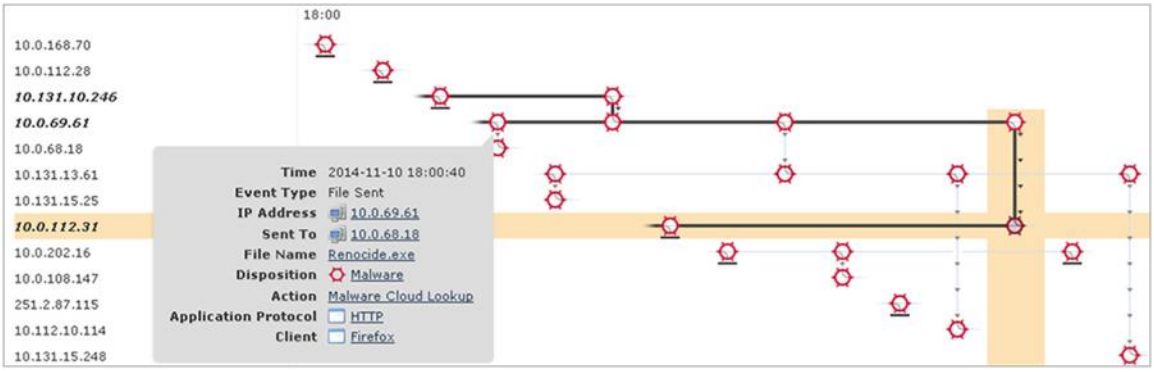

Figure 5.
File trajectory

Contain malware to prevent loss and outbreaks

When you make the decision to take action against an active attack, Malware Defense allows you to quickly contain the outbreak. You can block files and malware communications with a simple policy update. With custom detection lists, you are empowered to act whenever you decide to do so; there's no need to wait for a vendor-supplied update to take action.

Table 1 highlights the best-in-class capabilities of Malware Defense with Cisco Secure Firewall.

Table 1. Features and benefits of Malware Defense with Cisco Secure Firewall

Feature	Benefits
Continuous analysis	Once a file lands on the network, Malware Defense continues to watch, analyze, and record all file activity, regardless of the file's disposition. When malicious behavior is detected, Malware Defense shows you the recorded history of the malware's behavior over time to help you scope the compromise and respond quickly.
Retrospective security	Retrospective security is the ability to look back in time and trace processes, file activities, and communications in order to understand the full extent of an infection, establish root causes, and perform remediation. The need for retrospective security arises when any indication of a compromise occurs, such as an event trigger, a change in the disposition of a file, or an IoC trigger.
Firewall Management Center	Gain visibility into your environment through a single pane of glass—with a view into hosts, operating systems, applications, users, files, networks, geolocation information, and vulnerabilities—to provide a comprehensive contextual view so that you can make informed security decisions.
Comprehensive global threat intelligence	The Cisco Talos Security Intelligence and Research Group and the Secure Malware Analytics intelligence feeds represent the industry's largest collection of real-time threat intelligence with the broadest visibility, the largest footprint, and the ability to put it into action across multiple security platforms.
Indications of compromise	File, telemetry, and intrusion events are correlated and prioritized as potential active breaches, helping security teams to rapidly identify malware incidents and connect them to coordinated attacks.
File reputation	Advanced analytics and collective intelligence are gathered to determine whether a file is clean or malicious, allowing for more accurate detection.
File analysis and sandboxing	Secure Malware Analytics' highly secure environment helps you execute, analyze, and test malware behavior to discover previously unknown zero-day threats. The integration of Secure Malware Analytics' sandboxing technology into Malware Defense results in more dynamic analysis checked against a larger set of behavioral indicators.
Retrospective detection	Alerts are sent when a file disposition changes after extended analysis, giving you awareness and visibility to malware that evaded initial defenses.
File trajectory	Continuously track file propagation over time throughout your environment in order to achieve visibility and reduce the time required to scope a malware breach.

Feature	Benefits
Integrated SSL decryption	Identifies and decrypts SSL encrypted network traffic and performs inspection and detection on that traffic. You can also enforce SSL certificate policies and enable central SSL policy control for the network.
Integration with Secure Endpoint	Malware Defense through the Malware Defense license is compatible with Cisco Secure Endpoint, an advanced malware protection product for PCs, Macs, Linux, mobile devices, and virtual systems. By deploying both systems, your organization can achieve unmatched visibility and control throughout your entire extended IT ecosystem.
Integration with Threat Grid	The integration of Secure Malware Analytics' sandboxing technology and advanced malware analysis capabilities into Malware Defense provides over 800 unique behavioral indicators analyzing the actions of a file, easy-to-understand threat scores, and billions of malware artifacts at your disposal for exceptional scale and coverage from global threats.

Product performance and specifications

You can deploy Malware Defense license on any Cisco Secure Firewall appliance. However, the Cisco AMP dedicated appliances AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, and AMP8390 (see Table 2) give you all the benefits offered in the Malware Defense solution. They are deployed on appliance models that offer dedicated processing power and storage to meet specific goals in demanding environments.

Table 2. Hardware specifications: Dedicated Cisco AMP for Networks appliances

	AMP7150	AMP8050	AMP8150	AMP8350	AMP8360	AMP8370	AMP8390
Advanced Malware Protection throughput[1]	500 Mbps	1 Gbps	2 Gbps	5 Gbps	10 Gbps	15 Gbps	20 Gbps
Max monitoring interfaces[2]	12	12 (3 x 4-port RJ-45 NetMods)	12 (3 x 4-port RJ-45 NetMods)	28 (7 x 4-port RJ-45 NetMods)	24 (6 x 4-port RJ-45 NetMods)	20 (5 x 4-port RJ-45 NetMods)	16 (4 x 4-port RJ-45 NetMods)
Fixed monitoring interfaces	4 x 10/100/1000 (RJ-45)	0	0	0	0	0	0
Modular interfaces	8 SFP (1GB) No failover	Yes (requires NetMods)	Yes (requires NetMods)	Yes (requires NetMods)	Yes (requires NetMods)	Yes (requires NetMods)	Yes (requires NetMods)
NetMod expansion slots	0	3	3	7	6	5	4
Programmable fail-open interfaces	4 x 10/100/1000 (RJ-45)	Yes (requires NetMods)	Yes (requires NetMods)	Yes (requires NetMods)	Yes (requires NetMods)	Yes (requires NetMods)	Yes (requires NetMods)

	AMP7150	AMP8050	AMP8150	AMP8350	AMP8360	AMP8370	AMP8390
Management interfaces	1 x 10/100/1000 (RJ-45)	1 x 10/100/1000 (RJ-45)	1 x 10/100/1000 (RJ-45)	2 x 10/100/1000 (RJ-45)	2 x 10/100/1000 (RJ-45)	2 x 10/100/1000 (RJ-45)	2 x 10/100/1000 (RJ-45)
Average latency	<150 microseconds	<150 microseconds	<150 microseconds	<150 microseconds	<150 microseconds	<150 microseconds	<150 microseconds
Storage capacity (SSD)	120 GB	400 GB+	400 GB	400 GB+	800 GB+	1200 GB+	1600 GB+
Stackable	No	No	No	Yes	Yes	Yes	Yes
Cooling fans	5	10	10	6	12	18	24
Power supplies	2 (hot swappable)	2 (hot swappable)	2 (hot swappable)	2 (hot swappable)	4 (hot swappable)	6 (hot swappable)	8 (hot swappable)
Form factor	1RU	1RU	1RU	2RU	4RU	6RU	8RU
Dimensions in inches (depth x width x height)	21.6 x 19.0 x 1.73	27.25 x 16.93 x 1.7	27.25 x 16.93 x 1.7	29 x 17.2 x 3.48	29 x 17.2 x 6.96	29 x 17.2 x 10.44	29 x 17.2 x 13.92
Maximum shipping weight	29 lb (13.2 kg)	54 lb (25.5 kg)	54 lb (25.5 kg)	67 lb (30.5 kg)	2 X 67 lb	3 x 67 lb	4 X 67 lb
AC voltage[3]	100–240 VAC (nominal)	100–240 VAC (nominal)	100–240 VAC (nominal)	100–240 VAC (nominal)	100–240 VAC (nominal)	100–240 VAC (nominal)	100–240 VAC (nominal)
	90–264 VAC (max)	85–264 VAC (max)	85–264 VAC (max)	85–264 VAC (max)	85–264 VAC (max)	85–264 VAC (max)	85–264 VAC (max)
Current[4]	8A (max over full range)	8A (max over full range)	8A (max over full range)	11A (max over full range)	2 X 11A	3 X 11A	4 X 11A
DC voltage option	No	No	No	Yes	Yes	Yes	Yes
Max power output[5]	450W	650W	650W	1000W	2 X 1000W	3 X 1000W	4 X 1000W
Avg power consumption[7]	200W	400W	400W	635W	2 X 635W	3 X 635W	4 X 635W

	AMP7150	AMP8050	AMP8150	AMP8350	AMP8360	AMP8370	AMP8390
Operating temperature	5–40° C	10–35° C	10–35° C	5–40° C	5–40° C	5–40° C	5–40° C
Frequency range	47–63 Hz	47–63 Hz	47–63 Hz	47–63 Hz	47–63 Hz	47–63 Hz	47–63 Hz
Air flow	Front to back	Front to back	Front to back	Front to back[6]	Front to back[6]	Front to back[6]	Front to back[6]
Btu/hour rating (heavy load)	900 Btu	1725 Btu	1725 Btu	2900 Btu	2 X 2900 Btu	3 X 2900 Btu	4 X 2900 Btu
Operating humidity	5–85%	5–85%	5–85%	5–85%	5–85%	5–85%	5–85%
RoHS compliant	Yes	Yes	Yes	Yes	Yes	Yes	Yes

[1] AMP throughput numbers are inclusive of Firewall, IPS, and AMP features enabled. Exact network performance experienced will vary depending on conditions outside of the control of Cisco, including applied policies, protocol mix, and average packet size inspected.

[2] NetMods may be failover or nonfailover.

[3] All chassis have the same voltage input.

[4] Each chassis will pull current.

[5] Each chassis power supply is rated for 1000W of output power to chassis.

[6] Has two 1" sq. side intakes per appliance.

[7] Power supplies are 1+1 redundant.

[8] AMP 8360, 8370, and 8390 are stacked appliances; therefore certain specifications are simply multiplied by the number in each stack (2, 3, and 4, respectively).

[*] Specifics around NGIPS/NGFW performance numbers can be referenced on the Cisco Firepower appliance Data Sheet at www.cisco.com/go/ngips.

[**] Secure Firewall appliances and dedicated AMP appliances maintain the same platform equivalency (for instance, FP8350 versus AMP8350) and are same appliances + integrated malware storage pack.

Software requirements

Software requirements are outlined in Table 3.

Table 3. Software requirements

Network-based advanced malware protection: • Supported on all Cisco Firepower® 7000 and 8000 Series appliances, and the virtual 64-bit appliance • Supported on all Cisco Firepower 4100 and 9300 Series appliances • Requires v5.3 or later • Requires Cisco Firewall Management Center (the Management Center requires connection over Internet to the Collective Security Intelligence cloud or the on-premises Cisco AMP Private Cloud Virtual Appliance)	File types supported for reputation lookup (with example extensions): • Microsoft Office documents (doc and xls) • Portable documents (pdf) • Archive files (jar) • Multimedia files (swf) • Executable binaries (msexe and jar.pack)
Supported application protocols: • HTTP • SMTP • IMAP • POP3 • FTP • NetBIOS-ssn (SMB)	Dispositions for reputation lookups: • Clean (known good) • Unknown (neutral or not enough data) • Malicious (known bad)
Bidirectional inspection and control	Actions for file identification: • Detect or block (by file type, transfer direction, or protocol) • Malware cloud lookup (query for reputation)
Supports blocking of file by geographical source or destination	Event types or data sources supported for IoC correlation: • IPS events (network) • Cisco Secure Endpoint • Malware events (network) • Security intelligence (network plus endpoint) • Cisco Firepower contextual data
Supports dynamic blocked lists provided by the Collective Security Intelligence cloud	Custom detections (user-defined blocked and allowed lists)
Automated submission for dynamic analysis in the Collective Security Intelligence cloud: • Microsoft executables (msexe, dll) • Threat score and dynamic analysis reports available after analysis	

Platform support and compatibility

The solution comprises the Secure Firewall appliance of your choosing, with the Malware Defense license, and optional subscriptions for IPS, applications, and URL Filtering. Malware Defense license is managed through the Cisco Firewall Management Center.

Warranty information

Find warranty information at the Cisco.com Product Warranties page.

Ordering information

To place an order, visit the Cisco Ordering Home Page, contact your Cisco sales representative, or call us at 800 553 6387.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

For more information

For more information, please visit the following link:

- Malware Defense license for Cisco Secure Firewall

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-733182-08 03/21