ANTIMALWARE SUPPORT WITH ENHANCED ENDPOINT SECURITY LICENSE

Product Overview

Juniper Networks MAG Series Junos Pulse Gateways, SA Series SSL VPN Appliances, and IC Series Unified Access Control Appliances—the policy management servers at the heart of Unified Access Control—deliver dynamic antimalware download capabilities to endpoint devices such as Microsoft Windows-based laptops and desktop PCs through the Enhanced Endpoint Security license. Malware cost enterprises time, money, and productivity—requiring them to locate infected endpoints, place them under quarantine, and remediate those endpoints before granting them network access. Juniper's Enhanced Endpoint Security antimalware offering protects valuable and sensitive corporate resources from being harmed by infected endpoints on the LAN and the WAN.

Product Description

The number of newly discovered malicious programs that can infiltrate and harm endpoint devices, such as PCs, continues to grow and replicate at an alarming rate. Often, malware are designed to steal confidential data for financial gain. These insidious programs can be hidden deep within a downloaded program or as a rootkit, and can remain undetected for long periods of time—until they are hatched and spring to life. As a result, organizations must have a powerful solution in place to combat malware across all endpoints on their LAN and for their remote users. Otherwise, malware can cost their enterprise an increasing amount of money annually in an effort to quarantine and remediate infected endpoints.

To prevent your endpoints—either on the LAN or WAN—from being infected with malware, Juniper Networks® offers the Enhanced Endpoint Security license option with its MAG Series Junos Pulse Gateways, SA Series SSL VPN Appliances, or Unified Access Control solutions. This license provides a full-featured, dynamically deployable antimalware module that is an OEM of Webroot's industry-leading Spy Sweeper product. With this new capability, organizations can ensure that unmanaged and managed Microsoft Windows endpoint devices conform to corporate security policies before they are allowed access to the network, applications, and resources. For example, potentially harmful keyloggers can be found and removed from an endpoint device before users enter sensitive information such as their user credentials. The Enhanced Endpoint Security license protects endpoints from infection in real time and ensures that only clean endpoints are granted network access.

Architecture and Key Components

The Enhanced Endpoint Security antimalware module is offered as part of the Enhanced Endpoint Security licenses for the MAG Series Junos Pulse Gateways, SA Series, and IC Series These new antimalware capabilities utilize a signature database to detect malware and threats. The signature database is facilitated and updated through an automatic download from the Webroot website, along with information on the definition version and the date/time of the last successful download. These new antimalware capabilities are delivered to each user device via an .msi package, downloaded to each endpoint and silently installed.

If customers have already installed the commercially available version of Webroot's Spy Sweeper on their endpoint devices, the new Enhanced Endpoint Security antimalware protection module in MAG Series, UAC, or the SA Series simply determines the device's real-time protection status through Spy Sweeper. In this instance, no real-time threat or remediation information would be available to the MAG Series, SA Series, or UAC, since the already loaded commercial version of Spy Sweeper is fully protecting the device from malware and threats. Policy decisions for real-time protection status are determined by periodic queries—at intervals of 15 to 30 seconds—of the commercially available Spy Sweeper installed on the user's endpoint.

Enhanced Endpoint Security performs its memory, registry and selected folder scans during initial handshake. Any threat detected in real time during the scan process is immediately reported back through the MAG Series, SA Series, or UAC's existing granular policy management framework and addressed through quarantine and automatic remediation.

The Enhanced Endpoint Security licenses for the MAG Series, SA Series, and UAC are available in 1-year, 2-year, and 3-year subscription options (see the "Ordering Information" section for more details) and can be used with any MAG Series Junos Pulse Gateway model, Juniper Networks SA Series SSL VPN Appliances—including the SA2500, SA4500, SA4500 FIPS, SA6500, and SA6500 FIPS—and Juniper Networks IC Series Unified Access Control Appliances, including the IC4500, IC6500, and IC6500 FIPS products.

Enhanced Endpoint Security for LAN Users

For the LAN environment, organizations might not only have employees—but also contractors, partners, and guests—who need to access their corporate network resources while they are at the corporate office, in order to be productive. However, granting access to these users can open the organization and its network to infiltration from all sorts of malware. For example, consider the case of a contractor who comes to the office and needs to connect his own personal, unmanaged laptop to your network. Earlier, the contractor inserted a USB memory stick into the laptop to download a large file and the USB memory stick was riddled with malware, infecting the unmanaged laptop that is now going to be connected to your network—potentially inflicting harm to or providing a hack into your corporate network and sensitive resources. But, with Juniper Networks MAG Series or Unified Access Control and its Enhanced Endpoint Security module, when the contractor attempts to log in to your network, the IC Series appliance—the centralized policy engine of UAC—dynamically downloads antimalware software to the contractor's laptop, detects the insidious malware, quarantines the laptop, and removes the malware—all before the user can log in to your network with his device!

Another example is a full-time employee whose PC has been infected with a keylogger program hidden in a rootkit. A keylogger program can capture all of the employee's keystrokes on his PC including his username and password information. When the employee tries to log in to the network, the IC Series appliance dynamically downloads the licensed Enhanced Endpoint Security module to the PC, detects the rootkit hidden deep in the recesses of the system's memory, and removes the keylogger program before the employee and his contaminated device are allowed network access. Figure 1 provides a visual depiction on how the IC Series with a licensed Enhanced Endpoint Security module addresses the infected devices in both of these examples. In this example, all the endpoints attempting access to your LAN are scrubbed clean of any malware before they are allowed entry to your network—alleviating any damage from malware and mitigating potential breaches and threats.

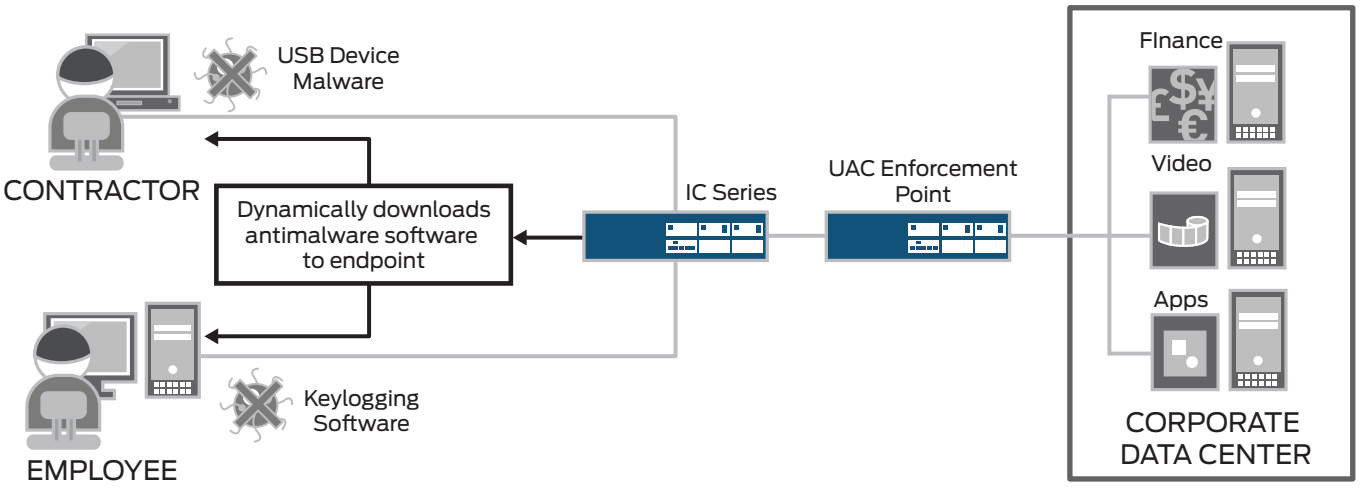

Figure 1: LAN access with Enhanced Endpoint Security

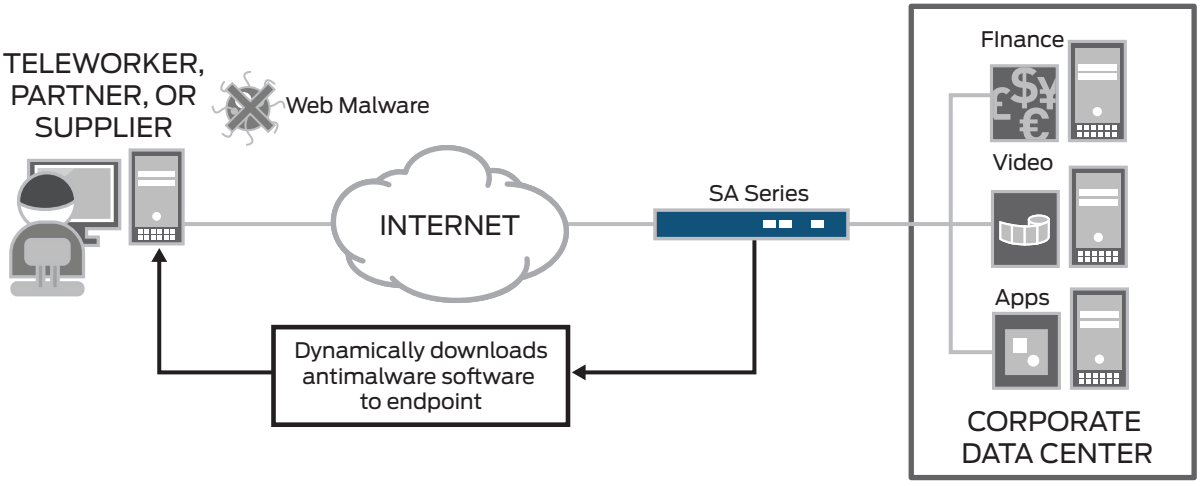

Figure 2: Remote access with Enhanced Endpoint Security

Enhanced Endpoint Security for Remote Users

For the remote access environment, you typically have users—such as teleworkers, partners, or suppliers—who need access to corporate resources from any location at any time in order to stay productive. In this scenario, this could mean various malware entering the corporate network from remote users at various locations. Let's look at the case of a teleworker who works primarily from home. This teleworker might be using his laptop not only to access the corporate network, but also occasionally for personal tasks. For example, the teleworker might have visited a search engine website and a malware program was installed on his laptop without his knowledge. When the teleworker tries to log in to the network with the same laptop, the MAG Series or SA Series appliance dynamically downloads the antimalware software to the teleworker's laptop and removes the malware program before the user and the laptop can be granted access to the network. Figure 2 provides a diagram on how the SA Series with the Enhanced Endpoint Security license can remove the malware program from the teleworker. In this example, all the endpoints of remote users are cleaned up from any malware before they attempt to access the network remotely.

Features and Benefits

Enhanced Endpoint Security Effectively Detects, Blocks and Removes Malware Threats

- Enhanced Endpoint Security Is based on Spy-Sweeper from Webroot, the market leader and trusted vendor in antimalware solutions
- Removes wide array of contemporary threats including all types of malware, trojans, worms, and adware
- Ensures only healthy devices are granted access
- Protects corporate resources from infected endpoints

Real-Time Threat Protection with Smart Shields

- Blocks sophisticated malware threats in real time, before they can infect a device
- Blocks malware from ever installing on-read, on-write, or on-execute functionality
- Prevents malware from modifying security settings
- Is always on to scan memory and virus signatures to detect malware variants

End-to-End Solution for both LAN and WAN Endpoints

- With either the MAG Series or UAC, the licensed Enhanced Endpoint Security module protect corporate networks from infected devices of LAN users—even those infected with malware in rootkits—such as employees, contractors, and guests.
- With either the MAG Series or SA Series, the Enhanced Endpoint Security license ensure that remote users such as teleworkers, partners, and suppliers have clean devices before being granted access to the network.
- Juniper's subscription-based Enhanced Endpoint Security licensed module prevents malware on all endpoints at all times, regardless of the endpoint's location or user.

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services**.

Ordering Information for Enhanced Endpoint Security (EES) Subscription

MODEL NUMBER	MODEL NAME AND DESCRIPTION
ACCESS-EES-50U-1YR	Enhanced Endpoint Security subscription, 50 concurrent users, 1-year
ACCESS-EES-100U-1YR	Enhanced Endpoint Security subscription, 100 concurrent users, 1-year
ACCESS-EES-250U-1YR	Enhanced Endpoint Security subscription, 250 concurrent users, 1-year
ACCESS-EES-500U-1YR	Enhanced Endpoint Security subscription, 500 concurrent users, 1-year
ACCESS-EES-1000U-1YR	Enhanced Endpoint Security subscription, 1,000 concurrent users, 1-year
ACCESS-EES-2500U-1YR	Enhanced Endpoint Security subscription, 2,500 concurrent users, 1-year
ACCESS-EES-5000U-1YR	Enhanced Endpoint Security subscription, 5,000 concurrent users, 1-year
ACCESS-EES-7500U-1YR	Enhanced Endpoint Security subscription, 7,500 concurrent users, 1-year
ACCESS-EES-10KU-1YR	Enhanced Endpoint Security subscription, 10,000 concurrent users, 1-year
ACCESS-EES-15KU-1YR	Enhanced Endpoint Security subscription, 15,000 concurrent users, 1-year
ACCESS-EES-20KU-1YR	Enhanced Endpoint Security subscription, 20,000 concurrent users, 1-year
ACCESS-EES-25KU-1YR	Enhanced Endpoint Security subscription, 25,000 concurrent users, 1-year
ACCESS-EES-50U-2YR	Enhanced Endpoint Security subscription, 50 concurrent users, 2-year
ACCESS-EES-100U-2YR	Enhanced Endpoint Security subscription, 100 concurrent Users, 2-year
ACCESS-EES-250U-2YR	Enhanced Endpoint Security subscription, 250 concurrent users, 2-year
ACCESS-EES-500U-2YR	Enhanced Endpoint Security subscription, 500 concurrent users, 2-year
ACCESS-EES-1000U-2YR	Enhanced Endpoint Security subscription, 1,000 concurrent users, 2-year
ACCESS-EES-2500U-2YR	Enhanced Endpoint Security subscription, 2,500 concurrent users, 2-year
ACCESS-EES-5000U-2YR	Enhanced Endpoint Security subscription, 5,000 concurrent users, 2-year
ACCESS-EES-7500U-2YR	Enhanced Endpoint Security subscription, 7,500 concurrent users, 2-year
ACCESS-EES-10KU-2YR	Enhanced Endpoint Security subscription, 10,000 concurrent users, 2-year
ACCESS-EES-15KU-2YR	Enhanced Endpoint Security subscription, 15,000 concurrent users, 2-year
ACCESS-EES-20KU-2YR	Enhanced Endpoint Security subscription, 20,000 concurrent users, 2-year
ACCESS-EES-25KU-2YR	Enhanced Endpoint Security subscription, 25,000 concurrent users, 2-year
ACCESS-EES-50U-3YR	Enhanced Endpoint Security subscription, 50 concurrent users, 3-year
ACCESS-EES-100U-3YR	Enhanced Endpoint Security subscription, 100 concurrent users, 3-year
ACCESS-EES-250U-3YR	Enhanced Endpoint Security subscription, 250 concurrent users, 3-year
ACCESS-EES-500U-3YR	Enhanced Endpoint Security subscription, 500 concurrent users, 3-year
ACCESS-EES-1000U-3YR	Enhanced Endpoint Security subscription, 1,000 concurrent users, 3-year
ACCESS-EES-2500U-3YR	Enhanced Endpoint Security subscription, 2,500 concurrent users, 3-year
ACCESS-EES-5000U-3YR	Enhanced Endpoint Security subscription, 5,000 concurrent users, 3-year
ACCESS-EES-7500U-3YR	Enhanced Endpoint Security subscription, 7,500 concurrent users, 3-year
ACCESS-EES-10KU-3YR	Enhanced Endpoint Security subscription, 10,000 concurrent users, 3-year
ACCESS-EES-15KU-3YR	Enhanced Endpoint Security subscription, 15,000 concurrent users, 3-year
ACCESS-EES-20KU-3YR	Enhanced Endpoint Security subscription, 20,000 concurrent users, 3-year
ACCESS-EES-25KU-3YR	Enhanced Endpoint Security subscription, 25,000 concurrent users, 3-year

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

1000293-005-EN July 2011

Printed on recycled paper