MRG Effitas
Efficacy Assessment & Assurance

AV comparatives

Anti-Virus Comparative

Comparison of "Next-Generation" Security Products 2016

Language: English
September 2016

Last Revision: 7th November 2016

www.av-comparatives.org
www.mrg-effitas.com

Table of Contents

Introduction	3
Approved NextGen Products	5
Malware Protection Test	6
Barracuda NextGen Firewall VF100	14
CrowdStrike Falcon Host	18
Palo Alto Traps	23
SentinelOne Endpoint Protection Platform	28

Introduction

"Next Generation" is a vague term used to describe security products that work on a different principle from traditional antivirus software. Currently these are available mainly for business networks rather than home users. They may work by monitoring incoming traffic on the network, as is the case for the Barracuda NextGen Firewall, or by installing client software which is managed and monitored centrally from a console, as is the case for the other products we have reviewed here. The latter type is intended to replace the antivirus software on client PCs, while the former could still be used in conjunction with traditional AV products.

This report marks the first time AV-Comparatives has tested and included next-generation security products in a public comparative test report. We had reached out to many leading vendors in this space, requesting their participation in the test. Unfortunately, a number of vendors refused to participate in this independent evaluation. Since their products could not be included in this public report, we are unable to approve them as valuable next-generation security products. We look forward to their future participation in independent tests.

For this assessment, MRG Effitas and AV-Comparatives combined their strengths to conduct a joint test. The reviews and Malware Protection Tests were performed by AV-Comparatives, while the Exploit Test was performed by MRG Effitas.

Notes

Some of the products in this review may only provide logging and analysis of threats (useful for incident response), rather than actually protecting against them. In some cases, protection features are deactivated by default and have to be enabled and configured by the administrator before they can be used. Not all of the products covered here may be available as a trial version. In fact, a few "next-gen" vendors try to avoid having their products publicly tested or independently scrutinized. To this end, they do not sell their products to testing labs, and may even revoke a license key – without a refund - if they find out or suspect that it was bought anonymously by a testing lab.

Products reviewed

The following products have been reviewed/tested under Windows 10 64-bit and are included in this public report:

- Barracuda NextGen Firewall VF100 7.0.1
- CrowdStrike Falcon Host 2.0.19.3908
- Palo Alto Traps 3.4.0.15678
- Sentinel One Endpoint Protection Platform 1.6.2.5021

Review format

We have covered the following points in this review:

Supported operating systems

Here we list Windows client and Windows Server operating systems supported by the manufacturer (and virtualisation systems where applicable).

Documentation

We have looked at the external documentation, i.e. manuals and online knowledge base (as opposed to the console's built-in help features). These could be used to help install the console where applicable, whereas a help feature built into the console obviously could not.

Management Console

Installation and configuration

How to set up the console so that the administrator can proceed with deploying endpoint protection software to clients.

Layout

Console design, with emphasis on finding major features.

Preparing devices for deployment

Is it necessary to configure the management server and/or the clients, e.g. by opening firewall ports or enabling file sharing, to enable deployment and management?

Deploying the endpoint protection software

Deployment methods available, e.g. remote push, emailing a link to users, local installation on the client itself. For the purposes of the test, we used the simplest method available to deploy the endpoint protection software to the clients.

Monitoring the network

Status and alerts

How does the console show overall security status of the network, and warn of anything that the administrator should take action on, such as malware detections or outdated signatures?

Responding to alerts

How can the administrator find more details of any warnings shown?

Program version

Which version of the client software is currently installed on each device?

Managing the network

Scanning

How to run on-demand malware scans on protected devices.

Scheduling Scans

How to set up a regular scheduled scan.

Updates

How to run a manual update of malware definitions on managed clients.

Removing devices from the console

If a device is lost, stolen or becomes unusable, how can its entry be deleted?

Integrated help feature

Details of the console's built-in help feature (if any) and how to access this.

Approved Products

The following products showed decent results in the malware protection tests without issuing too many false alarms, and receive our *Approved Business Security* Award:

Malware Protection Test

All tests were performed with an active Internet connection (i.e. with cloud connection). We tested the products reviewed here as follows:

RTTL: 500 most prevalent malicious samples according to the AMTSO Real-Time Threat List (RTTL) were **executed** on the system.

AVC: 500 most recent and prevalent malicious samples from our own database were **executed** on the system. Some of the tested products function also as an incident response, where the system is compromised but a detection alert is reported in the web interface. The additional detection rate for the AVC score is noted in brackets.

WPDT: 50 malicious websites were tested by using our **Real-World Testing** Framework, which simulates the activities of a typical computer user (whether at home or in the office) surfing the Internet. The test was run in parallel with "traditional" business antivirus products, enabling a comparison of the threat-protection capabilities of traditional and next-gen products.

FPs: a false alarm test in which 1000 clean files have been **executed** on the system has also been performed. The false positive test measures the ability of products to distinguish clean from malicious files.

Exploit Test: 21 exploits have been used in the Exploit test.

The tests were performed during September and October 2016.

Settings Used

Some vendors made configuration changes to their products remotely before the tests. Protection relevant changes were as follows:

Barracuda: *Detect All Types* set to *Yes*, *URL Filter Enabled* set to *True*.

CrowdStrike: *File Attribute Analysis* and *File Analysis* set to *Aggressive*, and all available protection options enabled.

Palo Alto: *WildFire activation* set to *On*, *Action* is *prevention*, *Action is applied on grayware*, *Local analysis* is *enabled*, *Upload files for WildFire* is *enabled*.

Sentinel One: *Show Suspicious Activities* enabled, *Auto Immune* enabled, *Actions* set to *Quarantine*.

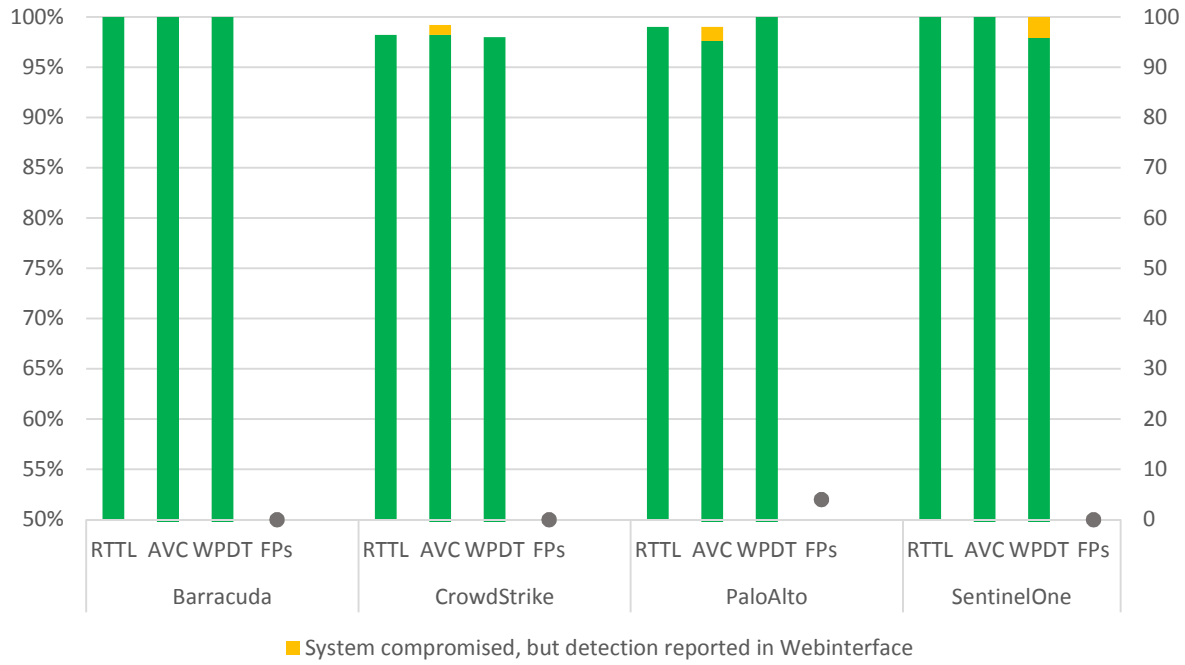
Results

Malware Protection and False Alarm Test

Below are the results achieved by the next-gen products in the malware protection tests performed by AV-Comparatives. In general, the protection rates are quite high, and comparable with the scores reached by conventional business products.

The scores in brackets shows the total detection rate if notifications in the web interface are counted as detections (i.e. cases where the system was compromised, but an alert was shown in the web interface).

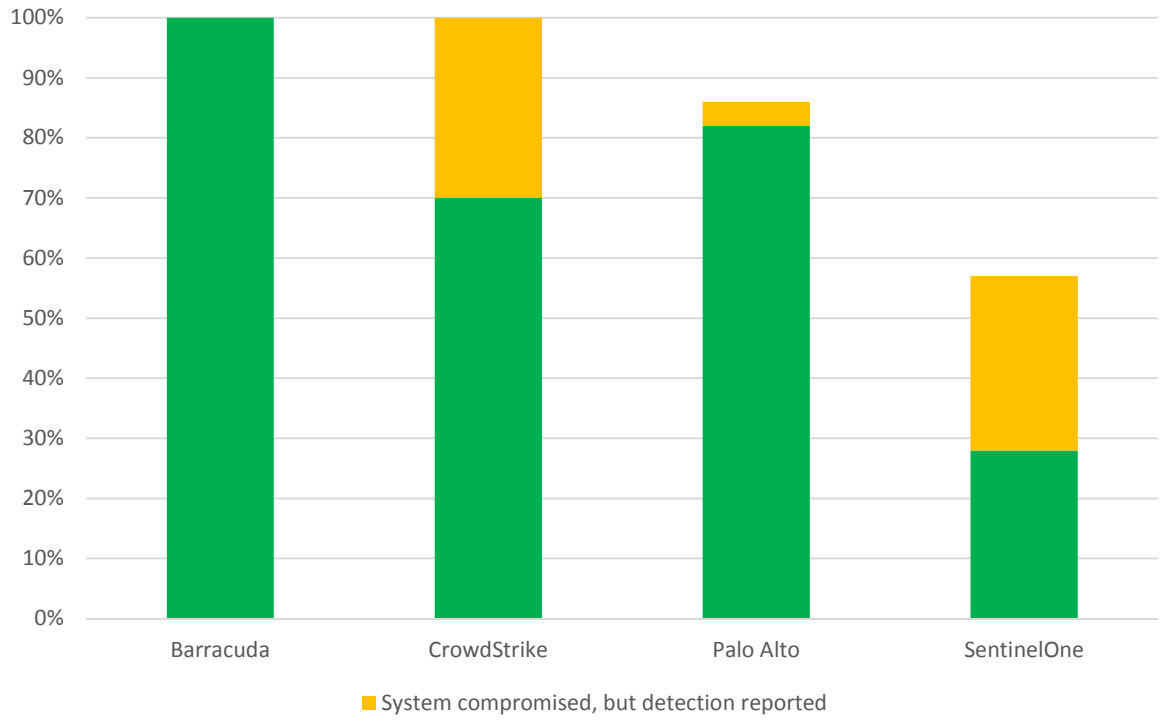
	RTTL	AVC	WPDT	FPs
Barracuda	100.0%	100.0%	100%	0
CrowdStrike	98.2%	98.2% (99.2%)	98%	0
Palo Alto	99.0%	97.6% (99.0%)	100%	4
SentinelOne	100.0%	100.0%	98% (100%)	0



Exploit Test

Below are the results achieved by the next-gen products in the exploit tests performed by MRG Effitas.

	Protection Rate (Detection Rate)
Barracuda	100% (100%)
CrowdStrike	70% (100%)
Palo Alto	82% (86%)
SentinelOne	28% (57%)



Scoring / Calculation of Results

Scoring Of The Exploit Protection/Detection Results

We defined the following stages, at which the exploit can be prevented by the endpoint protection system:

1. Blocking the URL (infected URL, exploit kit URL, redirection URL, malware URL) by the URL database (local or cloud). For example, a typical result is the browser displaying a "site has been blocked" message by the endpoint protection. The sooner the threat is detected in the exploit chain, the easier it is to remove the malicious files from the system, the less information can be gathered from the system by the attackers, and the lower the risk of an attack targeting the particular security solution on an endpoint.

2. Analyzing and blocking the page containing a malicious HTML code, JavaScripts (redirects, iframes, obfuscated JavaScripts, etc.), or Flash files.

3. Blocking the exploit before the shellcode is executed.

4. Blocking the downloaded payload by analyzing the malware before it is started. For example, the malware payload download (either the clear-text binary or the encrypted/encoded binary) can be seen in the proxy traffic, but no malware process starts.

5. The malware execution is blocked (no process create, load library).

6. There is a successful start by the dropped malware.

7. There is a successful start by the dropped malware, but after some time, all dropped malware is terminated and deleted ("malware starts, but blocked later").

The "protection" scoring of the results was calculated as the followings:

- If no malicious untrusted code was able to run on the endpoint, 5 points were given to the products. This can be achieved via blocking the exploit in step 1, 2 or 3.
- If malicious untrusted code ran on the system (exploit shellcode, downloader code), but the final malware was not able start, 4 points were given to the product. This can be achieved via blocking the exploit in step 4 or 5.
- If both the exploit shellcode (or downloader code) and the final malware were able to run, 0 points were given to the product.
- If at any stage of the infection, a medium or high severity alert was generated (even if the infection was not prevented), 1 point was given to the product.

The "detection" scoring of the results was calculated as follows:

- If at any stage of the infection, a medium or high severity alert was generated (even if the infection was not prevented), 1 point was given to the product.

We used this scoring for the following reasons:

- The scope of the test was exploit prevention and not the detection of malware running on the system.
- It is not possible to determine what kind of commands have been executed or what information exfiltrated by the malware. Data exfiltration cannot be undone or remediated.
- It cannot be determined if the malware exited because the endpoint protection system blocked it, or if malware quit because it detected monitor processes, virtualization, or quit because it did not find its target environment.
- Checking for malware remediation can be too time-consuming and remediation scoring very difficult in an enterprise environment. For example, in recent years we have seen several alerts stating that the endpoint protection system blocked a URL/page/exploit/malware, but still the malware was able to execute and run on the system. On other occasions, the malware code was deleted from the disk by the endpoint protection system, but the malware process was still running, or some parts of the malware were detected and killed, while others were not.
- In a complex enterprise environment multiple network and endpoint products protect the endpoints. If one network product alerts that malicious binary has been downloaded to the endpoint, administrators have to cross-check the alerts with the endpoint protection alerts, or do a full forensics investigation to be sure that no malware was running on the endpoint. This process can be time and resource consuming, which is why it is better to block the exploit before the shellcode starts.
- Usually the exploit shellcode is only a simple stage to download and execute a new piece of malware, but in targeted attacks, the exploit shellcode can be more complex.

We believe that such zero-tolerance scoring helps enterprises to choose the best products, using simple metrics. Manually verifying the successful remediation of the malware in an enterprise environment is a very resource-intensive process and costs a lot of money. In our view, malware needs to be blocked before it has a chance to run, and no exploit shellcode should be able to run.

Test Procedure / Methodology

Exploit Test Setup

Testing Cycle for Each Test Case

1) One default-installation Windows 10 64-bit virtual machine (VirtualBox) endpoint was created. The default HTTP/HTTPS proxy was configured to point to a proxy running on a different machine. SSL/TLS traffic was not intercepted on the proxy.

2) The security of the OS was weakened by the following actions:
   a) Windows Defender was disabled
   b) Internet Explorer SmartScreen was disabled
   c) Vulnerable software was installed, see "Software Installed" for details.
   d) Windows Update was disabled

3) From this point, different snapshots were created from the virtual machine, several with different endpoint protection products and one with none. This procedure ensured that the base system was exactly the same in all test systems.

   The following endpoint security suites, with the following configuration, were defined for this test:

   a) No additional protection
      this snapshot was used to infect the OS and to verify the exploit replay
   b) Product 1 installed
   c) Product 2 installed
   d) …

The endpoint systems were installed with the default configuration, potentially unwanted software removal was enabled, and where the option was provided during the installation, cloud/community participation was enabled.

4) The exploit sources can be divided into two categories: In-the-wild threats and Metasploit. VBscript based downloaders and Office macro documents were also in scope, as these threats are usually not included in other test scenarios.

5) The virtual machine was reverted to a clean state and traffic was replayed by the proxy server. The replay meant that the browser was used as before, but instead of the original webservers, the proxy server answered the requests based on the recorded traffic. When the "replayed exploit" was able to infect the OS, the exploit traffic was marked as a source for the tests. This method guarantees that exactly the same traffic will be seen by the endpoint protection systems, even if the original exploit kit goes down during the tests. This exploit replay is NOT to be confused with tcpreplay type replay.

6) After new exploit traffic was approved, the endpoint protection systems were tested. Before the exploit site was tested, it was verified that the endpoint protection had been updated to the latest version with the latest signatures and that every cloud connection was working. If there was a need to restart the system, it was restarted. In the proxy setup, unmatched requests were allowed to pass through and SSL/TLS was not decrypted to ensure AV connectivity. VPN was used during the test on the host machine. When user interaction was needed from the endpoint protection (e.g. site visit not recommended, etc.), the block/deny action was chosen. When user interaction was needed from Windows, we chose the run/allow options. No other processes were running on the system, except the Process Monitor/Process Explorer from SysInternals and Wireshark (both installed to non-default directories).

7) After navigating to the exploit site, the system was monitored to check for new processes, loaded DLLs or C&C traffic.

8) The process went back to step 5. until all exploit site test cases were reached.

The following hardware was dedicated to the virtual machine:

- 4 GB RAM memory
- 2 processors dedicated from AMD FX 8370E CPU
- 65 GB free space
- 1 network interface
- SSD drive

The VirtualBox host and guest system for the exploit test has been hardened in a way that common virtualization and sandbox detection techniques cannot detect the system as an analysis system.

Analysis Of The Exploit Kits Used In The Exploit Test

Unfortunately, the time of the test and OS configuration was not in favor for the exploit test. At the time of the tests, two exploit kits dominated the Internet. Sundown and RIG. Unfortunately, RIG used old (mostly Flash) exploits, which was unable to exploit the test configuration at all. That is why it was important to test with Metasploit and with some not super-fresh, but not too-old exploit kits as well (Neutrino). We also used two samples, which are not an exploit itself, but rather non-PE downloader, like an Office macro and a WSF downloader. We added these into the mix because these exotic file types are often excluded from Real World tests, but meanwhile, prevalent in-the-wild.

A total of 21 test cases have been tested.

- 8 Sundown EK
- 5 Neutrino EK
- 4 Metasploit
- 1 Powershell Empire
- 1 Metasploit Macro
- 1 Locky malspam WSF
- 1 unknown EK

These exploit kits were targeting Adobe Flash, Internet Explorer, Microsoft Office (macro), Silverlight, Firefox, Java.

Software Installed

For the exploit test part, the following vulnerable software was installed:

Vendor	Product	Version		Vendor	Product	Version
Adobe	Flash Player ActiveX - builtin	21.0.0.182		Microsoft	SilverLight	5.1.10411.0
AutoIT	AutoIT	3.3.12.0		Mozilla	Firefox	31.0
Microsoft	Internet Explorer	11.162.10586		Oracle	Java	1.7.0.17
Microsoft	Office	2016				

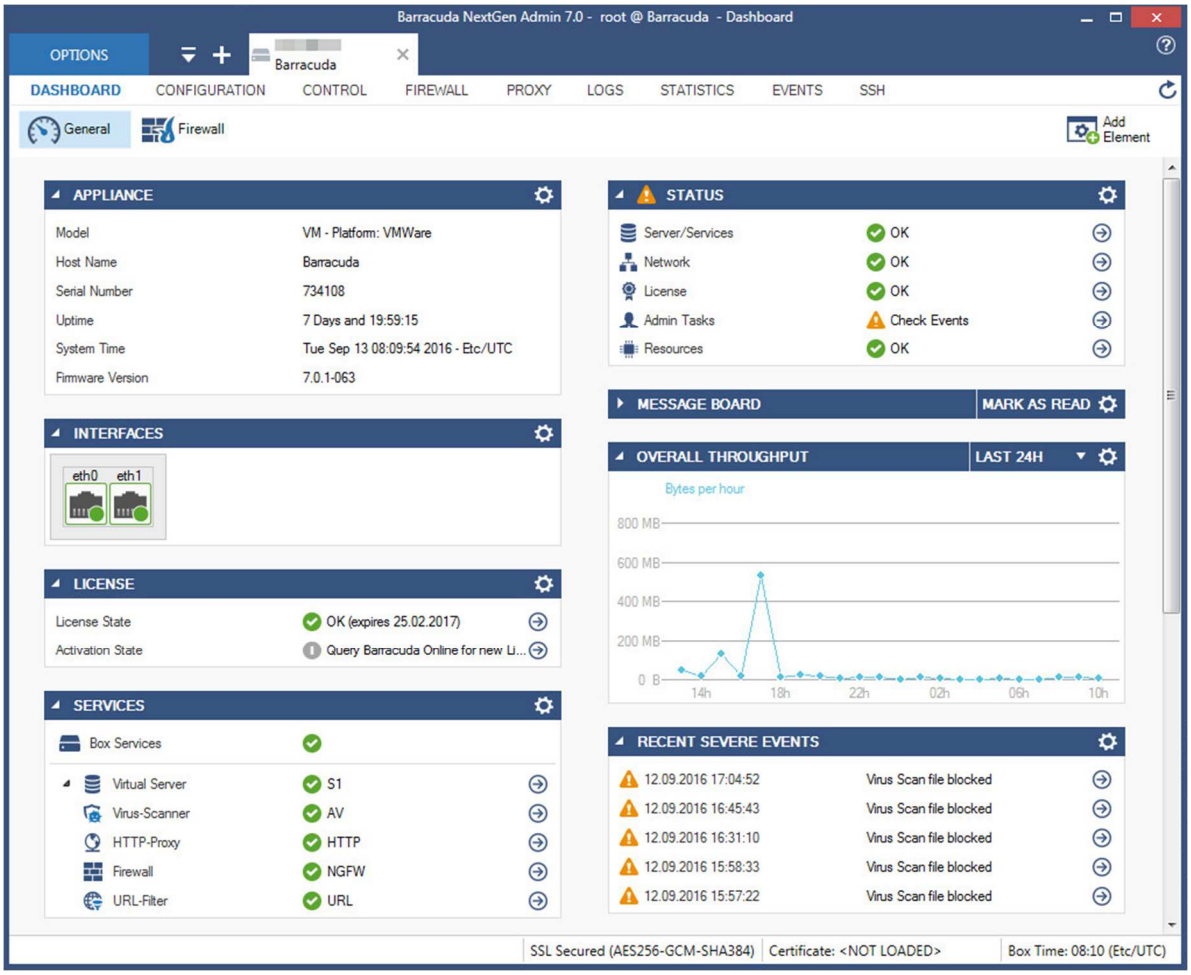
Scoring of the Malware Protection Results

The scoring of the malware protection is straightforward, whenever the system got compromised by the malware, 0 point were given to the product, and whenever the malware was blocked or remediated, 1 point was given.

False positive test

The same scoring principle as described above has been applied for the false alarms test. In this test, 1000 non-malicious applications have been used to measure the ability of the products to distinguish clean from malicious files.

Barracuda NextGen Firewall VF100



Overview

Product version reviewed

Barracuda NextGen Firewall VF100 Firmware Version 7.0.1 on VM Ware.

Operating systems supported

Supported Hypervisors for the virtual appliance version: VMware, XenServer (Full Virtualization & Paravirtualization), Hyper-V, KVM

Requirements for the administration software: Windows Vista, Windows 7, Windows 8/8.1 or Windows 10

About the product

Barracuda NextGen Firewalls are available as a hardware appliance, virtual appliance or Cloud options (Amazon AWS, Microsoft Azure, Google Cloud Engine, VMWare vCloud Air); we tested the VMware virtual appliance. As its name suggests, it includes a next generation firewall with application and user awareness, but also antimalware features such as signature based anti-virus engine and Barracuda's Advanced Threat Detection (ATD) feature. ATD is a cloud-based sandboxing service specialized in real-time malware-analysis by running suspicious files in various operating systems. All interaction with the cloud based ATD service is fully integrated into the Windows-based administration console. ATD is available for all Barracuda NextGen-Series Firewall products, which aims to detect known and unknown threats and preventing these threats from entering the network. As the product is network-based rather than client-based, a traditional antivirus product should be deployed on clients as additional protection layer; this would also be necessary for devices that are used outside of the company LAN. In addition to Barracuda's own features, the Avira antivirus engine is used by the appliance for additional malware detection.

Product page on vendor's website

https://ngf.barracuda.com

Documentation

Manuals

Documentation for Barracuda NextGen Firewalls as for all Barracuda product are available online[1].

Knowledge base

Available as part of the online documentation.

Good points

The administration program is more feature-rich than the typical web interfaces for next-gen AV solutions, because it is also used to configure the firewall. Nonetheless, the interface is well-structured and status information and features can be accessed in an intuitive way.

Suggestions for improvement

Clicking on the help icon in the administration console opens the landing page for the product in online documentation portal. We feel that it could be helpful to administrators to open the help page dedicated to the currently active page in the console software instead.

[1] https://campus.barracuda.com/product/nextgenfirewallf/article/NGF/

Management Console

Installation and configuration

The administration software is a standalone executable and does not need to be installed. After starting the software, administrators only need to enter the IP address of the firewall and their login credentials to access the management console.

Layout

The console opens on the *General* tab of the *Dashboard* page, providing mostly status information, as well as a list of recently detected threats. Administrators may also choose to hide some sections from the *Dashboard* page, allowing them to concentrate on the most important items for them. The menu at the top of the console window allows navigation to the other main pages: *Configuration*, *Control*, *Firewall*, *Proxy*, *Logs*, *Statistics*, *Events*, and *SSH*. The content of each page is further divided into multiple tabs.

Preparing devices for deployment

No preparations are necessary.

Deploying the endpoint protection software

Since the product is a firewall, no software needs to be deployed.

Monitoring the network

Status and alerts

Apart from the short list of recent threats on the *General* tab, the main page also provides s *Firewall Dashboard* that list threats most commonly encountered by the system. More details about detected threats can be retrieved from the *Firewall* main page of the console. The *ATD* (Advanced Threat Detection) tab provides a list of detected threats. Administrators can download a report for each threat, including detailed static and dynamic analysis.

Responding to alerts

Since threats are blocked automatically by the firewall, administrators are not required to manually respond to alerts. If desired, alerts can be created if a predefined threshold of found viruses or IPS hits per timeframe is exceeded (e.g. more than 2000 IPS hits per hour). These alerts can be sent out via email, syslog or even via Apple Push Notification service to configured IPhones or IPads

Program version

The major program version of the administration software is displayed in the title bar of the console window. More detailed information about the software version running can be obtained from the *Options* menu.

Managing the network

Scanning

The firewall automatically scans incoming and outgoing Web, FTP and Mail traffic for threats. Built-in deep SSL-Inspection extends this to encrypted communications (HTTPS/SMTPS) via a sanctioned man–in-the-middle approach. Additionally, administrators can manually upload malicious files for analysis in the sandbox.

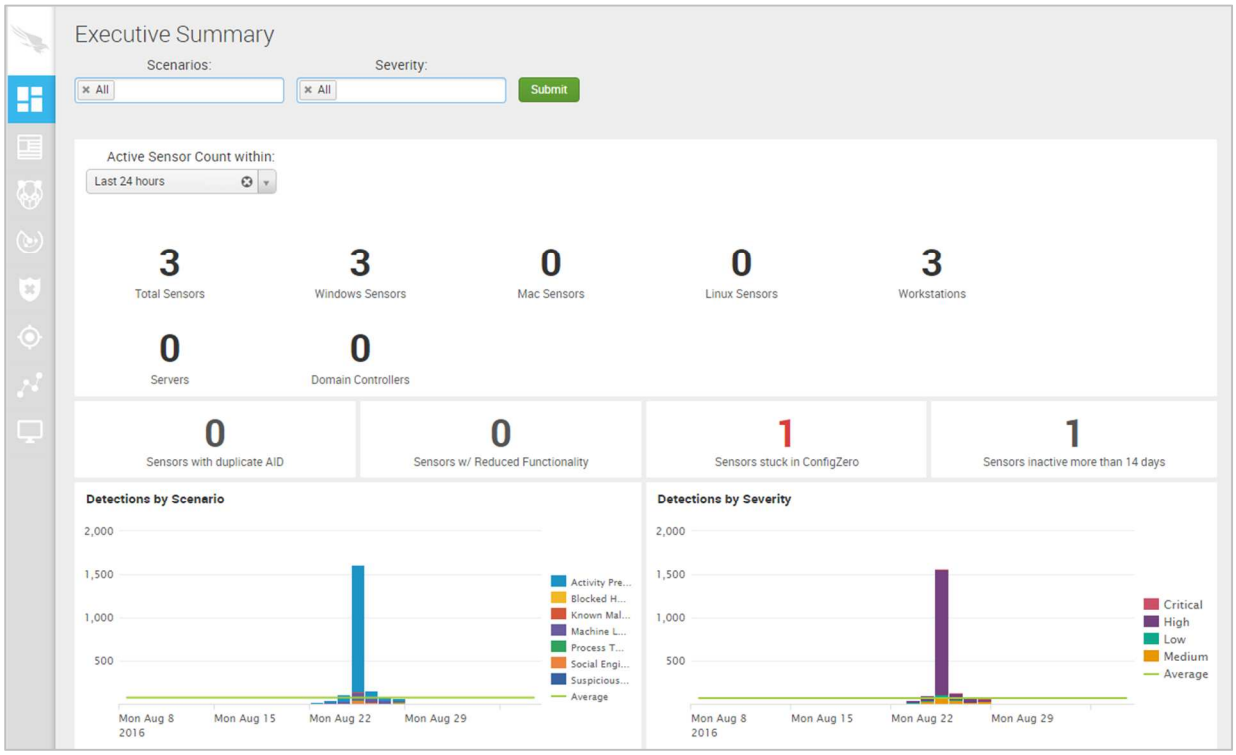
Updates

New versions of the firewall firmware can be installed directly from the Updates Element on the *General Dashboard* page. New versions of the administration software can also directly be downloaded from the Updates Element on the *General Dashboard* page.

Client protection software

In keeping with the nature of the product, there is no client software to be installed.

CrowdStrike Falcon Host



Overview

Product version reviewed

CrowdStrike Falcon Host 2.0

Operating systems supported

Windows 7, 8/8.1, 10, all 32 and 64-bit)
Windows Server 2008 R2, 2012/R2, Core 2012
Apple Macintosh OS X 10.10, 10.11
RHEL 6.2-6.8, 7.0-7.2
CentOS 6.2-6.8, 7.0-7.2
Ubuntu 14.04 LTS (minimum kernel version 3.13.0-32)
SUSE Linux Enterprise Server 11.3-11.4 (minimum kernel version 3.0.101-0.47.55.1)
SUSE Linux Enterprise Server 12-12.1 (minimum kernel version 3.12.39-47)
(only 64-bit GNU/Linux systems are supported)

About the product

CrowdStrike Falcon Host is a cloud-based Next-Generation security platform, utilizing machine learning techniques with the aim of detecting known and unknown attacks on endpoints in the network. Endpoints are monitored for suspicious events continuously, providing detailed static and dynamic analysis of potential attacks to administrators.

Product page on vendor's website

https://www.crowdstrike.com/products/falcon-host/

Good points

The management console provides a modern look-and-feel and is well organized. Detailed analysis reports allow administrators to keep track of malicious activity in the network.

Documentation

Manuals

A range of documents in .PDF format can be downloaded via the console, by clicking on the falcon graphic.

Knowledge base

There is a knowledge base on the vendor's website[2]

[2] https://www.crowdstrike.com/blog/tech-center/

Management Console

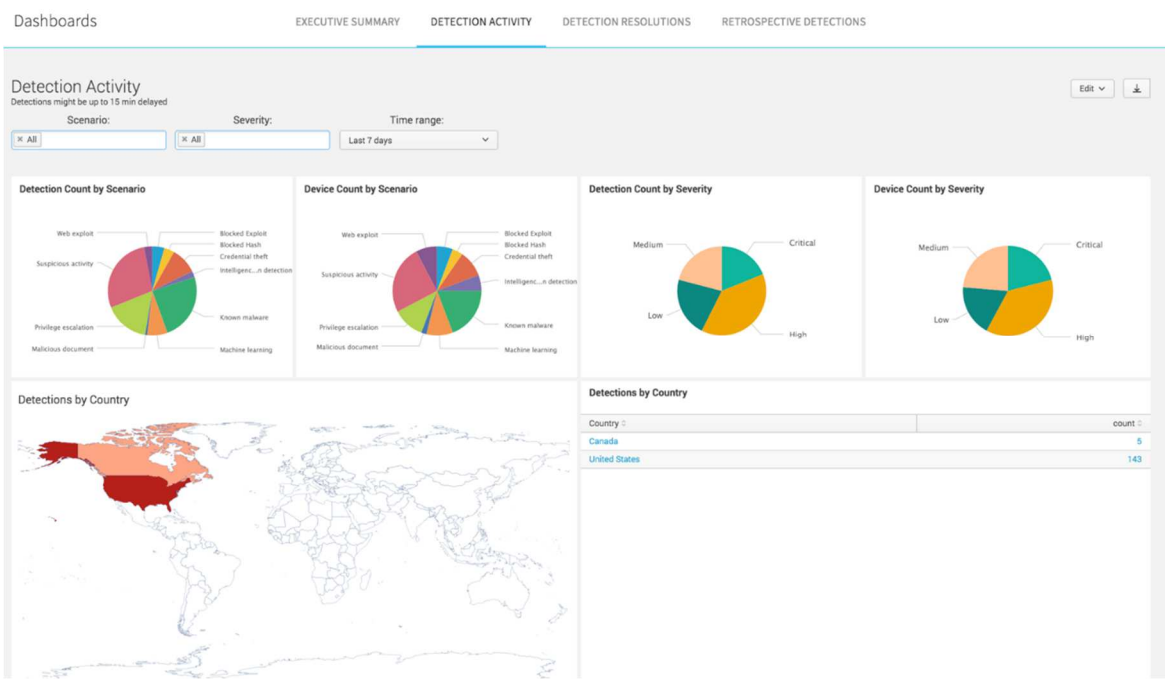
Installation and configuration

The console is cloud-based, so no installation is required.

In the standard configuration, many of the protection features are disabled, and so have to be enabled/configured before the product can be used effectively.

Layout

The console opens on the *Detections* page. This page provides an overview of detected and unresolved threats and allows administrators to quickly assess the security status of the monitored network. The menu on the left-hand side of the console allows navigation to the console's other main pages: *Platform*, *Dashboards*, *News*, *Actors*, *Respond*, *Investigate*, *Events*, and *Devices*.



Preparing devices for deployment

We did not need to make any changes to client or server machines before deploying the protection software.

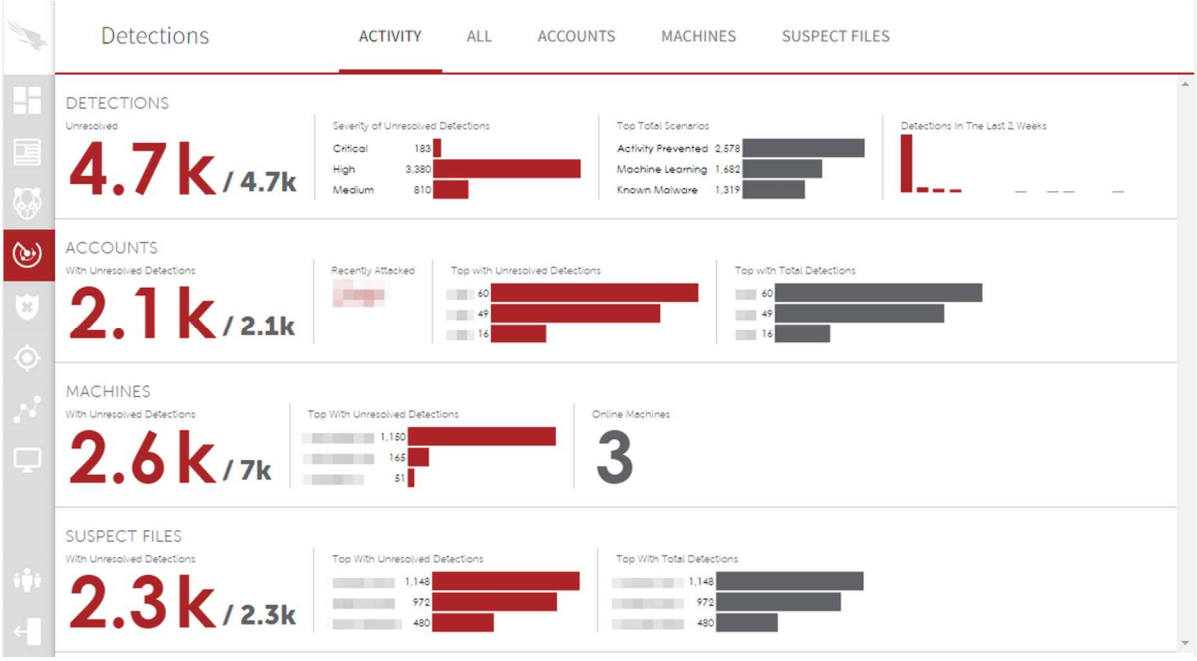
Deploying the endpoint protection software

We deployed the endpoint software by logging on to the cloud console from the machine to be protected, and downloading the installer directly.

Monitoring the network

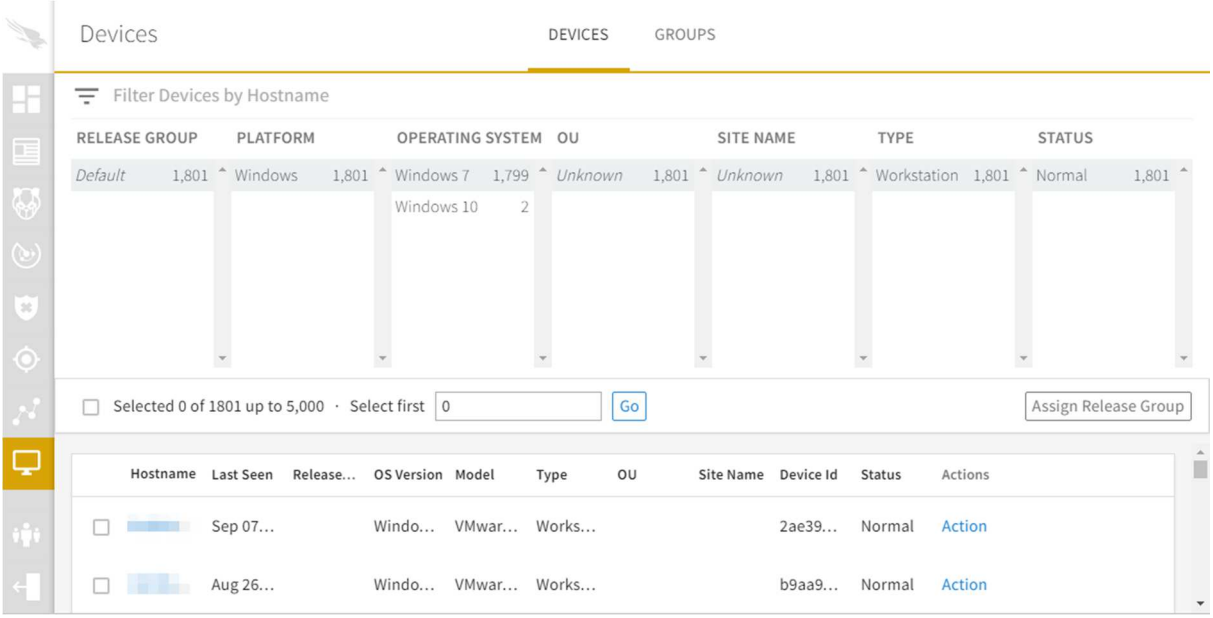
Status and alerts

The *Dashboards* page provides an overview of the number of connected clients as well as various statistics, such as a summary of the top ten hosts, users, and files with the most detections. Detailed information about detected threats can be found on the *Detections* page of the console:



Detections are grouped by accounts attacked, machines and files. For each category, threat details can be obtained by selecting the relevant section from the menu at the top of the page. From the *All* section, administrators can obtain detailed forensic analysis reports about discovered threats.

Information about connected clients can be obtained from the *Devices* page:



Responding to alerts

Administrators can mark detected threats as resolved by selecting the relevant detection on the *Detections* page of the console.

Program version

The management console does not display its product version in the user interface. The product version of installed endpoint clients can be seen by selecting the relevant device on the *Devices* page.

Managing the network

Scanning

The product does not feature on-demand scanning. Threats are detected automatically as they occur.

Updates

Product and content updates are set to happen automatically by default, but CrowdStrike also offers the ability for the administrator to control when systems receive updates.

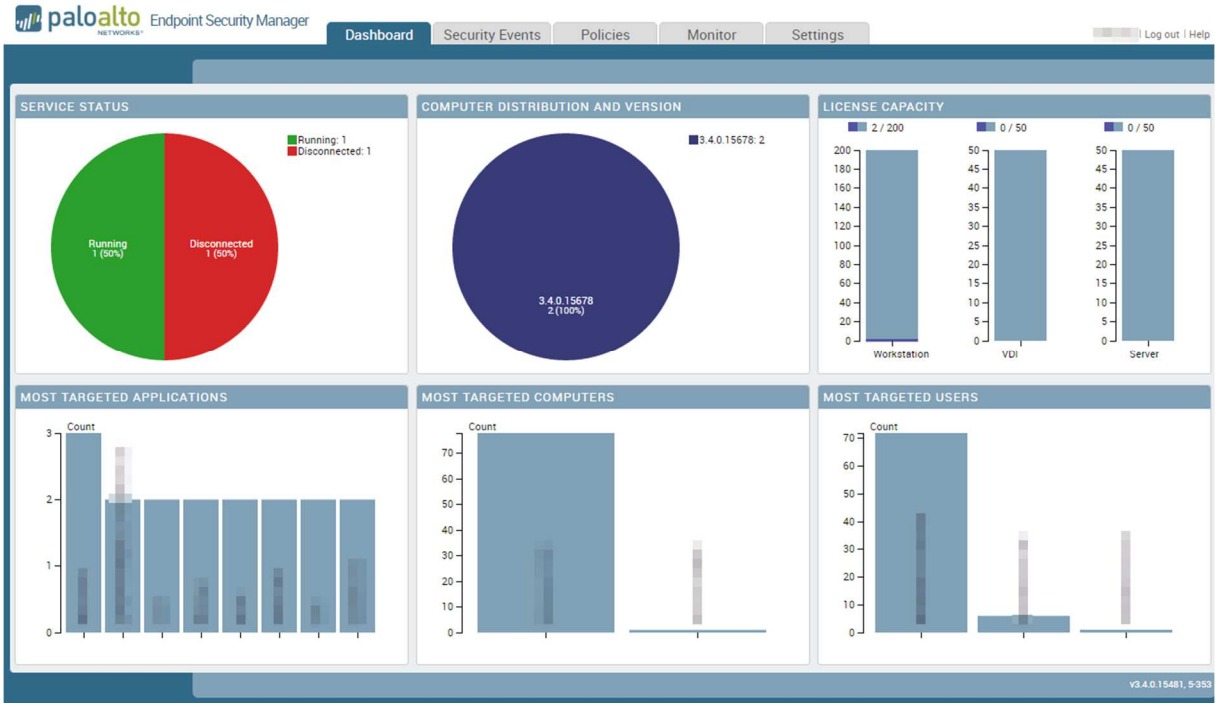
Removing devices from the console

The web interface cannot be used to remove devices from the console.

Windows client protection software

The client protection software does not have any visible user interface, but registers in Windows Security Center as antivirus and antispyware.

Palo Alto Traps



Overview

Product version reviewed

Palo Alto Networks Endpoint Security Manager v3.4.0.15481
Palo Alto Networks Traps agent 3.4.0.15678

Operating systems supported

Windows XP (32-bit); Windows Vista, 7, 8/8.1, 10 (32 and 64-bit); Windows Server 2003/R2 (32-bit); 2008/R2 (32 and 64-bit); 2012/R2 (64-bit)

About the product

Palo Alto Security Manager is a next-generation security platform for securing Windows endpoints. The system employs proprietary malware- and exploit-prevention methods with the aim of protecting clients from known and unknown attacks. Administrators can track the security status of their network using a single management console.

Product page on vendor's website

https://www.paloaltonetworks.com/products/secure-the-endpoint/traps

Good points

The functionality of the Endpoint Security Manager console can be accessed intuitively from 5 tabs. For each detected threat, the product provides static and dynamic analysis, which allows administrators to gain detailed knowledge about malicious-software activities in their network.

Suggestions for improvement

We feel that the update process could be a target for improvement. Depending on the frequency of product updates, automatic updates could be beneficial to administrators.
Additionally, we would suggest incorporating relevant parts of threat analysis results into the web interface, providing a better threat overview without having to handle separate pdf files.
Lastly, we would suggest adding client support for operating systems other than Microsoft Windows.

Documentation

Manual

Documentation for Palo Alto's products are available online[3].

Knowledge base

A knowledge base is provided. The link in the console contains an individualised URL relating to the licence used.

[3] https://www.paloaltonetworks.com/documentation/34/endpoint

Management Console

Installation and configuration

The console we used was cloud-based, so no installation or configuration is required. The Endpoint Security Manager is typically deployed on-premise.

Layout

The Endpoint Security Manager console opens on the *Dashboard* page. The page provides version and licensing information, as well as the connection status of managed clients. It also provides statistics about which users, computers and applications are most targeted by threats. The other main pages of the management console can be accessed from a tab-like menu at the top of the console (*Security Events*, *Policies*, *Monitor*, and *Settings*).

Preparing devices for deployment

We did not need to make any changes to client or server machines before deploying the protection software.

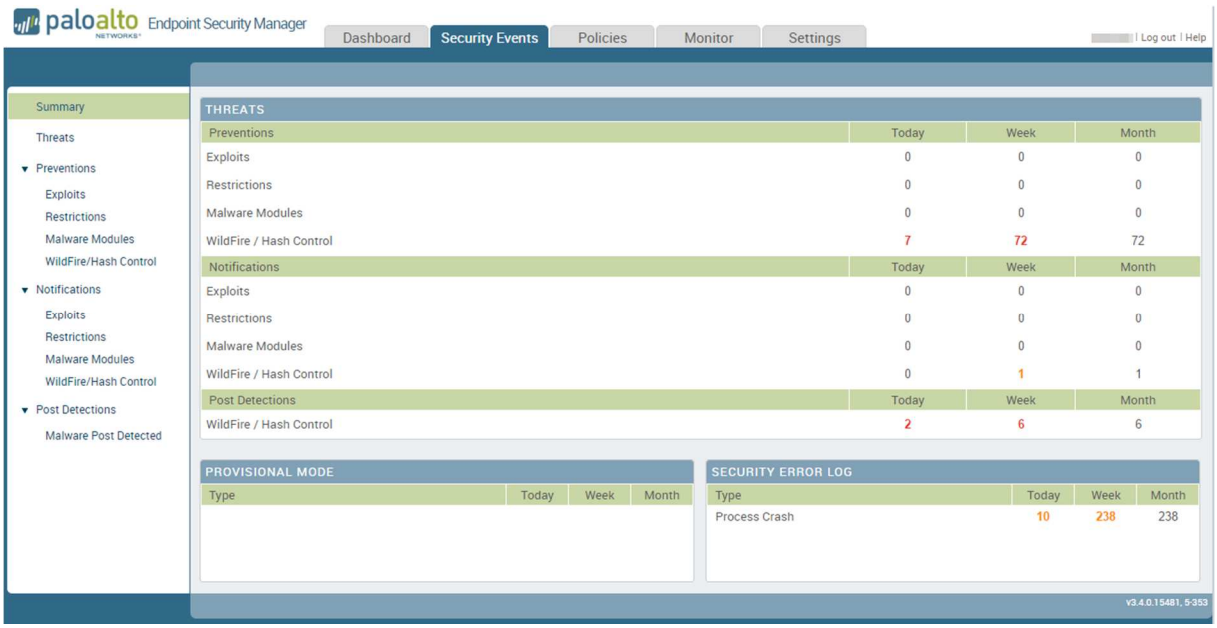
Deploying the endpoint protection software

We deployed the endpoint software by logging on to the cloud console from the machine to be protected, and downloading the installer directly.

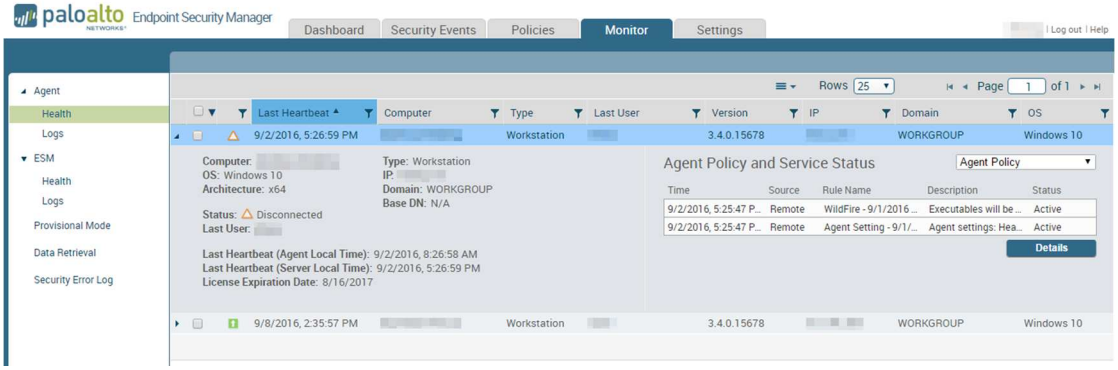
Monitoring the network

Status and alerts

The *Summary* section of the *Security Events* page displays an overview of threats encountered on the network. Threats are organized into groups according to their detection status (*Prevention*, *Notification*, and *Post Detection*) and further divided according to the type of threat encountered. Threat details can be obtained by first selecting the relevant threat category and then selecting the relevant threat from the list displayed.



Information about connected devices can be accessed from the *Agent Health* section of the *Monitor* page.



Responding to alerts

Administrators can obtain more information about detected threats on the *Security Events* page of the management console. For each threat, admins can download a detailed report in pdf Format. Typically, administrators do not need to perform remedial actions manually, as these actions are handled automatically according to the defined policies.

Program version

The program version of the management console is displayed in the bottom-right corner of the console. Agent versions of client devices are displayed on the *Dashboard* page. For a specific endpoint, the agent version can be obtained by selecting the endpoint on the *Monitor* page of the console.

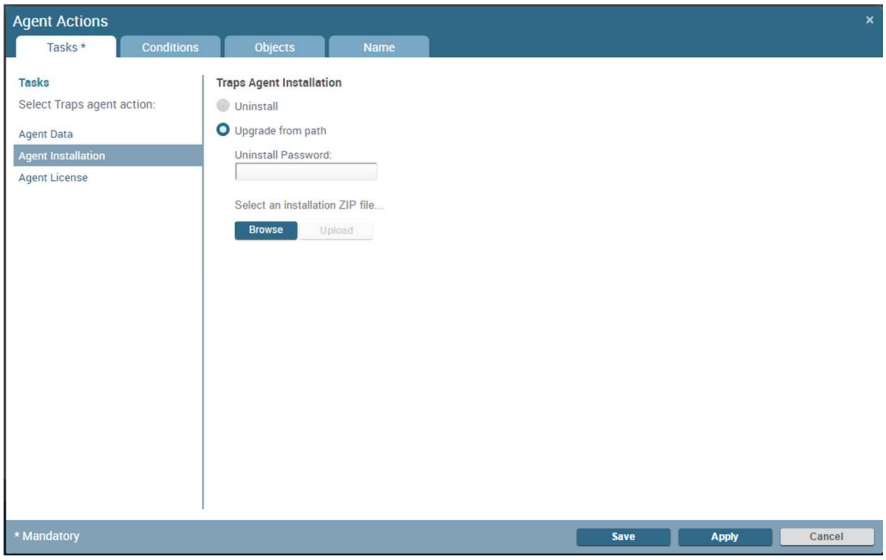
Managing the network

Scanning

The product does not feature on-demand scanning. Threats are detected automatically as they occur.

Updates

Agent updates can be performed by creating an agent action on the Settings page of the console. An administrator has to specify a local installation archive to upload and install.



Removing devices from the console

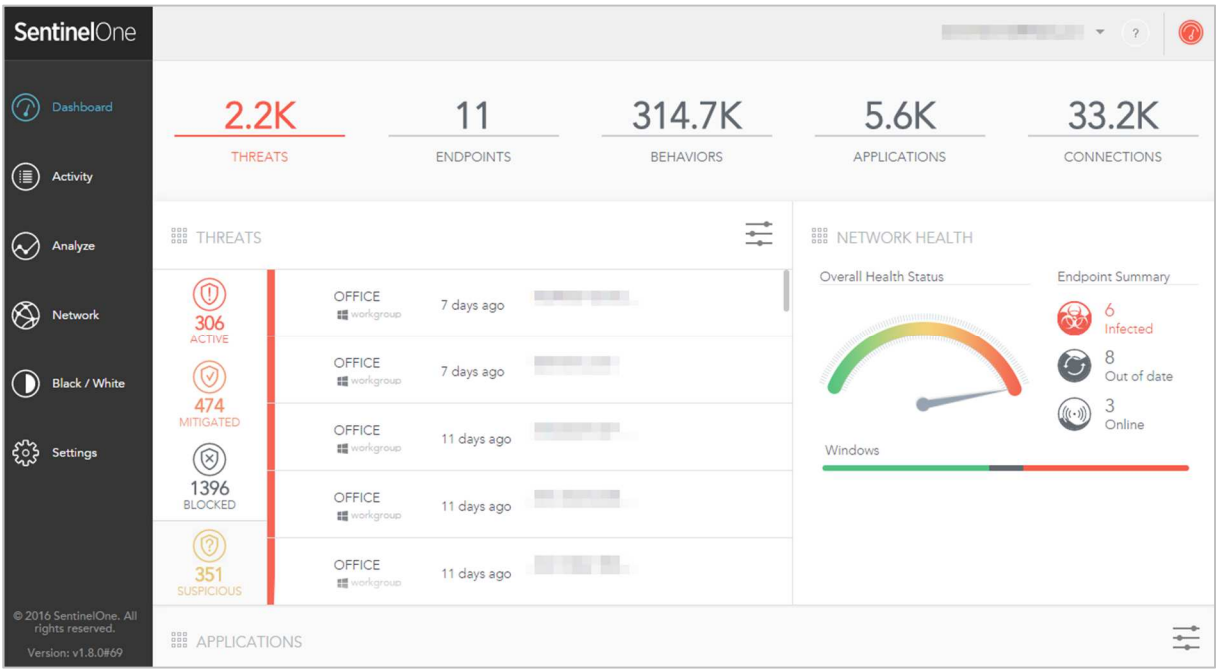
Clients can be removed from the console by first selecting the relevant devices on the *Monitor* page of the console and then choosing the delete option from the menu at the top-right of the list.

Client software

The client software has a GUI with a status display:

It does not register in Windows Security Center as antivirus or antispyware.

SentinelOne Endpoint Protection Platform



Overview

Product version reviewed

SentinelOne Endpoint Protection Platform (Management Server v1.8.0#69, Agent 1.6.2.5021)

Operating systems supported

Windows 7, 8, 8.1, 10
Windows Server 2008 R2, 2012 R2
OS X 10.9.x, 10.10.x, 10.11
Red Hat Linux, CentOS 6.5 and above

About the product

SentinelOne Endpoint Protection Platform provides a multi-layered approach for detecting malware, exploit and script-based attacks using a combination of machine learning coupled with both static analysis and system-wide behaviour monitoring to isolate and mitigate threats in real time. The management system, which can be deployed either in the cloud or on-premise, provides forensic analysis of threats and allows administrators to quickly resolve attacks through automated remediation and rollback features.

Product page on vendor's website

https://sentinelone.com/products/

Documentation

Manual

There is no manual on the vendor's website, but after login in the web console, a detailed Admin and API Guide can be found within SentinelOne's Knowledge Base under "Documentation" (see notes below).

Knowledge base

A knowledge base is provided,[4] which requires the user to log in to access any of the articles/features. In our test, the login credentials used for the management console did not work for the knowledge base.

Good points

The cloud management console is well organized and can be used intuitively. The analysis capabilities of the platform allow administrators to clearly identify each event that occurred during a security incident in the network. For each detected attack, the console generates an *Attack Story Line*, providing a quick overview of events that took place during the attack. From the settings console users can create group-based policies triggering various response actions from "alert" to "kill" to "quarantine" of a threat as soon as it's detected.

Suggestions for improvement

We feel manually downloading update packages only to re-upload them to the console to be redundant. We suggest allowing administrators to perform software updates by just selecting the new software version to be installed, and/or to implement automatic updates.

SentinelOne claims that customers will be notified when product updates are available, so that administrators are aware that they need to do download and install the new version. We find this a very inefficient means of distributing product updates, and note that during the course of our testing, we did not receive any email notifications from the manufacturer, even though a new version had been released.

Management Console

Installation and configuration

We tested the cloud-based version of SentinelOne's console, so no installation or configuration was required.

Layout

The console opens on the *Dashboard* page, which provides an overview of client activities and detected threats. The network health indicator on the dashboard page allows administrators to quickly see if there are any active or mitigated threats, such as malware infections, occurred on the monitored network. The menu on the left-hand side of the console allows navigation to the other main pages: *Activity*, *Analyze*, *Network*, *Black / White*, and *Settings*.

---

[4] https://sentinelone.com/support/

Preparing devices for deployment

We did not need to make any changes to client or server machines before deploying the protection software.

Deploying the endpoint protection software

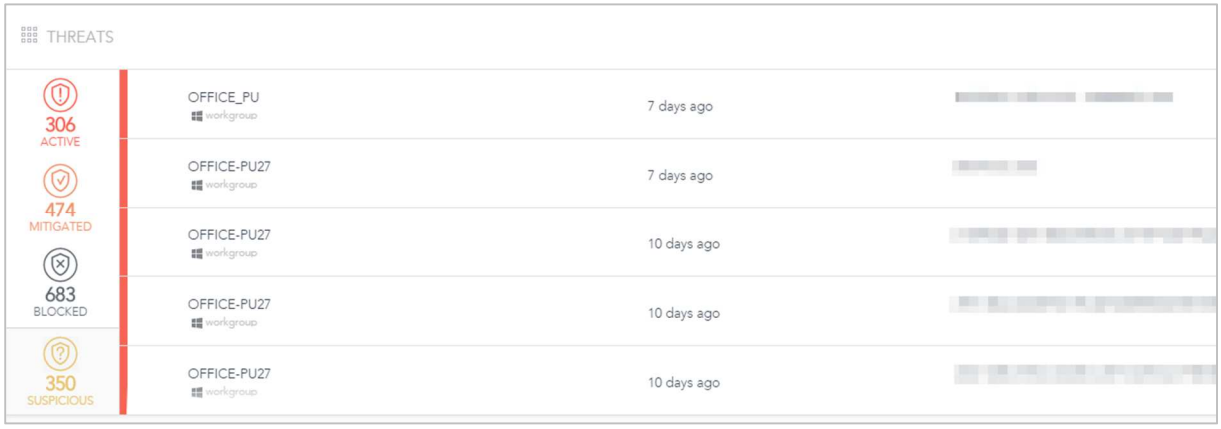
We deployed the endpoint software by logging on to the cloud console from the machine to be protected, and downloading the installer directly.

Monitoring the network

Status and alerts

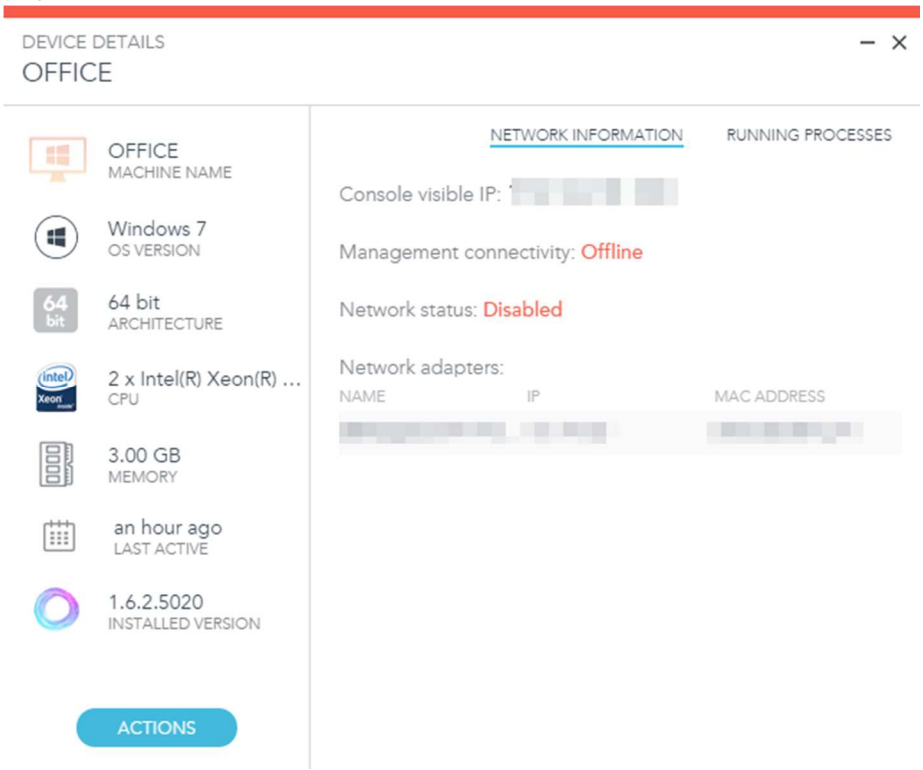
The *Threats* section on the *Dashboard* page lists all threats monitored on the network. Threats are divided into four categories: *Active*, *Mitigated*, *Blocked*, and *Suspicious*. Threats in the Active category are always displayed first in the threat list. The other categories can be added and removed from the threat list by clicking the respective icon in the management console.

The following alert is shown on the client when a threat is detected:



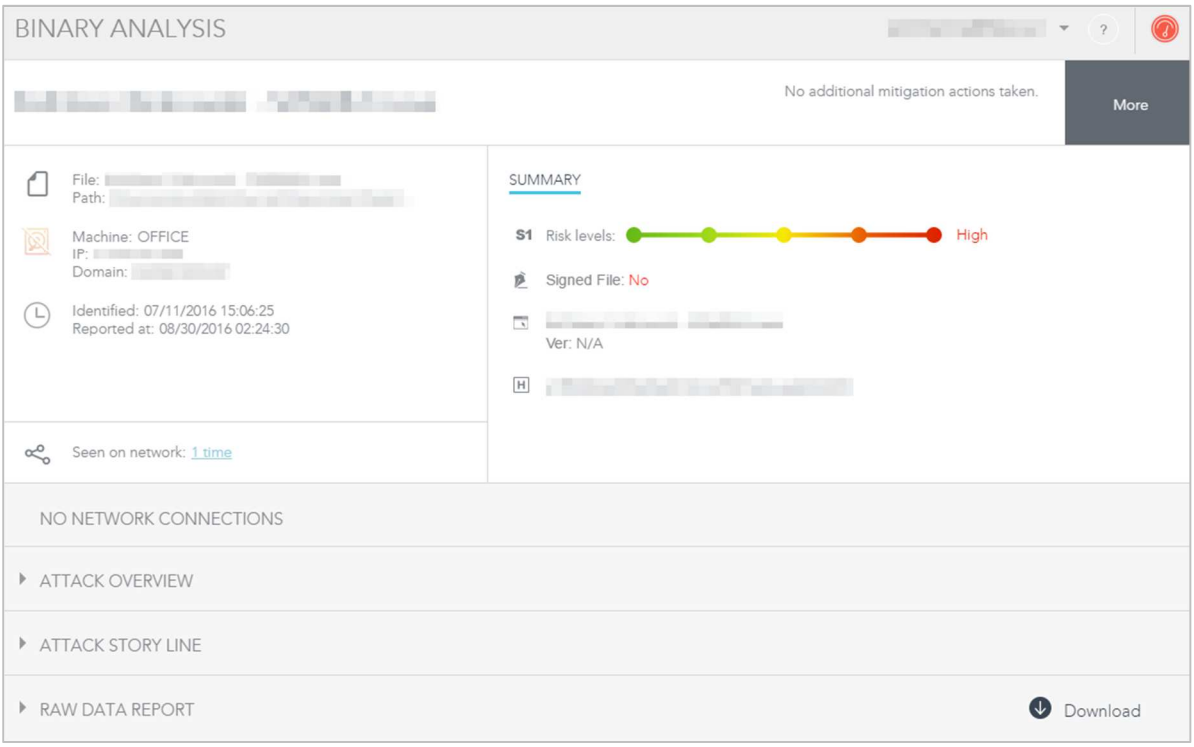
Furthermore, the *Network Health* section on the *Dashboard* page also provides a status summary for connected endpoints. The section displays the number of endpoints with detected infections or out-of-date protection software, as well as the number of currently online endpoints.

More detailed information about specific connected endpoints can be retrieved from the *Network* page:



Responding to alerts

If an alert is shown on the dashboard page, the admin can obtain more information about the alert by hovering the mouse over the relevant line and selecting *Analyze* from the menu at the right-hand side of the line. The analysis page of a threat provides information about all actions that were recorded during the attack.



If the endpoint was configured in alert-only mode, an administrator can select a manual mitigation action from the More menu and mark the threat as resolved. However, according to the vendor, manual intervention should rarely be needed. Although not set by default, SentinelOne recommends a kill or quarantine mode which automates the mitigation process.

Program version

The product version of the cloud console is displayed in the bottom right corner of the console screen.

The version of the installed endpoint protection software can be accessed by opening the details window of the relevant client from the *Network* page of the console.

Managing the network

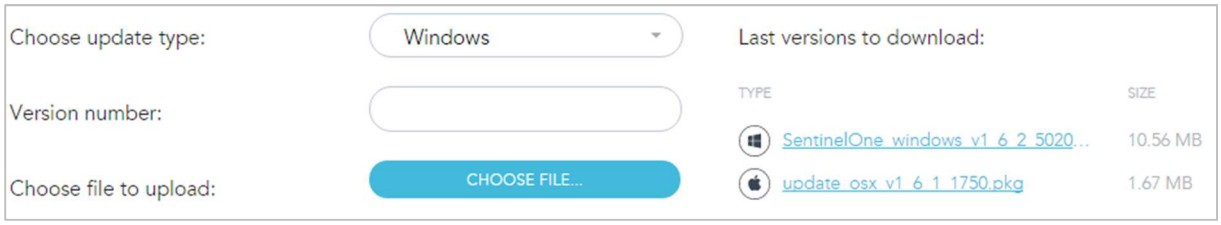
Scanning

There is no on-demand scanning feature, but the product does scan files through its Cloud Intelligence feature on-access, when the binary is added to disk.

Updates

Updates to endpoint software or the management console can be performed in the *Updates* section of the *Settings* page.

Updates need to be applied manually. The update process feels slightly awkward: To update existing software, an admin has to download the newest version of the respective software from a list presented on the right-hand side of the *Updates* page. After downloading the software update, the admin needs to upload the installation package to the console and manually specify the new version number.



Removing devices from the console

Using the *Actions* menu on the *Network* page, an administrator can uninstall the endpoint software of connected clients, thereby removing those devices from the console.

Client software

The client software has a minimal user interface and does not register with Windows Security Center as antivirus or antispyware.

About the test-labs

AV-Comparatives

AV-Comparatives is a vendor-independent organization offering systematic testing that checks whether security software such as PC/Mac-based antivirus products and mobile security solutions lives up to its promises. Using one of the largest sample collections worldwide, AV-Comparatives create real-world environments for accurate security tool testing offering freely accessible results to individuals, media and scientific institutions. Certification by AV-Comparatives provides an official seal of approval for software performance which is globally recognized. Currently, the Real-World Protection Test is the most comprehensive and complex test available when it comes to evaluating real-life protection capabilities of antivirus software. For this purpose AV-Comparatives runs one of the world largest IT security testing frameworks in a data centre located in Innsbruck.

Members of AV-Comparatives give frequently talks at the major IT security conferences like Virus Bulletin, AVAR, EICAR, IEEE Malware Conference, WATeR, AMTSO, BSides, Ninjacon.

The methodology of AV-Comparatives' Real-World Protection Test has received the following awards and certifications, including:

- **Constantinus Award** – given by the Austrian government
- **Cluster Award** – given by the Standortagentur Tirol – Tyrolean government
- **eAward** – given by report.at (Magazine for Computer Science) and the Office of the Federal Chancellor
- **Innovationspreis IT** – "Best Of" – given by Initiative Mittelstand Germany

AV-Comparatives' Management System is ISO 9001:2015 certified. The certification has been received from TÜV Austria for the management system with scope "Independent Tests of Anti-Virus Software".

AV-Comparatives is the first certified EICAR Trusted IT-Security Lab.

The data centre where AV-Comparatives runs the test equipment is ISO 27001:2013 certified.

MRG Effitas

MRG Effitas is a UK based, independent IT security research organisation which focuses on providing cutting edge efficacy assessment and assurance services, supply of malware samples to vendors and the latest news concerning new threats and other information in the field of IT security.

MRG Effitas' origin began when the "Malware Research Group" was formed in 2009 by Sveta Miladinov, an independent security researcher and consultant. In June 2009, Chris Pickard, joined, bringing expertise in process and methodology design, gained in the business process outsourcing market.

The Malware Research Group rapidly gained a reputation as being the leading efficacy assessor in the browser and online banking space and due to increasing demand for its services, was restructured in 2011 and became "MRG Effitas" with the parent company "Effitas".

Today, MRG Effitas has a team of analysts, researchers and associates across EMEA, USA and China, ensuring a truly global presence.

Since its inception, MRG Effitas has focused on providing ground-breaking testing processes, realistically modelling real world environments in order to generate the most accurate efficacy assessments possible.

MRG Effitas is recognised by several leading security vendors as being the leading testing and assessment organisation in the online banking, browser security and cloud security spaces and has become the partner of choice.

Members of MRG Effitas give frequently talks at the major IT security conferences like Botconf, DEF CON, WATeR (AMTSO), Hacktivity, Hacker Halted etc.

Our professionals hold the following certifications: CISSP, OSCP, OSCE, GPEN, SLAE, SPSE, CPTS, CHFI, MCP, OSWP.

Copyright and Disclaimer

This publication is Copyright © 2016 by AV-Comparatives ® / MRG Effitas ®. Any use of the results, etc. in whole or in part, is ONLY permitted with the explicit written agreement of the management board of AV-Comparatives / MRG Effitas, prior to any publication. AV-Comparatives / MRG Effitas and its testers cannot be held liable for any damage or loss which might occur as a result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives / MRG Effitas. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No-one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use (or inability to use), the services provided by the website, test documents or any related data.

For more information about AV-Comparatives / MRG Effitas and the testing methodologies please visit our website.

AV-Comparatives / MRG Effitas (November 2016)