SONICWALL

FAQ SONICWALL CAPTURE CLIENT

Performance & Operations

Q: How much memory does the Capture Client take up on top of SentinelOne?

A: The memory added by Capture Client in addition to that taken by SentinelOne is negligible (between 50-250 MB), as it does not have the same operating system hooks that the SentinelOne agent has. The Capture Client is more like a container for the SentinelOne engine and mostly functions as a policy/event broker and a watchdog service apart from the antivirus engine.

Q: How does behavior analysis work? What makes it different?

A: Behavior analysis relies on the ability to trace all activities on a system, including the creation/modification of files, execution of processes and scripts on disk and memory, and monitoring of inter-process communication to identify malicious activity. This information is analyzed by complex machine-learning models to detect malware based on behavioral patterns instead of static signatures. This allows the Capture Client to identify never-before-seen malware and threats, without the dependency of a signature/content update or a cloud lookup.

Q: Is there a file-size limit the client can handle?

A: No. There is no specific limit, because there is no explicit scanning function on the file. Instead, the Capture Client only monitors what the file does and, as such, does not need to handle the file.

Q: What platforms will it work on, including mobile?

A: The client will run on Window and MacOS at launch. A Linux version of the client is expected to be released at a later time.

Q: What operating systems will it support?

A: At launch, it will support Microsoft Windows (7 or later) and Mac OS (10.10 or later). We expect to include Windows Server support shortly after.

Q: Is there a local cache of signatures on the endpoint?

A: No. The technology does not work on signatures. AI-based antivirus is proven to be more successful.

Q: Why not use signatures?

A: The basic limitation of signatures is that they are based on a set of known patterns. However, the rate of growth of malware variations (in 2017 SonicWall cataloged over 58 million) is so fast that it is not possible to write and add new known patterns/signatures to the set. Signature AV requires near-constant updates, and significantly bogs down local system resources. Thus, signature-based technologies are unable to detect newer malware variants without research and signature-authoring for every variant. They also hamper system performance and offer disparate online and offline parity.

Q: Does Capture Client detect malware before or after execution?

A: Capture Client applies AI-powered malware analysis techniques both pre-execution and on-execution. Pre-execution, static AI, techniques include blacklists, whitelists and cloud intelligence, along with complex analysis of pre-execution attributes. On-execution, behavioral AI techniques focus on behavior that indicate lateral movement, credential theft, exploits, and other threat vectors used by malware. SentinelOne's static and behavioral AI models reside on the endpoint to provide autonomous prevention, detection, and response capability, regardless of an internet connection.

Rollback

Q: How does the rollback option work? Is it a shadow copy or an image?

A: The rollback function uses the Windows Volume Shadow Copy Service (VSS) available on all MS Windows endpoints. Currently, the rollback function is only available for MS Windows endpoints.

Q: How do you protect the shadow copy of the backup?

A: The Capture Client has an anti-tampering mechanism that protects the system, agent and underlying components. End-users and attackers cannot disable or uninstall the agent without authorization, which is provided in the form of a device-specific passphrase. Attempts to modify or tamper with the agent or VSS are monitored, logged and prevented.

Q: Does rollback work on Mac?

A: No. Rollback is not supported on MacOS endpoints.

Q: How often does it backup?

A: The rollback function reverts files to the last available version prior to its modification by the malware. Windows systems are pre-scheduled to back up at least every 4 hours. Backup frequency is customizable. Customers typically allocate 10 percent of free disk space to store volume shadow copies, which is sufficient to track changes over a period of 2 weeks or more.

Q: How much room does the shadow copy take up?

A: This depends on the size of the disk. A maximum limit can be set for every endpoint using Window policies. This is fully managed by the Windows operating system, and Capture Client only leverages the existence of shadow copies for rollback. Most end users will see no performance or system impact, as while they may not be aware of it, they already have VS running.

Q: How does the rollback option work for malware that delays its execution?

A: Rollback is useful in two situations:

1. When Capture Client is running in monitoring mode alongside a traditional AV, malware may be detected, but not blocked by Capture Client. Admins can initiate a rollback from the console to clean the system, instead of reimaging the system.
2. When there is a false negative (e.g., a threat that is not detected by Capture Client's engines), and the admin is notified, that admin can mark any process (and its children) as a threat and initiate rollback. This kills the malware process, adds it to the blacklist to immunize the whole network, and gets the user back to full productivity in a matter of minutes.

Rollback is a huge time-saver because of its ability to clean a system, and it eliminates need for remote troubleshooting, shipping the device to the IT helpdesk and reimaging the system.

Q: How long does it take to do the rollback?

A: This will usually depend on the size of the shadow copy, but it should be more than a few minutes for the larger disks.

SonicWall Integration

Q: Do you need a firewall?

A: A firewall is not necessary for the protection of endpoint clients using the Capture Client products.

Q: Will the endpoints be able to be managed by GMS on premises?

A: No. Capture Client is designed to be managed using a cloud-based management console. They will not be manageable using an on-premises GMS appliance at this time.

Q: Will Capture Client instances be managed by Cloud GMS?

A: Eventually Capture Client will be managed by a more-evolved version of Cloud GMS, called Capture Cloud.

Q: What SSL certificate (DPI-SSL) should you load?

A: This is left to the discretion of the administrator – it is advised not to use the SonicWall self-signed certificates for security purposes. Customers can generate their own using their in-house Public Key Infrastructure (PKI).

Q: Will the malware found on the endpoint be updated on the firewall (GAV)?

A: Not at this time. However, when Capture Client is integrated with Capture ATP, any new detections will automatically be shared with the firewalls as well, to reduce the need for multiple analyses.

Administration & Management

Q: Do we have administration delegation on the portal?

A: Yes, administrators can add multiple admins/viewers to the Cloud Management Console to delegate responsibilities.

Q: What powers do admins have?

A: Admins have complete access privileges for the tenant that they are an administrator of, including managing protected devices, managing protected users, modifying tenant settings, modify policies and auctioning threat events.

Q: Will there be a charge for the cloud-based management?

A: No, this is free of charge.

Q: Can you whitelist files such as medical records?

A: Yes, on the management console files can be marked as benign to be whitelisted.

Third-Party Integration

Q: Will it work in conjunction with other clients?

A: Capture Client will theoretically work in tandem with any other endpoint client. However, we highly recommend not to run multiple client security technologies on the same endpoint, as this could cause performance issues and productivity frustrations for the end-user.

Q: Will it support the Firefox root store?

A: At this time, Firefox is supported by forcing Firefox to use the Windows certificate store. Support for the Firefox root store is slated for a later release.

Q: Is there any integration with ticketing systems?

A: Capture Client's Cloud Management Console makes available a set of open APIs that allow for easy integration with any third-party ticketing system. We are reviewing the possibility of strategic integrations with popular ticketing systems used by our customers.

Others

Q: How often does SentinelOne get tested by NSS Labs?

A: Every year.

Q: Is this a viable replacement for imaging systems?

A: No. It is not recommended to use it in that fashion.

Q: What if you install it on an already compromised PC?

A: If the Capture Client is installed on a compromised system, all processes and activity will be monitored and actioned accordingly. Should malware be active or other active threats/ suspicious scripts be running, SentinelOne will autonomously respond at machine speed. The solution also has a background scan capability upon install, if the end customer/partner is interested in "cleaning house." The background scan is a useful tool to run, as it will illustrate existing malware and threats missed by whichever AV resided on the system prior to the Capture Client.

Q: How is the client deployed to an entire organization?

A: There are three basic methods by which clients can be distributed:

a. A Windows Installer (MSI) package and a Mac OS Package are available to be deployed through any third-party software rollout platforms like MS SCCM. This may also be manually distributed for machines not managed by domains.
b. A customized URL is auto-created for every tenant where clients can go and download and have the client installed by themselves. This can also be automated in domain-managed networks using startup scripts via Group Policy Objects (GPO).
c. For endpoints protected by SonicWall firewalls, enforcement policies can be applied to force clients to download and install the client from the URL, without which they will be unable to use network service protected by the firewall.

In all of these conditions, the end user need not enter any information to proceed through the installer.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com