ABOUT US

enSilo comprehensively secures the endpoint with automated detection and response against advanced malware, without further burdening cybersecurity staff.

enSilo's single lightweight agent includes next generation antivirus (NGAV), automated endpoint detection and response (EDR).

Coupled with a patented approach that has full system visibility, enSilo's endpoint security solution stops modern malware pre and post infection real time.

Cybersecurity staff with enSilo can effectively manage malware threats without alert fatigue, dwell time or breach anxiety.

enSilo cloud management platform is intuitive and extensible to meet operational needs that stop malware impact.

A Single Lightweight Security Agent

Capable of running on Windows, Mac, and Linux, our agent is modular and unified, providing the lightest and fastest protection available.

New in enSilo Version 2.6

Threat Hunting: Are blind or burdened? Most endpoint security is blind to advanced modern malware or is so dependent on real human monitoring it, that it's a burden to use. enSilo gives you the real-time threat visibility without the burden. It can find malware that's already dormant (and hiding) in your enterprise.

Use threat hunting to expedite incident response using automatic searches of historical data, or to find and remediate dormant threats in your environment. This feature requires additional licensing from enSilo.

Communicating Applications Reputation Scoring: enSilo provides the most comprehensive endpoint security on the market. With application reputation scores you can now simplify decision making and add greater visibility to each application in your enterprise. Don't let don't let vulnerable or notorious applications communicate outside your systems. Get full path and hash data to enable better forensic investigation.

System Events: Get improved visibility to your endpoint's total health with the new System Events Viewer.

Additional Capabilities: enSilo 2.6 gives you all the capability to you need to protect your enterprise against the latest advanced malware threats, without the additive cost you get with manual EDR. enSilo's automated endpoint security gives you one comprehensive platform that offers real-time blocking of pre-and post-execution malware. Our automated protection preserves your business continuity and user productivity. With enSilo you never have to physically isolate an infected server. Instead, let enSilo block the threat while your users continue to work, and your business continues to operate like normal.

Real-Time Protection: Our NextGen Antivirus provides sound pre-execution malware protection that protects endpoints from countless malware threats. When used in conjunction with our Application Communication Control and Automated EDR, enSilo provides the most comprehensive endpoint security solution available.

No other solution can reduce your response gap as effectively as enSilo

- We block in real-time
- Customizable, fully-automated courses of action
- Lightweight local agent, cloud or local premise hosted

www.ensilo.com 182 Second Street, Suite 210 San Francisco, CA 94105

enSilo – Version 2.6 – Release Notes

These release notes describe the main new features and known issues in the enSilo version 2.6 release.

Version Highlights

- Threat Hunting – Hunt for threats residing in your environment and expedite incident response using automatic searches of historical data, in order to find and remediate dormant threats in the environment. The Threat Hunting feature requires a specific license from enSilo.
- Communicating Applications Reputation Scoring – Application Reputation scores are now available to simplify decision making and Communication Control module operation. In addition, greater visibility into an application's full path and hash enable better forensics investigation.
- System Events – Improved visibility into the system state and better health monitoring are now possible via the new System Events viewer. System events can be retrieved also via Syslog, email and the enSilo API.
- Exception Manager Redesign – A redesigned Exception Manager enables easier navigation and better performance.
- Improved License Capacity Management – Devices that have not connected to the system for more than 30 days are not counted towards your enSilo license.
- Loading Server Certificate – Tighten security and enhance privacy by uploading a specific SSL certificate into the enSilo Central Manger.
- System Inventory Enhancements – Inventory enhancements enable simplified Collector inventory management and device tracing. Enhancements include the addition of the Collector's MAC address and additional sorting capabilities.

Resolved Issues

- Security Events Emails – Emails regarding Security events from the enSilo system now include the corresponding Collector group.
- Syslog – Issues when using syslog over SSL were resolved. The HEADER of the syslog message now includes the IP of the Center Manager.

Known Issues

- Component Backwards Compatibility – The V2.6 Central Manager supports Cores/Collectors from older versions with limited functionality. Some new features introduced in later versions will not work.
- Communication Control Deny Action – When the Core is not accessible, applications that are set to *deny* will not be blocked.
- Threat Hunting – Threat hunting data is available for files saved/executed after the enSilo Collector was installed, and only for devices running Collectors V2.6 and up.
- AVG Connection Issues – When AVG is installed on the device, it blocks the Collector connection.

  Workaround to resolve this issue –

  - Set exceptions in AVG on the enSilo Collector.
- Downgrade the Collector Version – When downgrading and restarting a device, the Collector does not start.

  Workaround to resolve this issue –

  - Uninstall the Collector, reboot the device and then install the older version.