CSO
FROM IDG
February 28, 2018 www.csoonline.com

REVIEW

Review: The enSilo platform traps threats that bypass traditional endpoint defenses

The enSilo platform offers traditional endpoint protection alongside the ability to offer post-infection protection. It can also trap threats, holding them in place and rendering them harmless until a threat hunter can arrive to investigate.

By John Breeden II

There are two intersecting trends in cybersecurity that almost every organization will need to soon address. First, endpoints are the new battleground for network protection. They are the gateway that advanced persistent threats use to enter a network, and sometimes also comprise the target for certain attacks. Second, almost every organization, no matter how secure, will eventually get breached.

The enSilo platform sits at the intersection of those two trends, offering traditional endpoint protection alongside the ability to offer post-infection protection. It can also trap threats, holding them in place and rendering them harmless until a threat hunter can arrive to investigate, though that feature is completely optional.

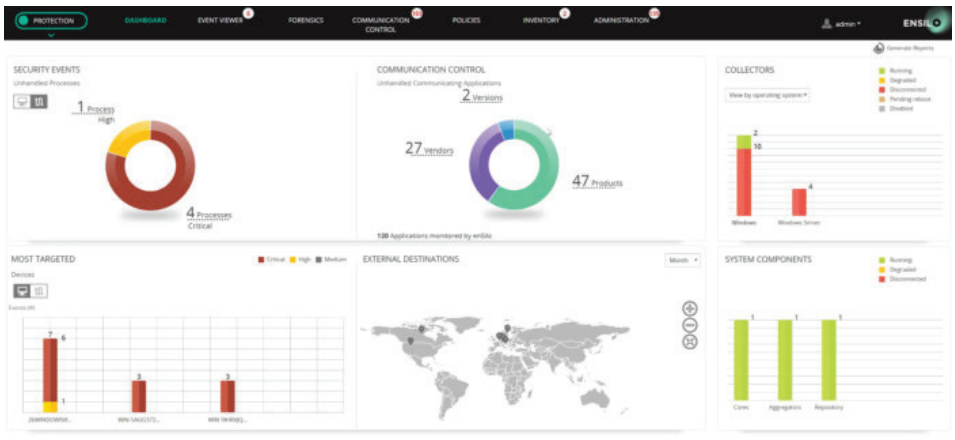
Installing enSilo is not unlike other agent-based security programs. There is a central console called the Core where administrators set policies that get deployed to agents, which are called collectors by the program. Collectors can be lightweight, simply reporting threats and information back to the central console, or much more powerful, taking actions and remediating threats as they are detected. They can even be set to work autonomously when disconnected from a network or the Core, a huge boon for laptops and other devices that don't spend their days tethered to network cables.

The collectors work with devices installed on-premises or in the cloud, or any hybrid setup. Pricing for enSilo is based on the number protected devices the program is protecting, with volume discounts available for large enterprises.

When thoroughly examined, enSilo is different from most other forms of protection available for endpoints, with a lot of control available to help it fit into organizations regardless of their cybersecurity maturity. It can be almost completely manual, or fully automated, though those are just two options in a wide spectrum.

The reason that enSilo works so well is because it's based on allowed behaviors of programs and procedures as set forth by the operating system (OS). In the case of Windows, the teams at enSilo have reverse engineered how the OS works, what processes it allows, and the reasons for those actions. Collectors, once installed, sit between the OS and the rest of the system, giving administrators total control over what kinds of activities are allowed on endpoints.

For example, Windows allows some processes to communicate, while others are restricted. Advanced threats often break or bypass those rules. However, to do so on a machine protected by enSilo, the malware would have to pass through an enSilo collector first, which will trigger a rules violation even against a previously unknown threat. And because administrators have total control, they can allow some malware to take a few steps down the kill chain, while still preventing it from doing any actual harm. That way, it essentially traps the unknown malware in place, rendering it harmless but not removing it, so it can be studied to help build future defenses, or to

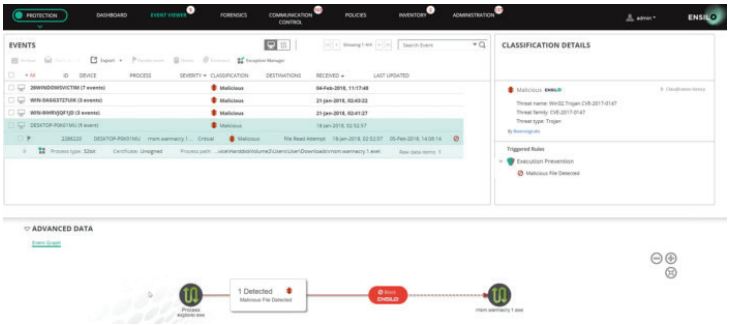


John Breeden II/IDG

The dashboard for enSilo shows all devices that need attention, including any that have been infected, but have the threat under control and trapped for analysis.

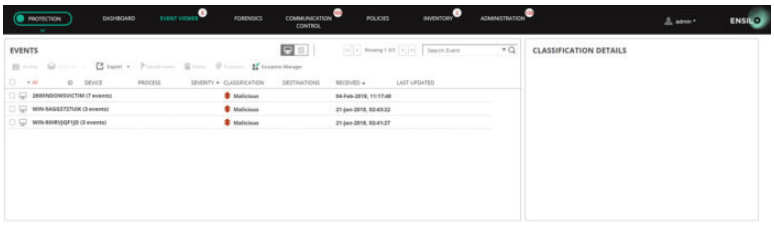
reveal targeted campaigns and threat actors.

Organizations with mature cybersecurity postures, such as those that use threat hunting, can send in human hunters to analyze trapped malware, discovering where it was trying to beacon out to, what its goals were, what tactics the attackers planned to use to evade network protections and other critical information about the attack. This is what good threat hunters do anyway, but most of the time they must use advanced toolsets and spend a lot of time finding malicious programs that have breached their network and remained hidden. With enSilo, they are pointed to the exact spot where the unknown threat is trapped and can examine it at their leisure. It's less like threat hunting, and more like threat trapping.



John Breeden II/IDG

Akin to traditional protection, enSilo can be set to block and eliminate threats found on any protected endpoint, even post-breach. Here, WannaCry has been blocked and removed.



John Breeden II/IDG

The events panel shows a list of threats that evaded frontline antivirus protection, only to get caught post-breach by enSilo. They can be remediated from here, studied to learn more about advanced attackers, or set to automatically be eliminated from the network.

Not every threat needs to go up against such advanced protection. There are millions of known viruses and malware programs out there, and millions of variants on common themes. Regular antivirus or antimalware protection can stop them, so enSilo ships with its own AV program for its front end. Organizations that are required by policy to have antivirus protection on their endpoints can thus install enSilo and get advanced protection alongside compliance. Or, enSilo can work with any existing antivirus or next-generation antivirus that an organization already has installed. Because any AV sits at the perimeter, and enSilo is installed between the OS and everything else, they are completely compatible and never even cross paths. Every threat stopped by AV is one less that enSilo has to worry about.

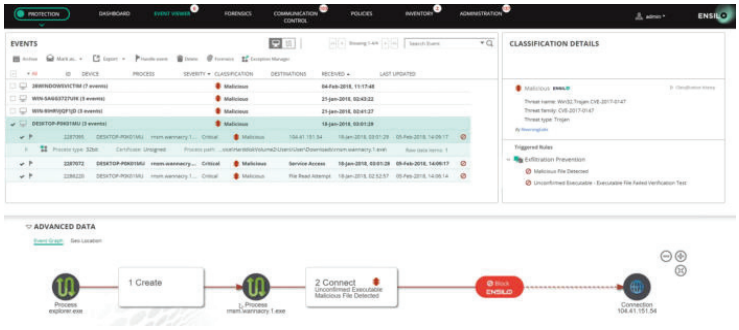
In addition to blocking or trapping malware, there are many other options. These include reporting the unknown threat to a SIEM, sending out an e-mail or creating a trouble ticket among others. Automatic remediation is also possible, eliminating threats after they attempt to do something malicious. Any combination of all those actions is also possible, and different policies can be applied to different groups within an organization, or to individual users.

With so many options, testing enSilo was extremely interesting. To see the range of the protection available, a collector sitting on an endpoint was first set to block and remediate threats. When infected with a new WannaCry variant, it blocked it from beaconing out and eliminated the threat as ordered, even though it was able to bypass AV and was essentially an unknown program.

After that, the enSilo Core was reprogrammed to instead capture threats, and that policy pushed out to collectors. Now when WannaCry showed up, it was allowed to initially execute, though its beaconing was blocked, with the attempt recorded. It was also prevented from encrypting anything or taking any hostile action. It was still technically infecting the targeted endpoint, yet there were no ill effects. The SIEM could be notified and threat hunters dispatched to examine it, but they could do so at their leisure. There would be no rush to see what a malicious program is doing, or to try and stop data exfiltration. The malware was simply stuck in limbo on the endpoint waiting for investigators to examine it. Users likely would not even know that it was there.

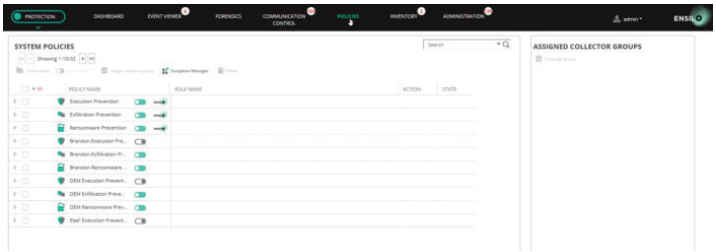
The enSilo platform is a unique and powerful way to protect endpoints. Its biggest strength, besides having a nearly perfect detection rate based on program behavior within specific operating systems, is its flexibility. It can be set to be little more than post-breach insurance, automatically detecting and killing malware that bypasses AV protection. Or it can be configured as an advanced investigation tool, halting unknown threats and letting security teams examine them in safety. Or it can be just about anything in-between.

Any organization that wants to get serous about protecting their endpoints against both common threats and advanced ones that bypass traditional protection will find a powerful ally in the enSilo platform. It's fast, extremely flexible, and accurate.



John Breeden II/IDG

And here, WannaCry has been allowed to infect an endpoint by enSilo. But have no fear, because while the insidious malware is technically installed on the system, it has been prevented from contacting control servers or encrypting any files. It's essentially trapped and harmless, ready for threat hunters to study at their leisure.



John Breeden II/IDG

One of the strengths of enSilo is its ability to automatically fix problems and security breaches that it encounters, if you configure it to do so. It can even fix problems on systems that have been disconnected from a network.