SANS

WHAT WORKS™

WhatWorks in Endpoint Security: Surviving Advanced Targeted Attacks by Augmenting (or Replacing) Legacy AV with enSilo

SPONSORED BY

WhatWorks is a user-to-user program in which security managers who have implemented effective Internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned. Got a story of your own? A product you'd like to know about? Let us know.

www.sans.org/whatworks

Every security professional knows that traditional signature-based antiviral software is ineffective against advanced targeted attacks. While more advanced endpoint detection and response products have proven to be effective against advanced threats, fears of false positives and the impact of changing security software on the desktop have caused many enterprises to hesitate in improving endpoint security – and the rise in business-damaging breaches continues.

During this SANS WhatWorks webcast, the cybersecurity manager at a global, diversified firm will provide details of his deployment of enSilo to enable continuous monitoring and real-time remediation on Windows and Mac desktops, reduced impact and demonstrating benefits to increased integrity and availability of critical business processes.

Join SANS Director of Emerging Security Trends John Pescatore and the user to hear details on the selection, deployment and experience using enSilo. The webcast will contain a discussion of lessons learned and best practices as well as detail the metrics used to demonstrate the value of enSilo.

ABOUT THE INTERVIEWER

John Pescatore, Director of Emerging Security Trends, SANS Institute

John Pescatore joined SANS as director of emerging security trends in January 2013 after more than 13 years as lead security analyst for Gartner, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and voice systems "and the occasional ballistic armor installation." John has testified before Congress about cyber security, was named one of the 15 most-influential people in security in 2008 and remains an NSA-certified cryptologic engineer.

Q First, tell me a little bit about your company and what role you play in the company?

A Our company is set up globally, and we are in more than 150 different countries today. We are in different areas starting from the retail business to the music industry. I am the IT security manager, and I am part of the digital security team within the company. We are a team with about 10 people who are taking care of security for the whole company worldwide.

Q Since you ended up with enSilo's Endpoint Security Platform what problems were you trying to address when you started looking into this area?

A We started two or three years ago and the one of the biggest pain points we had was ransomware. We mainly searched for a solution to stop ransomware and all of the advanced targeted threats, all new threats coming to us which can't be solved by classical antivirus software.

Q I assume you had mostly Windows PCs in use with standard antiviral or endpoint protection suite on every PC?

A Three out of four of our user workstations are Windows clients and the rest are Mac devices. We had a lot of ransomware and we searched for a global solution which would work seamlessly without annoying the user. We needed a solution which is lightweight, classic antivirus solutions are very heavy and can cause some startup delays and other issues that impact the user.

Q Can you walk us through what process you used to look at possible products and processes and how you evaluated them?

A We evaluated almost every product out there, or at least every big one which was on the market at that time. We had a Proof of Concept (POC) which included almost everybody. I think we tested 10 different applications over one year. We had certain criteria like detection of advanced malware, the performance on the client, how easy it is to use, what is the effort for us and what is the impact on the users were the main goals for us to have a solution in place. There were some vendors which we eliminated very easily because we were unable to use the product because if you install their solution in full protection mode every keystroke took a couple of seconds, which was unacceptable. On others we spent a little bit more time doing more detailed evaluation.

What we liked most about enSilo is the post-infection protection. It took me almost 3 months until I really got what it's doing but it's great. On other tools you just get statistical values like the application you are trying to execute is scored "70", but what does "70" really mean and where's the threshold between good and bad? enSilo makes it the other way around. You are executing it, they are "recording" what is happening, and they stop any negative consequences., Their software really knows what it is doing, and they don't have to deal with statistical values. This is what in the end made enSilo the winner for us.

Q How did the malware detection rate perform?

A We had a good detection rate since for us almost every malware we pen tested was caught by them. We just had one sample which we were able to bypass and to fix it afterwards.

Q For your proof of concept, you put it on the desktops of the IT security team, of IT people? This is often a hard area for enterprises to do proof of concepts. How did you do it?

A With the 10 vendors at first, we just had a single desktop installation where we made some pretesting and selected the three best for us. We made an IT-wide comparison. We rolled it out to approximately 100 machines and compared the results.

Q You talked about a high detection rate, how about false positives?

A With enSilo we have very, very few false positives. We adjusted the policy set and now it is perfect for our environment. We can be very granular which allows us to whitelist our own applications, so we are currently running almost without any false positives. On the other products we had bigger issues because of the statistical values and the threshold just was applied. For example, our business planning tool was impacted and we would have no longer been able to it.

Q You went through the evaluation and enSilo won the competition. Once you made the decision to go with them how did you go about rolling the product out operationally?

A We did it in small chunks, country by country. We started very slowly because we were afraid of false positives at the beginning, but it went so smooth in the end we moved to bigger chunks. So, our plan was to do it in half a year and we managed to do it in three months.

Q Did you start in some sort of monitoring mode and then turn on more active capabilities or how did that work?

A Yes. This is what we are currently also doing. During the rollout every client was placed in monitoring mode. After a couple of weeks, we just set it to a medium security policy setting and if we see a malicious event on the client we put it into a blocking mode. This is the same approach we have used during the rollout and we just stick to this process. If we add new clients, they always start for two weeks with monitoring mode just to see what's going on and to avoid any impact for users. This is necessary for us because we don't have a single "golden" image on our desktops. We have several areas of operations, we have several different desktop products and applications used in different areas. For example, the Italian employees can use other products compared to those in Germany or the US and so on. Every country has the freedom of using the application they need to work. We can't say before a client is coming to the system what applications are going to be run on it. So, we decided to always start in monitoring mode.

Q Are you using enSilo in addition to the antiviral products used in those different countries versus replacing AV?

A In the beginning we had Mac clients run enSilo and a classical antivirus solution in parallel, but we removed the classical antivirus on Mac OS completely, so we are just running enSilo on them. For the standard Windows clients we are going to remove the incumbent antivirus and just stick to enSilo and in certain areas we just enable the built-in antivirus solution in addition. But the product we most rely on regarding malware is enSilo because it is also proven effective in detecting standard malware which would be caught by classical antivirus system.

Q I think you said it is about 15,000 endpoints which is a pretty big number. How have you found their products management capabilities to support a large installation?

A They have a nice interface, we can do everything we need. There is always room for improvements, but I am completely satisfied.

Q Architecturally, there is software on the endpoints and is there some sort of management server or servers that you put out or how is the architecture when you've deployed it?

A We are using it in the cloud, software as a service. So, enSilo is running almost everything for us. We just have the client which we are rolling out with our standard client solution or client management system and that is it. We don't have anything running inhouse on servers. We don't have any maintenance for the server for the application or anything. We just get information that a new version is available and if we want to have it installed, and as soon as it's installed, it's fine.

Q How do you manage this? You mentioned alerts and then you would put things into blocking mode so how is this managed? Is there some additional administrator for this? Is it part of somebody else who was already in charge of endpoint security? How does that work?

A We have a services partner who is taking care of our client environment. We trained several people at our site together with enSilo to handle basic events so they are doing it 24/7 for us. If they have a question or an event they are unsure about, they can send it to enSilo service team and we'll get an answer. So mainly, our partner who is managing our clients, who knows our clients and the applications best, is also operating enSilo. And the events they are finding, they send directly to the security operations center who will investigate and do a follow-up on it.

Q So, the partner managing the desktops is managing overall IT support for the desktops, not just security. Is that right?

A Yes. enSilo is the first security tool they are using, and we made this decision because they know the clients best. Our partner knows which scripts are running on it, if something looks suspicious which is not normal they can identify it more easily compared to an external partner because they don't know our environment, they don't know which scripts we are using and how we manage clients. We do it probably a little bit different to other companies.

Q How long have you had enSilo operationally now?

A At least one and a half years.

Q Is there some recent event, maybe some malware or ransomware that hit you in 2018 you could sort of walk us through how it worked from the ransomware hitting their machine or some number of machines and how that worked through to resolution?

A Meltdown and Spectre, come to mind. Everybody read about it in the media, including our CEO. He wanted to know if we were at risk, so we just sent an email to enSilo and ask them were we at risk from this vulnerability? Is enSilo protecting us against it and are we safe? They quickly came back with an email saying no, attackers could try to exploit the vulnerability but enSilo stopped any possible consequences. Meaning if somebody is gathering data from the CPU, this could work, but the data will never leave the machine. The consequence is stopped. And the best thing is we can say to our CEO yes, we are secure, nothing will happen to our data. I assume at this time almost nobody in the IT could say we don't have an issue with Meltdown and Spectre, we are secure. which is a great thing for us. We don't have to worry about it. We don't have to patch the firmware of 15,000 devices on a disruptive rush schedule. It gives us more time.

The bigger benefit we showed our CEO was that we no longer have any business impact from ransomware or advanced malware. We see it that it reaches our PCs, so the behavior of the user hasn't changed but there is no consequence for us and if the CEO and his peers are sitting together and talking about ransomware he can say hey, we are absolutely fine which is perfect for us and then for our reputation from the security department and from the client security department

Q People are always wondering about the tuning required for these types of products. How much initial and ongoing effort is involved in tuning the enSilo product?

A The only thing we changed from the out of the box product is the policy set but this has been done during the POC. We adjusted certain policies from blocking to logging mode to have better visibility and to avoid false positives and we are working great with this policy set. We have never adjusted it and the policies set is for every division of the company is the same.

Q How do you handle removal of malware? I know the enSilo product can prevent execution and bad things from happening, does it also handle removal?

A I know it from the POCs that there is a remediation functionality. However, if we have real heavy events on the clients we are going to reimage the machine for two reasons. We just want to show the user that he has done something with consequence, so he should also feel that he has done something bad, but he is not harming the company. He should get the feeling that next time it won't happen to him. Another thing, from my point of view you will never really know what is left behind on the client if you are hit by a true zero day or advanced targeted threat. So, if you just do some simple remediation and cleanup process I don't know what is left behind. That is the reason why we reimaged all of the machines after heavy events. If we have smaller events the country administrators go to the users and do the remediation because the users should see that something happened, and it causes effort for the company.

Q Many companies find it difficult to change security products on the desktops. How did you get the management approval and funding to go ahead and do this since it is a big effort to do this across 15,000 desktops?

A We just showed our CEO the results from our POC. So, it was quite easy, and our managers trusted us. We have worked hard to build credibility, so if we say this is the right product for us then he says okay, we trust you. If you trust in the vendor of the product, no problem at all.

Q Since you've been going for roughly a year and a half now how have you found this support to be from enSilo?

A Incredible. I think some of it might be because they are quite young but if you shoot them a question you will get an answer in maximum one hour. So, it has never taken long and if we see some enhancements or some features needed they will be implemented very, very quickly. So, it is professional and fast if we have any question or regards on enSilo.

Q Knowing what you now know and the lessons you learned in getting this far is there something you would do differently if you were starting again today, some lessons learned you can pass on to our audience?

A There is just one major lesson learned. enSilo has also the capability for "communication control" which means you can stop the network traffic for a certain application. We use it for our "Potential unwanted applications" for example.

enSilo grabs the information from the machine, the meta information like vendor, product or version from the executables. Based on this information you can deny network traffic. We use it for example to prevent BitTorrent or Tor Browsers. This needs to be handled with caution. If you do it on a vendor level, imagine what will happen if you block all network traffic from the vendor "Microsoft."

Q Do you forward alerts or information that comes from the enSilo product? Are you forwarding that to a SIEM or some central security logging and monitoring type capability?

A Yes. We send it to several places, all of the log files. We have three tools which are consuming the data.

Q Are there any features or capabilities you have requested that you're looking forward to seeing coming in the product?

A I see especially some Endpoint Detection and Response (EDR) features which came up and which are as far as I know on the roadmap. They always have an ambitious roadmap and I am really looking forward to the next versions.

Q Were there any concerns that since it is doing some level of monitoring and capture that there are any privacy concerns in the different countries in Europe or the European regulations or did you have to go through any sort of look at privacy issues to roll it out?

A No, because we clarified everything beforehand, it was also part of the POC to determine which data is collected from the client. Very little data is collected and I don't see any privacy issue. If I'm running the machine completely normal without clicking on malicious links or something, nothing is recorded. I am never tracking the user where he is surfing to, what he is doing though it is not a tool which records everything a user is doing like web surfing, it is just recognizing malicious behavior. We discussed with all of the country managers all over the world and it was absolutely fine for them and there was no issue at any time or no question at any time about privacy.

Q Final question, do you have future plans for enhancing or doing different types of things with the enSilo product?

A Yes, we are thinking about having enSilo installed on our servers. Classical antivirus system is not the best thing for every server or every type of server, so currently we are evaluating the performance, the pros and cons from having enSilo on certain servers. This is the next step we are focusing on.