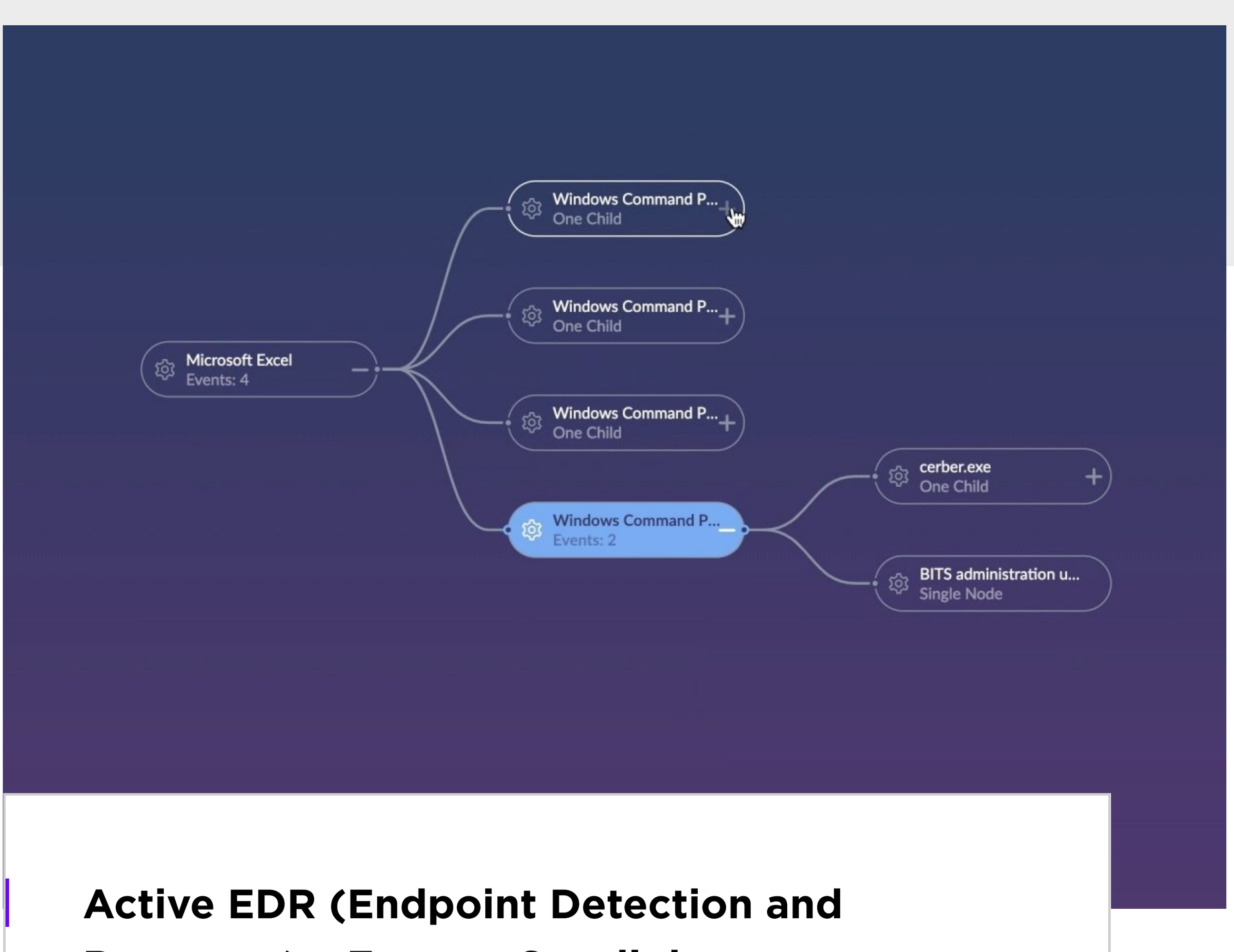
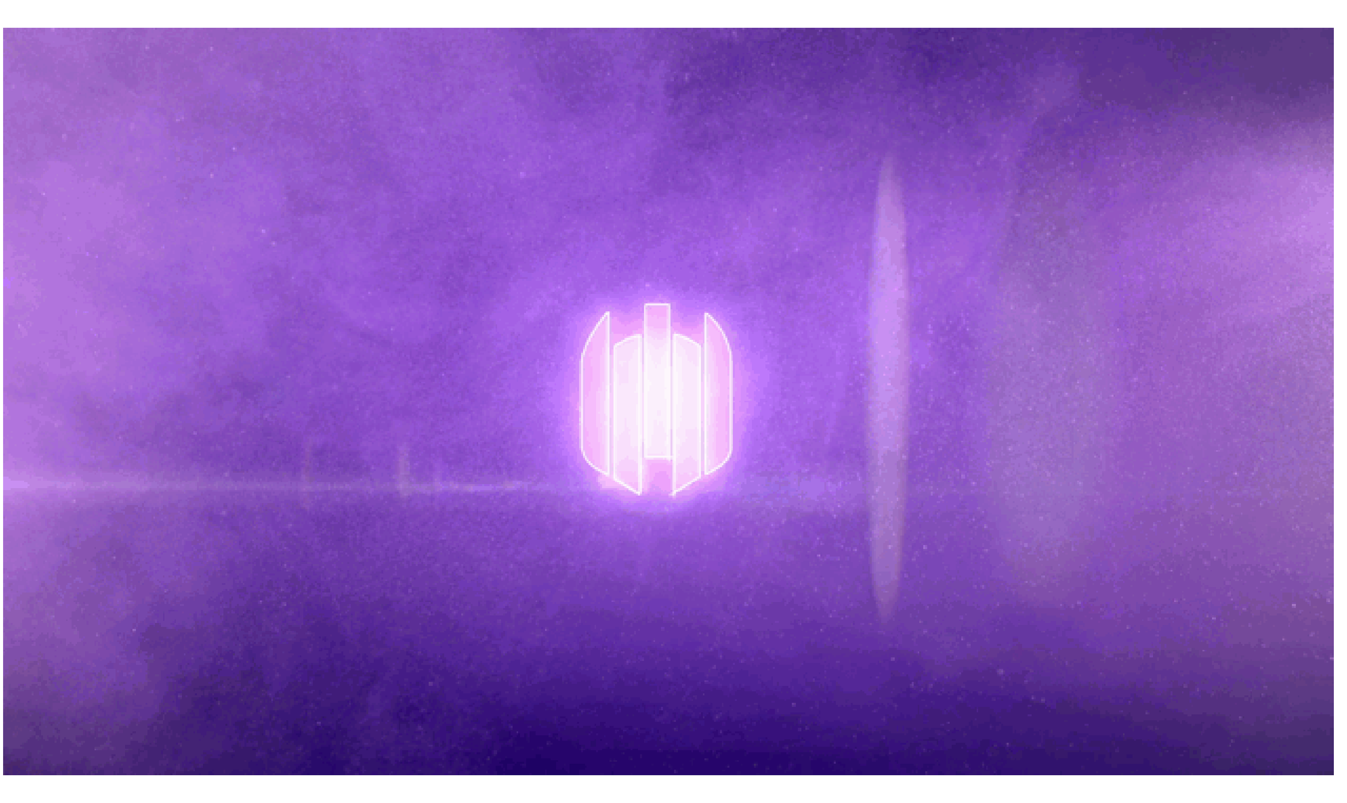


Active EDR (Endpoint Detection and Response) – Feature Spotlight

February 28, 2019
by Migo Kedem

Today we are pleased to announce the revolutionary technology of ActiveEDR. ActiveEDR solves the problems of EDR as you know it by tracking and contextualizing everything on a device. ActiveEDR is able to identify malicious acts in real time, automating the required responses and allowing easy threat hunting by searching on a single IOC. Read more to understand how we got here and how we created the first and only EDR that is truly active.



Background

In the short history of cybersecurity, we have seen how technologies become outdated pretty quickly as the threat landscape changes continuously. When threats began to emerge in the 90s, many businesses moved to install antivirus protection. These new products were able to fight against a relatively small amount of known viruses although they could not combat novel attacks.

Malware authors adapted quickly with trojan horses and worms running after the new gold.

Added to this was the explosion of the Dark Web and the ability of cybercriminals to share and sell tools and tactics without being traced. Trade in ransomware tools alone created a micro-economy among online criminals. When cryptocurrency was born, it solved a huge problem for these malicious groups, as they could now exploit individuals and businesses without leaving a financial trace.

Making AI Accessible to Everyone

To meet these challenges, enterprises needed better solutions. When AI technology became available, it did not take long for new innovative products to replace the legacy tools based on signature detection.

These new EPP (Endpoint Protection Platform) tools trained a model on a large number of samples, then used an agent on the endpoint to tackle file-based malware. As much file-based malware is a reuse of existing malware, the AI could be used to detect these similarities without having to provide a local agent with constant updates.

These new tools provided some relief to the enterprise, but malware groups quickly discovered that EPP products were utterly blind to memory based malware, lateral movement, and fileless malware attacks. To make things worse, sophisticated hacking tools made their way to a wider audience. Through NSA leaks, nation-state malware tools and techniques became available to cybercriminals. The enterprise needed a new solution.

To fill this gap, a new line of products called EDR (Endpoint Detection and Response) was born. EDR answered the need of the enterprise to be able to at least see what was happening on the corporate network. Visibility was the solution, and its new home was the cloud.

But these EDR solutions created a new set of problems. EDR, as it stands today, provides visibility, but requires skilled personnel that can take the vast amounts of data it generates, contextualize it, and then use it to mitigate the cyber threat. Greater demand for talented cyber analysts has created a massive labor shortage in the security industry. At the same time, cloud-based solutions suffer the problem of increased dwell time – the delay between infection and detection. Solving these problems is where ActiveEDR comes into play.

What is ActiveEDR

Track Everything

Contextualize and Identify Evil in Real Time

Respond & Rollback

Threat Hunt with TrueContext

With so many activities happening on every device, sending all this information to the cloud for analysis might offer visibility, but it is still far from solving the main problem: the flood of alerts facing understaffed security teams. What if you could put the equivalent of a skilled SOC analyst on each of your devices? An agent that can contextualize all the device's activities and identify and mitigate threat attempts in real time?

ActiveEDR has some similarities to other EDR solutions, but unlike those, it does not rely on cloud connectivity to make a detection. This effectively reduces dwell time to run time. The agent uses AI to take a decision without depending on cloud connectivity. The ActiveEDR constantly draws stories of what is happening on the endpoint. Once it detects harm, it is capable of mitigating not only malicious files and operations but the entire 'storyline'.

Consider this typical scenario: A user opens a tab in Google Chrome and downloads a file he believes to be safe. He then executes the file. This program is malicious, initiating PowerShell to delete the local backups and then start encrypting all data on the disk. ActiveEDR knows the full story, so it will mitigate this at run time, before encryption begins. When the story is mitigated, all the elements in that story will be taken care of, all the way to the Chrome tab the user opened in the browser. It works by giving each of the elements in the story the same TrueContext ID. These stories are then sent to the management console, allowing visibility and easy threat hunting for security analysts and IT administrators.

A New Experience for the Security Analyst

The work of a security analyst using passive EDR solutions can be hard.

Swamped with alerts, the analyst needs to assemble the data into a meaningful story. With ActiveEDR, this work is instead done by the agent on the endpoint. The stories are already assembled using TrueContext, so the security analyst can save time and focus on what matters. Instead of assembling stories, the analyst can review full, contextualized stories, based on a single IOC search. This allows security teams to understand the story and root cause behind a threat quickly. The technology can autonomously attribute each event on the endpoint to its root cause without any reliance on cloud resources.

Conclusion

Anti Virus, EPP and EDR as you know them do not solve the cybersecurity problem for the enterprise. To compensate, some rely on additional services to close the gap. But relying on the cloud increases dwell time. Depending on connectivity is too late in the game, as it takes only seconds for malicious activity to infect an endpoint, do harm, and remove traces of itself. This dependency is what makes the EDR tools of today passive as they rely on operators and services to respond after it's already too late. The technology of TrueContext transforms the EDR to be Active, as it responds in real time, turning dwell time into no time.

ActiveEDR empowers security teams and IT admins to focus on the alerts that matter, reducing the time and cost of bringing context to the complicated and overwhelming amount of data needed with other, passive EDR solutions.

The introduction of ActiveEDR is similar to other technologies that helped humans to be more efficient and save time and money. Like the car replaced the horse and the autonomous vehicle will replace vehicles as we know them today, ActiveEDR is transforming the way enterprises understand endpoint security.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- SentinelOne Ranger (IoT) – Technology Preview
- PowerQuery Brings New Data Analytics Capabilities to Singularity XDR
- Building Blocks For Your XDR Journey, Part 3 | The Value of Securing Identity
- Mobile Threat Defense | Bringing AI-Powered Endpoint Security To Your Mobile Devices
- Rapid Response with XDR One-Click Remediations
- Feature Spotlight | Introducing Singularity Dark Mode