The Simple Truth About Selecting Endpoint Security

BY CHRIS JORDAN

Fluency®

CEO VIEWPOINT

ENDPOINT SECURITY 101

#FLUENCYSECURITY

Chris Jordan

CEO & Co-Founder

For years, the focus has been on the network protecting the endpoint – that is now changing. What should you be considering when selecting endpoint security products?

At Fluency, we strive to make our customers secure. Part of that processes is helping them understand how to implement good security. With more people working remotely from home, it is critical to understand endpoint security. We often say antivirus when talking about securing the endpoint, yet this term is completely outdated and will lead to a bad decision when considering what to buy to protect your endpoint.

There are three acronyms that are important to understand when selecting an endpoint solution:

- Endpoint Protection (EPP)
- Endpoint Detection and Response (EDR)
- Extended Endpoint Detection and Response (XDR)

The base solution is EPP. This is the preventative layer. The recommended solution is EDR, it allows corporate security to provide an extra layer of prevention, but more importantly, it also offers additional analysis and response capabilities. XDR increases the analysis footprint into email and cloud services. A holistic SIEM with strong EDR integration is more effective than a single branded XDR solution.

Endpoint Protection (EPP)

The base capability of endpoint products is prevention. EPP is not antivirus from the '90s. New versions of EPP have a heavy reliance on behavior. But this does not mean that all behavioral systems are equal. Behavior means the algorithm examines secondary attributes, such as the calls from the process, to determine if a process is acting wrong. What attributes are being examined and how a product knows when to prevent actions differ greatly. However, it is clear that companies that leverage behavior analytics are performing better than their predecessors.

Most small businesses make the mistake of buying home EPP. This is a pure cost decision. Home EPP tends to be closer to the signature model with a heavy emphasis on file scanning. This is a small threat from attackers. For example, the growth of file-less malware has grown over the last 10 years and this type of attack is very effective against EPP.

Without central operations that commercial EPP provides, mistakes compound. Common mistakes are lax policies, out-of-date agents, and ignored alerts. A biotech company in Massachusetts had a number of critical systems bricked by ransomware due to out-of-date agents. Small mistakes that users make have large impacts on your company.

While there is commercial EPP, such as Symantec SEP, it pales in comparison to the administrative advantages of EDR. Commercial solutions provide management of the maintenance and central log collection. In short, a company updating or deploying endpoint security should be starting with EDR.

"Commercial solutions provide management of the maintenance and central log collection. In short, a company updating or deploying endpoint security should be starting with EDR."

Endpoint Detection and Response (EDR)

"When EPP fails, it fails completely. EDR, on the other hand, provides a path to mitigate and recover."

EDR is the preferred solution for endpoints. Penetration testers often referred to it as something that has had to make them raise their game. While EPP is focused specifically on files and processes, EDR is focused on behavior of the user. This means while a process analysis may fail detection, an action later by that process might cause detection and, in turn, prevention. Because EDR requires an ability to review, it is usually wrapped in managed detection and response (MDR) services.

Officially EDR differs from EPP in central behavioral analytics, as it performs its analytics in the cloud as opposed to the device. EDR software not only sends back file analysis, agent status, and alerts, but also sends data on changes to the registry, file activity, processes execution, port bindings, DNS caching and HTTP calls. EDR can provide a wealth of raw telemetry data that can be analyzed in the cloud for malicious activity. Buying EDR does not automatically give you access to this data. There is often a second license fee to gain access to this richer data set.

Why is it recommended that EDR be used as the base requirement for endpoint security? First, EDR solutions often include the ability to rollback a machine prior to ransomware. If ransomware is a concern, and it should be, then this is a required capability. Next, EDR provides a combination of timeliness and behavioral analytics. EDR offers superior management, with communications designed for when not on the corporate network – an important aspect of today's remote workforce. Lastly, EDR offers awareness far beyond file analysis.

In regard to ransomware, EDR can roll back to a pre-ransomware state, but it can also identify the Trojan that started the ransomware attack and prevent that too. Before ransomware does its thing, the delivery Trojan will try to spread laterally. This Trojan also needs to be addressed, or the ransomware will spread. Trojans can send back user credentials, meaning that a proper ransomware response needs to also update user credentials that may have been compromised.

From this ransomware example one can see that the complexity of the incident response is not just blocking a file. And this is why EDR is needed. Both the detection and response of EDR differ from EPP. When EPP fails, it fails completely. EDR, on the other hand, provides a path to mitigate and recover.

CEO VIEWPOINT

Extended Endpoint Detection and Response Protection (XDR)

#FluencySecurity

When we look at infrastructure, data and processing logs will exist on endpoints, email services, and web services. An attacker does not need access to an endpoint to cause damage. EDR is limited in its ability to see your entire infrastructure. Extended EDR, called XDR, is the idea that this triad of infrastructure elements can be put under one security tool.

XDR is a marketing term being pushed by Gartner. It is the idea that pulling in email and cloud understanding increases the endpoints solution. I call this a marketing term, for in Gartner's view an XDR solution requires XDR to be under a single brand or partnership. It also doesn't have the means to measure the effectiveness of such integration. In short, the idea of a more holistic view is obviously correct, but Gartner's insight in proper engineering is just as obviously incorrect.

We might use a different term to note tight integration between EDR and system services, such as extended SIEM (X-SIEM). As noted, integration to EDR is not the same as collecting alerts via a Syslog feed or an API call. EDRs have two types of output, alert output, and event output. This second type, which includes telemetry data, is what tight integration is about, and few SIEMs can do this. It is about the ability to leverage this data for detection and response.

XDR products also demonstrate the same pitfall of SIEM to EDR integration when it fails to analyze behavioral data impacting each other. There are no testing use cases that define product ability. And marketed XDR solutions appear to be just a dedicated SIEM by the vendor.

Conclusion

The focus of infrastructure security should be to get EDR pushed out to all endpoints, to include servers. This data is strong by itself, but there is still the need to review cloud service logs and email logs. A complete solution includes these three data aspects for your network. Regardless, EDR is a starting point for infrastructures today.

Chris Jordan is CEO and co-founder of Fluency (www.fluencysecurity.com).