SOLUTION BRIEF

REVERSINGLABS

Enhance EDR Solutions with Context-Rich Malware Intelligence

Enhance EDR Solutions with Context-Rich Malware Intelligence

Challenges

- Lack of file-level visibility on endpoints makes it difficult to find unknown malware
- Dynamic analysis solutions do not analyze all file types, can be slow, and can be evaded by advanced malware
- Malware hunting is a slow and manual process. Hunters work to piece together IOCs and determine the full scope of a threat

RL Benefits

- Instantly analyzes files identified by EDR tools and provides real-time file reputation status
- Exposes malware and provides verified threat classifications to drive the appropriate response actions
- Increases analyst productivity by integrating file reputation and threat context into EDR dashboards and workflows

The lack of file-level visibility into suspicious files with Endpoint Detection and Response (EDR) solutions often inhibits event investigation and response efforts of security teams. Threat vectors like email, web apps, and collaboration tools force organizations to analyze an ever-increasing number of files residing on endpoints in order to defend against attacks effectively. Unfortunately, many EDR products cannot identify embedded malware in complex file structures or new malware variants. And, more often than not, when files are flagged as 'suspicious' by these products, there's not adequate information or the necessary threat details for security analysts to respond effectively. Subsequently, analysts attempt to learn about suspicious files by uploading samples to public reputation services. Not only does this practice expose sensitive information to the public, but the results usually lack actionable intelligence. In addition to reputation lookup services, security teams often leverage dynamic analysis solutions (sandboxes). Still, these cannot scale with large volumes of files and can be easily evaded by advanced malware techniques. Lastly, dynamic analysis solutions face limitations when it comes to file size and file types that can be analyzed. All of this combined leads to significant gaps in an organization's file analysis capabilities and in turn, increased threat exposure.

Solution

ReversingLabs delivers industry-leading malware intelligence that can be easily integrated into existing EDR solutions, enabling organizations to fill in threat detection gaps that could be detrimental to the business. With ReversingLabs, security teams can instantly assess files and get definitive threat classifications from our authoritative file reputation database of more than 40 billion goodware and malware samples. Files are analyzed and classified in milliseconds, including severity level, threat classification, threat name, malware type, and more. Results are displayed in the EDR's user interface with clear and straightforward language, giving much-needed visibility into suspicious files and exposing malware pre-execution. Analysts get all the information they need to prioritize and accelerate their responses to advanced file-based threats across the organization.

And, with tens of billions of samples being continuously processed in ReversingLabs' global threat repository and millions of new samples added daily, analysts can rest assured they're getting the most up-to-date intelligence with the widest coverage in the industry to stay ahead of increasingly sophisticated malware threats.

Use Case 1

Instantly Identify and Prioritize Files by Threat Severity

Challenge:

Security teams are often put in a difficult position when trying to respond quickly and accurately to threats. Too often, the contextual details of why files have been flagged as suspicious are just not available, and high volumes of alerts create even more complexity and stress to overburdened analysts. As a result, response times increase, files get misclassified or missed altogether, and incidents of compromise go up. These risks are due to the lack of information that should be readily available to security analysts and incident response teams.

Solution:

With ReversingLabs' extensible and flexible API, organizations can integrate real-time file reputation data and relevant threat context into their EDR solutions and other security controls. Analysts are immediately armed with clear, easy-to-understand results, including verified threat classifications and severity levels, so they can effectively prioritize and focus on the most critical threats. In short, ReversingLabs enables security teams with the right intelligence at the right time to identify advanced malware and contain threats before they can propagate to the larger network.

Use Case 2

Keep File Reputation Look-Ups Private

Challenge:

Privacy can be a major issue in today's file analysis process. Quite often, when a file is flagged as suspicious by a SOC analyst or EDR administrator, the file is manually uploaded to a public/crowd-sourced file reputation service. The files are then compared against a file reputation database to identify known malware indicators embedded within the file. Unfortunately for the analyst and the business, the file's content is publicly exposed, risking compromise of the business's sensitive data.

Solution:

ReversingLabs' global file reputation service alleviates these concerns with built-in privacy controls, including secure APIs, private file submissions, user-controlled sharing options, and a threat repository that is not publicly accessible. Customers also have the option of an on-premise deployment. With ReversingLabs, organizations get the privacy they need to protect sensitive data, along with the most authoritative and trusted reputation data required to mitigate advanced malware threats.

Use Case 3

Dig Deeper with Pre- and Post-Incident Investigation and Hunting

Challenge:

Advanced, customized malware can adapt to and bypass organizations' security defenses and enter anywhere across global networks, making it extremely challenging for threat hunters and incident responders to defend their environments. Threat hunters need the right context around attacks to proactively search for hidden malware before it leads to a costly breach for the organization. Security analysts and incident responders need clarity, accuracy, and speed with all the relevant threat details to effectively respond and implement the necessary security controls to protect against future attacks.

Solution:

ReversingLabs solves this problem through its robust YARA rule capabilities, including the ability to build and test new rules with ease. YARA rules can be written to match all extracted malware details from files and objects. These rules can be quickly checked for efficacy against ReversingLabs' global data corpus and exported to EDR solutions for proactive threat detection. Using YARA rules also removes reliance on vendor-created malware signatures and increases protection against customized malware. Last but not least, YARA rules enhance the native search and hunt capabilities in EDR products, enabling threat hunters to use these rules for further investigation and advanced searches.

Case Study

A regional bank in the Midwest had a complete security infrastructure, but malware was still infecting their networks through their 20,000 endpoints. The bank implemented the Tanium platform for endpoint visibility and to flag suspicious activity needed to address the problem. Tanium collected all related suspicious files but provided no further information or context for the Tanium administrator to analyze, identify, and contain any advanced malware.

The Tanium platform integrates with third-party file reputation and intelligence services to help detect malicious files. This bank's initial third-party file reputation service displayed results in the Tanium user interface but only provided a thumbs up or thumbs down result. With no further information about severity level or malware type, this service did not help the bank's team prioritize their activities or define effective containment strategies. Additionally, the use of this third-party service caused a privacy issue in cases where the actual files were being uploaded for analysis by members of their security team. This team did not understand that the file reputation service they were using was exposing the content of those files, which became accessible by other customers of the same service.

“We rely on ReversingLabs analysis for threat level, severity, and malware identification. This classification is key to understanding the threat we’re dealing with and deal with it fast by getting data instantly on the profile of the file, so my team knows how to respond.”

SOC Manager, Regional Bank

Solution

ReversingLabs file reputation service and high-fidelity threat intelligence was seamlessly integrated with their Tanium implementation, enriching the bank’s file analysis results with context and actionable intelligence in real-time, including severity level, threat classification, malware type, and more. Plus, ReversingLabs cataloged known good files from trusted sources to ensure that analysts did not waste their time on safe files. Furthermore, ReversingLabs enhanced Tanium’s search results and the information displayed within the Tanium user interface so security operations teams could quickly see analysis results of unknown files. This enabled the bank’s analysts to rapidly determine whether or not a file was malicious and initiate an appropriate response based on the attack type.

Value Realized

The bank used the ReversingLabs and Tanium integration to run automated queries on their 20,000 endpoints every 24 hours to see newly downloaded files. Within seven days, 500 malware samples were found and classified by threat type, threat level, and severity. More than half of the malware samples detected were known by ReversingLabs, but were not detected by the bank's AV scanners. With ReversingLabs’ enriched data results, the bank’s analysts were able to increase their file review speeds by several orders of magnitude. Today, those analysts can quickly identify the highest severity risks and formulate the appropriate responses. They set rules that identify the highest severity level threats and automatically trigger escalated responses. For example, if 40 out of 40 AV products deem a file malicious in a crowd-sourced reputation check, the security team will likely prioritize the incident response playbooks for that file. With ReversingLabs, the results go beyond just reputation by providing rich context and relevant threat details. So, in the aforementioned example of the AV products deeming a file malicious, ReversingLabs goes even further in its designation to identify the file as simple adware (versus a high-level threat like ransomware) so the security team will know to de-prioritize that file in favor of more critical threats.

Conclusion

The ever-increasing number of endpoint devices connecting to enterprise networks has created more entry points for advanced malware to gain a foothold in the organization. To compound the issue, the growing complexity of destructive files and objects makes things even more difficult for SOC teams, especially given that most teams are under-resourced and understaffed. And, while a myriad of security tools are already in place, including detection and response tools, such as EDR, they often lack the speed and comprehensiveness to inspect files at the level required to combat today's evolving malware threats effectively.

ReversingLabs bridges this gap with industry-leading file reputation services and malware intelligence that provides the next-level coverage, accuracy, context, and performance security teams need to identify and contain advanced malware, as well as find destructive files and objects hidden within their endpoints and network in the fastest times possible.

About ReversingLabs

ReversingLabs is the trusted name in file and software security. We provide the modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, the ReversingLabs Spectra Core powers the software supply chain and file security insights, tracking over 40 billion searchable files daily with the ability to deconstruct full software binaries in seconds to minutes. Only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk to your organization and your customers.

Get Started!

We'll Show You How ReversingLabs
Detects and Analyzes More Hidden Threats

REQUEST A DEMO

reversinglabs.com

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com