RansomStop

Introducing RansomStop

Introduction

Ransomware has become an increasingly impactful risk for organizations around the world, with no signs of letting up. With extortion costs, remediation costs, reputation loss, regulatory requirements and operational downtime, ransomware has made itself a topic of discussion even in board rooms. RansomStop is designed to protect organizations specifically from these types of attacks.

Typical Ransomware Defense

Most companies deploy endpoint security products such as Anti-Virus (AV) and/or Endpoint Detection and Response (EDR) tools to prevent ransomware and use data backup solutions for the ability to restore data in case of emergency. As these tools have evolved to be better, attackers have evolved as well to find new ways to evade endpoint protection products. What this means is that, inevitably, attackers will get into your organization and deploy ransomware. At that point, organizations move into the containment and eradication phases, before recovery is possible. During these 3 phases, there is often an impact on business operations, hurting delivery of goods or services, revenue generation and reputational impact.

Why Ransomware Is So Hard To Prevent

Attackers and defenders are always playing a game of cat and mouse. As AV and EDR get better, attackers shift tactics to evade them. An oft-used phrase in cybersecurity, attackers only have to get it right once, defenders have to get it right every time. Some of the more recent evasions have included remote encryption, browser-based ransomware, living off the land

RansomStop

(LOTL) attacks, and EDR Killers. This has to do with the nature of endpoint security tools, which require the ability to see ransomware execute to prevent it.

In a broad survey by Sophos (1), 59% of respondents had ransomware attacks in the last year, with 70% of those attacks successfully encrypting data. In addition, 57% of those attacks included successfully compromising backups. You can see how an attack like this can spiral out of control very quickly and why they are so hard to prevent and expensive and time consuming to recover from.

Introducing RansomStop

RansomStop takes a different approach to ransomware prevention by monitoring data for malicious interactions. This is nearly impossible to evade since your data either gets encrypted or it doesn't, regardless of what or where the attack is coming from. RansomStop looks at file formats, contents, names, as well as access patterns by users to detect if there is ransomware activity. Once RansomStop detects malicious activity, it immediately takes automated steps to disrupt the attack, contain the ransomware and prevent further damages. The compromised user account is suspended, the IP address of the attacker is blocked, and any malicious processes are stopped. The automated response happens in seconds and effectively stops the attack in its tracks, protecting your organization's ability to operate.

RansomStop is specifically designed to protect against ransomware attacks that endpoint security products struggle with stopping. This includes remote encryption and living off the land attacks, as well as cloud and SaaS-based storage.

RansomStop is designed to be a set it and forget it solution. Installation takes just a few minutes per storage location. It does not require cybersecurity experience to configure or maintain and responds to attacks automatically in seconds without human intervention. Ransomware doesn't sleep and neither does RansomStop.

Deployment

With endpoint products, you need to ensure continuously that all your endpoints have your endpoint security product installed, and that it is up to date, operating and configured correctly. This can be a resource intensive task for your cybersecurity and IT teams. Any failure in this process can open up attack surfaces for ransomware groups. This is made even harder by the proliferation of unmanaged devices (e.g. personal devices accessing corporate systems), shadow IT, remote workers, etc.

RansomStop

Use Cases

Since RansomStop is designed to protect business critical data stores, the footprint is much more targeted. Users will generally deploy RansomStop on data that is important to business functions, like an accounting server, order processing application, manufacturing application, as well as high risk servers, like a Windows server with inbound Internet services.
Here are some examples of where to deploy RansomStop:

- File Servers
- SQL servers
- Application servers
- SharePoint servers
- Web servers
- Cloud Object Storage used by business applications
- NAS appliances
- Hypervisors

Architecture

RansomStop uses one or more containerized “analyzers”, which take event feeds from servers and appliances, or use APIs to monitor cloud and SaaS-based storage like Google Drive.

- For Windows servers, there is a lightweight agent that simply forwards Windows event logs to your on-prem analyzer and awaits response instructions in case of attack. The lightweight agent is designed purely to export file events, so it is very efficient and won’t interfere with other endpoint agents.
- For NAS appliances like Synology, the built-in syslog service forwards file events to the analyzer and a responder service.
- For cloud or Saas-based resources, the analyzer container runs in your cloud environment and uses native APIs to monitor file access and changes. This provides no-overhead, agentless protection for your cloud and SaaS-based storage.

The analyzers can be deployed on-prem or in your own cloud, meaning that your data never leaves your control, and is not copied or accessible externally.

Policy and Alert management is through a SaaS Admin Portal making configuration and management easy. Alerts can be viewed in the Admin Portal and can also be forwarded to your SIEM, SOAR or managed service provider for visibility.

Conclusion

Most organizations think they are prepared for a ransomware attack, but when it happens, they find out the hard way that there are too many gaps in the standard security toolkit to effectively prevent ransomware attacks. RansomStop is the solution to cover those gaps so that the next ransomware attack doesn’t become one of the worst days of your career.

RansomStop

References

1. The State of Ransomware 2024, Sophos

Terminology

AV: Anti-virus. Endpoint security tool to detect and stop malware from executing.
EDR: Endpoint Detection and Response. An Endpoint security tool that provides detection and response capabilities, above and beyond AV. Typically, this replaces AV on an endpoint.
LOTL: Living Off The Land Attacks. This is where attackers use legitimate system tools to accomplish or enable an attack. Since they are valid tools, they are used to evade endpoint security products.
XDR: Extended Detection and Response.
SIEM: Security Information and Event management.

RansomStop

www.ransomstop.com