FORTRA™

SOLUTION BRIEF (TRIPWIRE)

Stay Ahead of Ransomware with Tripwire Enterprise

Best Practices for Ransomware Prevention and Detection

The global impacts of ransomware have only intensified in the opening years of the 2020s. Verizon's *2021 Data Breach Investigations Report* found that ransomware is now present in 10 percent of all breaches as it continues to gain in popularity among cybercriminals.

Fortra's Tripwire® Enterprise helps protect against ransomware attacks by enabling you to identify and correct weakened security configurations that are often the entry point of a ransomware attack. It can then continuously monitor for suspicious changes and alert you real-time to the file encryptions and deletions that are at the heart of a ransomware attack.

You can also configure Tripwire Enterprise custom policies to search for specific indicators of compromise associated with a particular attack type, which enables you to identify, isolate, and restore compromised systems before the ransomware is activated.

CUSTOM POLICIES FOR KNOWN RANSOMWARE VARIANTS

Once a known type of ransomware is identified, you can configure a custom policy in Tripwire Enterprise to look for specific indicators of compromise associated with that particular attack type. For example, you can use it to detect specific registry keys and files that match SHA-256 file signatures known to be used in the WannaCry attack.

How Tripwire Enterprise Protects Against Ransomware

Tripwire Enterprise protects organizations from ransomware using two fundamental security controls: file integrity monitoring (FIM) and security configuration management (SCM).

File Integrity Monitoring

Every change can potentially lead to a breach. To detect the security gaps that could allow a ransomware attack to invade your systems, you first need to detect the configuration changes on a system and assess if they are valid and secure ones that adhere to your change control processes, or if they are potentially unsafe. File integrity monitoring is the security control that monitors and detects changes in your environment to alert you to all changes—including possible cybersecurity threats—and provides you with needed data to remediate the unwanted changes.

Tripwire Enterprise uses FIM to monitor the critical binaries, libraries, and configuration files for the operation system on a server. It can also be used to monitor the applications and other business-critical data present on that server. The Tripwire Customer Center includes Critical Change Audit (CCA) rules to give you a starting place for what needs to be monitored on an OS. Your internal stakeholders should also be consulted in order to identify business critical applications and data that also needs to be monitored.

Once FIM is up and running, a recommend next step is to use industry best practices for change controls on servers. This includes change request time windows, approval processes, and additional verification of intended versus actual changes (another area where FIM data collection can increase the thoroughness and efficiency of a process). Using a change window makes it easier to view monitored changes in Tripwire Enterprise and validate if they are likely-good or likely-bad just from the timing, in addition to the other forensic data available.

Email actions or syslog messages can be set up to alert appropriate teams for prompt review after detection using a scheduled scan or the agent's real-time monitoring (to reduce lag time between detection and response). Additionally, Tripwire Enterprise agents can browse the local file system of a monitored machine to make creating custom rules much easier once business critical applications and data have been identified.

> *"Our Tripwire admin was able to create a report to locate elements and identify servers in the environment that had files tied to the SolarWinds vulnerability. Tripwire has also created custom 'Indicator of Threat Compromise' rules that look for common hashes associated with Sunburst and SolarWinds."*
>
> —**Tripwire Customer**, 2021

Tripwire Enterprise can be configured to capture several different types of file hashes for all of the files it monitors. After a threat is identified in the wild, Tripwire Enterprise hash data can be used to validate if any monitored systems are infected by comparing the known bad file hashes found online to the data from your own systems.

Tripwire Enterprise also identifies ransomware attacks by detecting changes to files on the endpoints, in real-time, as a result of the malware encrypting the file systems. The malware will generally create a new, encrypted file and delete the original one. Tripwire Enterprise sees these file modifications or additions/removals, and therefore aids in the identification of the files affected by the ransomware. Setting up the aforementioned alerts will also reduce time-to-detection and recovery efforts by enabling you to quickly respond before a threat has a chance to take hold over a larger portion of your environment.

Security Configuration Management

SCM is the process of ensuring that system configurations meet security and compliance standards. SCM allows you to harden your systems from attack by identifying weak security configurations, which leaves fewer footholds for ransomware to successfully deploy. It protects servers as well as the software running on them.

Tripwire Enterprise supports dozens of security frameworks and standards, including PCI DSS, NERC CIP, the MITRE ATT&CK framework, and the CIS Controls, in addition to custom compliance standards created by your organization. The Tripwire Customer Center provides these policy frameworks for free download and easy import into your Tripwire Enterprise console.

Tripwire Enterprise's detection of a policy compliance failure can serve as an early warning sign that server or application configurations are being tampered with—often in the early stage of a ransomware attack. Tripwire Enterprise then helps you correct the problem through remediation advice and automated remediation scripts.

Tripwire Integrations

Available Tripwire Enterprise integrations include those that help parse authorized from unauthorized changes in real-time, further speeding up ransomware detection capabilities.

Tripwire Enterprise Integration Framework

Integrate your Tripwire Enterprise with your change management software (ServiceNow, Remedy, Cherwell, etc.) to easily approve known valid changes—and even create incident tickets for unknown changes to be researched by your teams.

Tripwire Dynamic Software Reconciliation

Tripwire Dynamic Software Reconciliation compares the detected file changes and software installations on your machines with the file manifests direct from Microsoft, Red Hat, and other sources to validate detected changes in your environment.

Tripwire Event Sender

For more customized syslog messages in a CEF format (ideal for Splunk), Tripwire Event Sender can turn a large volume of syslog events into a more concentrated set of actionable log messages, which enables your teams to spend more time focusing on business needs and less time researching incoming data.

Third-party Integrations

Tripwire also integrates with the third-party software you use throughout the organization, such as ticketing solutions, service management tools, and security information and event management (SIEM) software. These integrations can also reduce ransomware time-to-detection, giving you more time to gain control before cybercriminals are able to execute their attacks.

Summary

Once ransomware has a hold on your systems, it's often too late to undo the damage. That's why putting your focus on the prevention and rapid detection of ransomware is the key to shrinking your attack surface so that attackers are unable to gain entry in the first place. Tripwire Enterprise conducts continuous monitoring using SCM and FIM security controls to keep systems hardened against attacks and to quickly identify indicators of ransomware compromise before significant damage can occur.

> *"These [ransomware] attacks have some variety in terms of how the ransomware gets on the system, with actors having strong preferences that can be broken into several vectors. The first vector is through the use of stolen credentials or brute force. We've seen 60 percent of the ransomware cases involving direct install or installation through desktop sharing apps. The rest of the vectors that we saw were split between email, network propagation, and downloaded by other malware, which isn't surprising as we found in our web proxy detections dataset that 7.8 percent of organizations attempted to download at least one piece of known ransomware last year."*
>
> **—2021 Data Breach Investigations Report**

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.