Forcepoint

Solution Brief

Forcepoint's Zero Trust Content Disarm & Reconstruction Tool in Insider Risk Environments

Challenge

- To gather context and safely view documents such as email attachments and file transfers, which may contain malware.

Solution

- Forcepoint's Zero Trust Content Disarm & Reconstruction (Zero Trust CDR) capabilities works by extracting the valid data, verifying the information and then building brand-new data. Delivering pixel perfect, fully revisable, malware-free files in real time, with no delays for scanning or sandboxing.

Outcome

- Reduced UAM analyst downtime caused by exposure to hidden malware, zero-day threats, etc.
- Analysts can safely gather context and open files without creating additional risk.
- Mitigates risks inherent to collecting a wide variety of files from unknown origins.

A cohesive team thrives with the right tools to do the job

Insider risk teams are typically small, specialized teams of analysts and investigators. The impact of a team member experiencing prolonged downtime is large – as network or data security colleagues are not able to shift over and assist. Its key to provide the best tools to extend protection and uptime to these environments to ensure consistent operations.

Unprecedented ability to detect Insider Risk activity

Forcepoint's User Activity Monitoring (UAM) tools provide an unprecedented ability to detect indicators of Insider Risk activity as well as support analysis and investigation of possible Insider Risk actors. This is achieved through the collection of a wide-variety of files across web, email, file shares, and more. With access to these channels comes inherent risk in collecting and viewing files that may have come from untrusted sources.

For example, an analyst may support an investigation into a person of interest (POI) whom authorities believe is surreptitiously communicating with a member of a foreign government. This analyst uses UAM tools to collect all emails, both corporate and web based, that the POI receives from high-threat and trusted networks and all documents downloaded from these networks including various file sharing websites. Unbeknownst to the analyst, one of the MS Office files collected contains zero-day malware that was not detected by the corporate anti-malware systems.

As the analyst views or downloads files collected in conjunction with the investigation, the analyst unwittingly detonates the malware contained in the file. The malware spreads to many computers and servers across the enterprise before the corporate cybersecurity service personnel and/or deployed cybersecurity tools detect the issue.

As a result, many of the analyst computers, servers, and data repositories must be reimaged to ensure the malware is completely eradicated. The outcome from such an event will require additional resources and associated time to recover from the effects of the malware along with system and analytical downtime to ensure no further impact to time sensitive investigations.

Figure 1 below is an implementation without Zero Trust CDR that relies solely on traditional anti-malware detection and firewalls to reduce the risk of malware spreading inside and outside the analyst enclave.

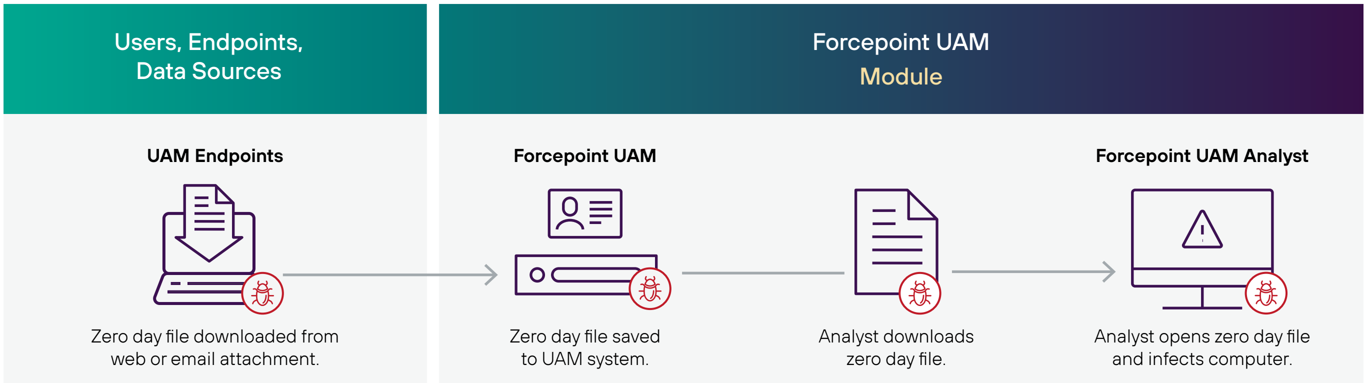

Figure 1 – WITHOUT Zero Trust CDR: Utilize traditional Anti-malware Detection and Firewalls to create a FENCE to isolate the analyst network.

Malware detection is dead. Prevention is key to combating malware and ransomware.

Forcepoint's Zero Trust CDR Solution:

Forcepoint Zero Trust CDR protects networks and users from malicious content. Rather than trying to detect malware, it assumes nothing can be trusted. It works by extracting the valid business information from files (either discarding or storing the originals), verifying the extracted information is well-structured, and then building new, fully functional files to carry the information to its destination. Zero Trust CDR is a game-changer for mitigating against the threat of even the most advanced zero-day attacks and exploits.

To mitigate the potential exposure in the example above, Zero Trust CDR is integrated into FP UAM tools allowing files to automatically passed from the UAM system through the Zero Trust CDR transformation process for analysts to view with no need for analyst interactions other than opening the clean and safe file. The UAM system does this while preserving the original document within the system of record for possible future forensic or investigative needs. Zero Trust CDR is simply giving the analysts content that is safe to view while maintaining integrity of the records.

How Zero Trust CDR Works

Hand us a piece of data – a document or an image –from an untrusted source. We transform it, extracting only the useful business information from it. We discard the original and hand a brand new one back to you!

Nothing travels end-to-end through this process but safe data. Figure 2 shows how documents are transformed in seconds. The result is pixel perfect, fully revisable data, but without the threats.

A unique process ensures NO threats in the content

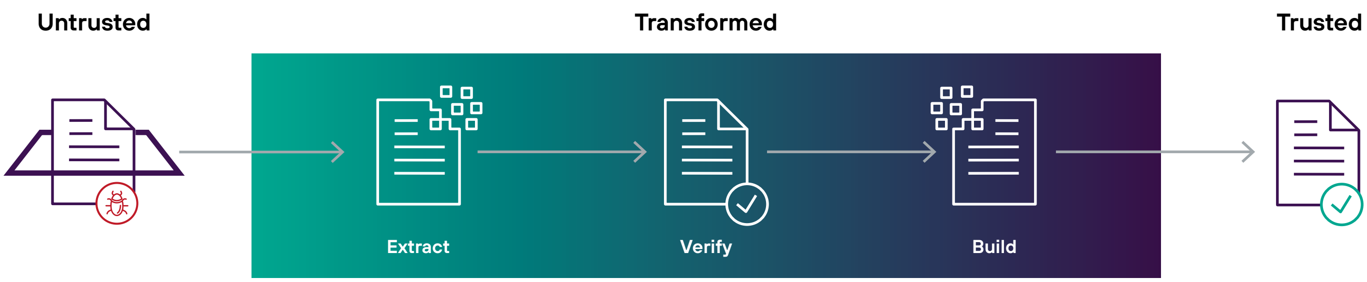

Figure 2: Zero Trust CDR

In Figure 3 Zero Trust CDR is implemented to further reduce the risk of malware entering the enclave from a high-threat external network by ensuring analysts receive clean and sanitized files.

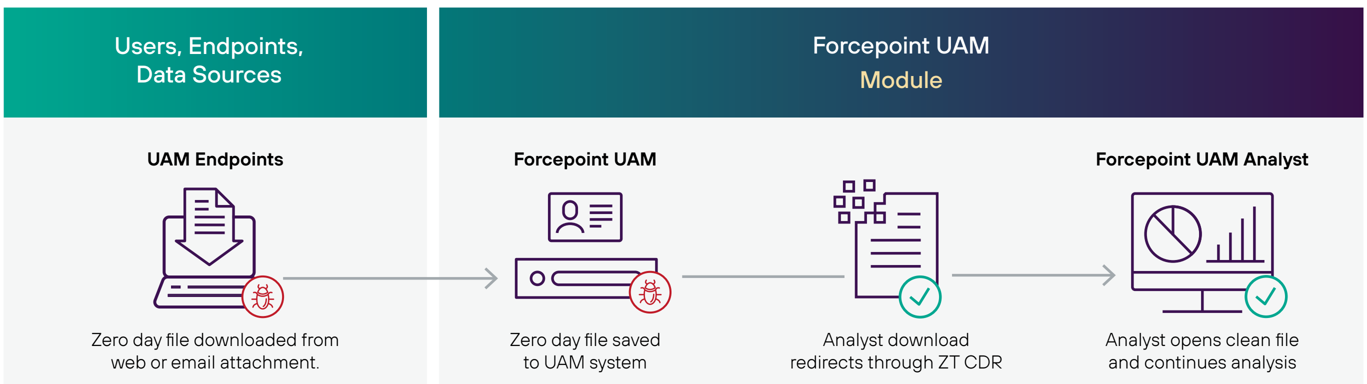

Figure 3 – WITH Zero Trust CDR: The risk of malware entering the enclave from a high-threat external network is further reduced.

Summary

Rather than trying to detect malware, Forcepoint Zero Trust CDR works by extracting the valid data, verifying the information, and then building brand-new data file. As analysts investigate and gather context, they will access only clean file content, avoiding malware and analyst downtime.

Forcepoint is the only company that offers both reconstructed clean data files free of executable code, and the market leader in insider risk investigation capabilities. Offering innovation in Detection, Collection, and Insight for investigation capabilities, we make the tools that enable your teams to remove risk from the equation.

forcepoint.com/contact

[FP-Zero Trust CDR Tool in Insider Risk Environments-Solution-Brief] 16Aug2022