SOLUTION BRIEF

RANSOMWARE MITIGATION

Ransomware has become progressively more advanced. Criminals are moving beyond simple system exploits to using APT-like tactics and techniques to conduct reconnaissance, escalate privileges, and move laterally to find high-value targets, such as production databases, Active Directory controllers, and other critical assets. By encrypting these essential services and waiting until they have a widespread presence in the network, the threat actors can demand higher amounts, and organizations are forced in many cases to pay or suffer extensive recovery efforts and costs. The Ransomware Weather Report recorded 14% more ransomware attacks in the first half of 2021 than in the second half of 2020. Organizations must take a different approach to thwart these more aggressive and destructive attackers. The Attivo Networks Endpoint Detection Net (EDN) suite's ransomware mitigation functions arm security teams with the defense they need to detect and derail both common and advanced ransomware attacks quickly.

RANSOMWARE ATTACKS

Typical ransomware spreads through several methods, most often through malicious emails, removable storage drives, or infected links. The ransomware infects the host and then looks for documents, spreadsheets, pictures, or other files and data to encrypt. Once it finishes encrypting the local files and folders, it will often look for network shares mapped to the endpoint and encrypt any files it can access, thus affecting a more significant number of people. It may also look for attached storage devices like USB flash drives to infect as another propagation method. Once it completes this activity, it will flash a ransom message on the screen with contact information and the amount the attacker demands for the unlock code.

Organizations use Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) solutions to detect less-sophisticated ransomware variants and prevent them from infecting endpoints. These endpoint solutions use signature matching or behavioral anomaly detection, identify malicious binaries, and then block their execution to stop the infection. With known malware samples or a good baseline, these systems can effectively prevent endpoint compromise.

> 70% of complex malware attack types are of the ransomware variety.
> - Verizon DBIR 2021

However, advanced, human-controlled ransomware can bypass these security controls. These threat actors often do not infect the first system they compromise. Instead, they use it as a foothold in the network to launch their attacks, conduct network discovery, probe Active Directory, move laterally to spread around to multiple systems, and identify high-value assets to target. At this stage of their attack, they stay hidden from view, unlike commodity ransomware

that encrypts any host it infects and then shows the ransom screen when it finishes encrypting files. Only when the attackers have found all the organization's essential assets and encrypted the critical data will they send their ransom demands. They may even threaten to disclose some stolen private data to discourage non-payment. To combat these advanced attackers, organizations are turning to the Attivo Networks EDN solution.

THE EDN SOLUTION

The Attivo Networks EDN solution, part of the ThreatDefend® platform, includes the ThreatStrike® solution for endpoint deception, the ThreatPath® solution for attack path visibility, and the ADSecure solution for Active Directory defense. Together, they augment existing endpoint defenses, like EPP and EDR, by detecting attacker tactics and techniques to move deeper into the network. Moreover, the solution misdirects, misinforms, and denies attackers unrestricted lateral movement from the initially infected system. The EDN suite packages these solutions under one license and comes as a standalone detection solution with the EDN Manager or as part of the ThreatDefend platform, which adds attacker engagement and network reconnaissance detection when used with the BOTsink® deception server decoys.

ANTI-RANSOMWARE SECURITY FEATURES AND MODULES

The Anti-Ransomware security feature comes with the EDN license, designed to monitor anomalous behavior and detect malicious activity in real-time. Attackers today use advanced evasion techniques like using live off the land tools, loading malware from VMs, and running in memory to bypass endpoint defenses. Some of the recent and more devastating attacks like Ryuk, WastedLocker, Revil, and other ransomware used targeted attack techniques and worm-like capabilities to move laterally to other systems. Defenders must stop attackers early in the attack, from delivery to hard-to-detect lateral movement, without impacting business. To stay ahead of fast-moving threats, they need behavior-based security that shuts down unknown threats before they can cause harm. The inline analysis stops exploits that lead to infection. Meanwhile, the always-up-to-date machine learning models monitor behavior, stopping unknown and zero-day threats pre-emptively, including ransomware.
The Anti-Ransomware feature consists of the following three modules.

KEY CAPABILITIES

Learn Ransomware Behaviors
Encryption of files, folders, decoys documents, change in entropy, deletion of files, security product termination, deletion of shadow volumes, etc.

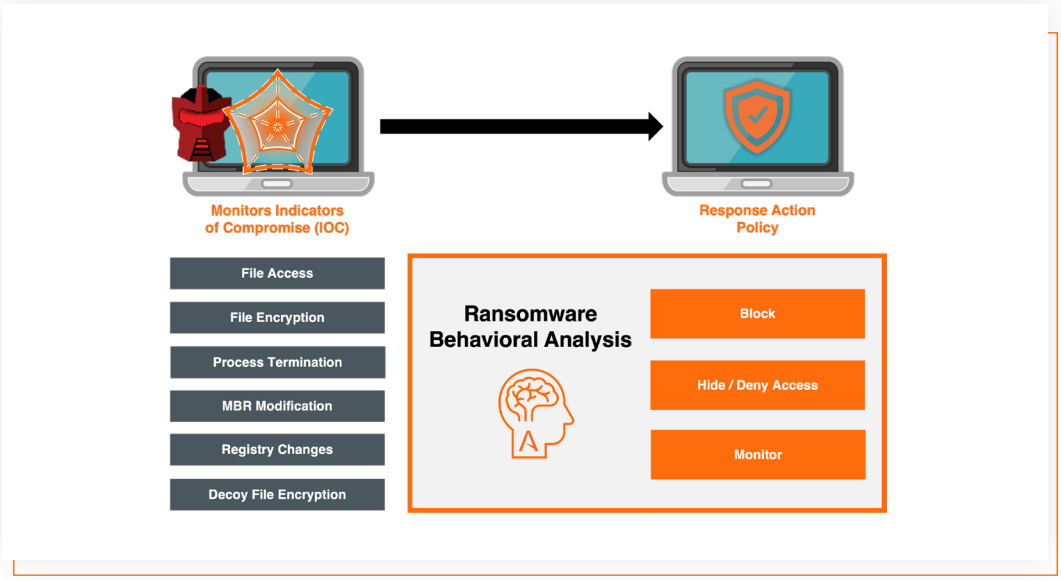
Scoring-Based Mitigation
Once the ransomware meets certain thresholds, mitigate it by blocking all IO operations and terminating the process.

Forensic Reporting
Generates alerts with context data from the endpoint based on Aggressive, Moderate, or Conservative behavioral detection.

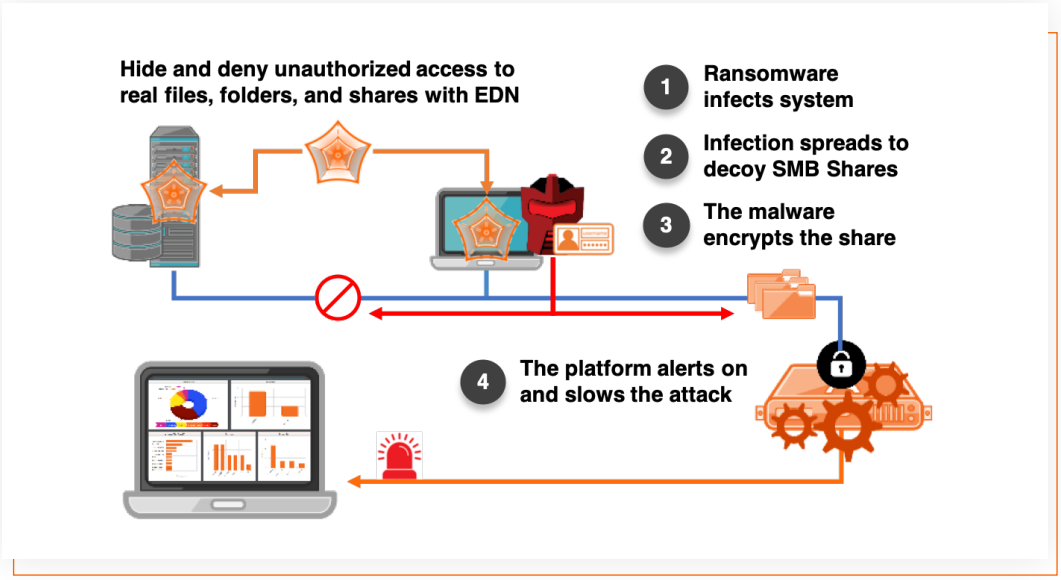
1. The DataCloak function prevents ransomware from accessing critical data. The function hides and denies attackers access to local files, folders, removable storage, network or cloud shares, local administrator accounts, and application credentials.

2. Behavior Detection leverages Machine Learning for ransomware detection by identifying and tracking suspicious behaviors.

3. Volume backup of endpoint applications and data provides options to take continuous backup of changes on the endpoint using native Microsoft tools. It prevents ransomware from deleting backup files created using Windows Volume Shadow Copy Service (VSS).



Attivo ransomware behavioral detection, prevention, and response.



Prevent ransomware from accessing production data, then high-interaction deception stalls the attack by feeding it unlimited fake data.

In a standalone EDN deployment, the EDN Manager generates alerts for every activity attempting to enumerate the local files and folders or access mapped shares. Alternatively, when used with the BOTsink server, these mapped file shares lead to network decoy servers populated with fake data. As the ransomware encrypts the files on the phony file shares, the decoys keep feeding the malware a never-ending stream of data to stall and occupy it, delaying the attack while alerting security teams. Additionally, both the EDN Manager and the BOTsink solution have native integrations with existing security solutions that can automatically isolate infected systems to give security teams time to remediate incidents and prevent the further spread of infection.

CONCLUSION

The EDN family of products is a powerful solution for preventing both standard and human-controlled ransomware attacks. Whether the adversary is stealing credentials, pulling critical accounts and information from AD, moving laterally, or activating the ransomware to encrypt files, the EDN solution quickly detects and derails these activities. The solution's flexibility allows security teams to deploy it either in standalone mode for detecting attacks or as part of a broader ThreatDefend platform deception fabric. The full platform adds forensic collection, attack analysis, threat intelligence development, native integrations, and the ability to feed the ransomware with unlimited data to stall the attack. By adding the EDN suite to existing EPP and EDR solutions, organizations can strengthen their endpoint ransomware defenses and deny attackers from getting both a foothold into the network and the opportunity to disrupt services.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in preventing identity privilege escalation and detecting lateral movement attacks, delivers a superior defense for countering threat activity. ThreatDefend® Platform customers gain unprecedented visibility to risks, attack surface reduction, and speed up attack detection. Patented innovative defenses cover critical points of attack, including at endpoints, in Active Directory (AD), in the cloud, and across the entire network. Concealment technology hides critical AD objects, data, and credentials. Bait and misdirection efficiently steer attackers away from production assets, and deception decoys derail lateral movement activities. Attivo has won over 150 awards for its technology innovation and leadership. www.attivonetworks.com