NOVEMBER 2021

THREAT USE CASE

ARMOR'S DEFENSE AGAINST RANSOMWARE

INTRODUCTION

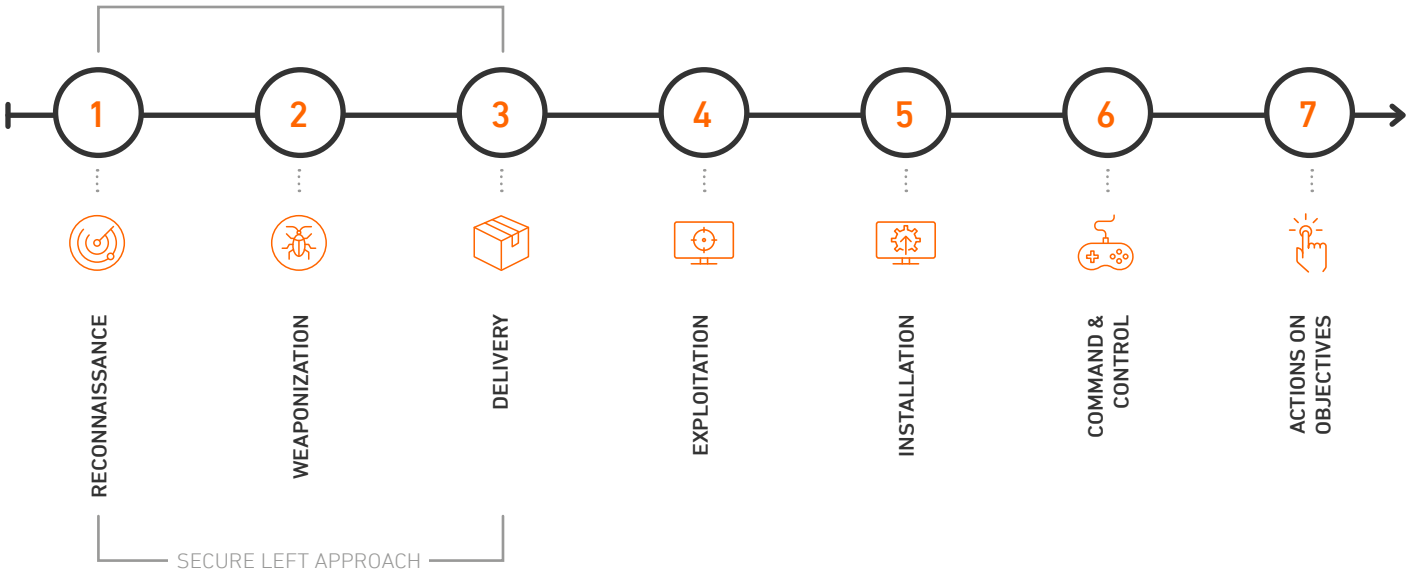
Ransomware is a destructive malware that uses encryption to seize a victim's servers, applications, communications systems, and data. The aim is primarily to extort money for the return of encrypted data or access to frozen networks or applications.

While this malware class isn't new, threat actors continue to develop a variety of destructive new applications and techniques. In a 2020 study, 51% of organizations indicated they were impacted by ransomware in the past year. Healthcare organizations, municipalities, and schools have all been victims.

Ransomware attacks vary by type and delivery method, but they primarily expose themselves at the last stage of the kill chain: actions on objectives. **The key to stopping ransomware lies in a layered "secure left" approach to cybersecurity in which threats are identified and eliminated early, before bad actors are able to carry out malicious actions against their target.** To effectively mitigate the impact of ransomware, organizations must protect both data integrity, assuring the accuracy and consistency of data over time, and data availability, assuring data is accessible when and where it is needed.

OF ORGANIZATIONS ARE FFECTED BY RANSOMWARE ATTACKS.

KILL CHAIN



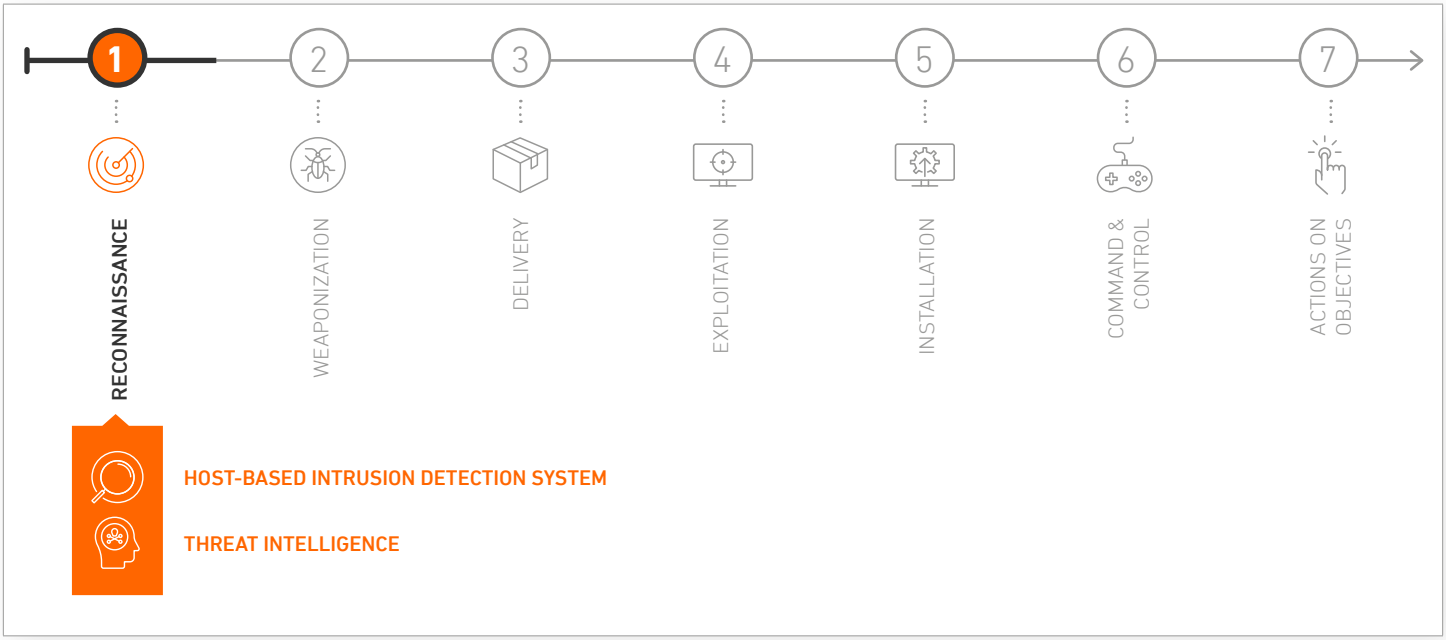
HOW ARMOR DETECTS & RESPONDS TO RANSOMWARE

Armor's industry-leading threat detection and response platform ingests logs from the Armor Anywhere agent, cloud-native sources, and third-party tools. It then correlates and analyzes those log events along with threat intelligence from Armor and other third parties. The output is used to protect against discovered threats, bolster an organization's detection capabilities, and provide response in the event of an incident.

Armor continuously monitors your customer environments for known malicious signatures that can signal a ransomware attack at the earliest stage of the kill chain.

Armor provides security controls that detect and respond to cyberattacks at various stages of the kill chain. As part of a layered approach to cybersecurity, Armor provides:

- File Integrity Monitoring (FIM)
- Vulnerability Scanning
- Endpoint Protection (Antivirus/Antimalware)
- Threat Intelligence



If an attack progresses to the **exploitation phase** of the kill chain, changes to the integrity of operating system and application software files can be detected by our **file integrity monitoring (FIM)**, as they are checked against a baseline state. FIM looks for changes to critical OS files and processes such as directories, registry keys, and values. It also watches for changes to application files, rogue applications running on the host, and unusual process and port activity, as well as system incompatibilities.

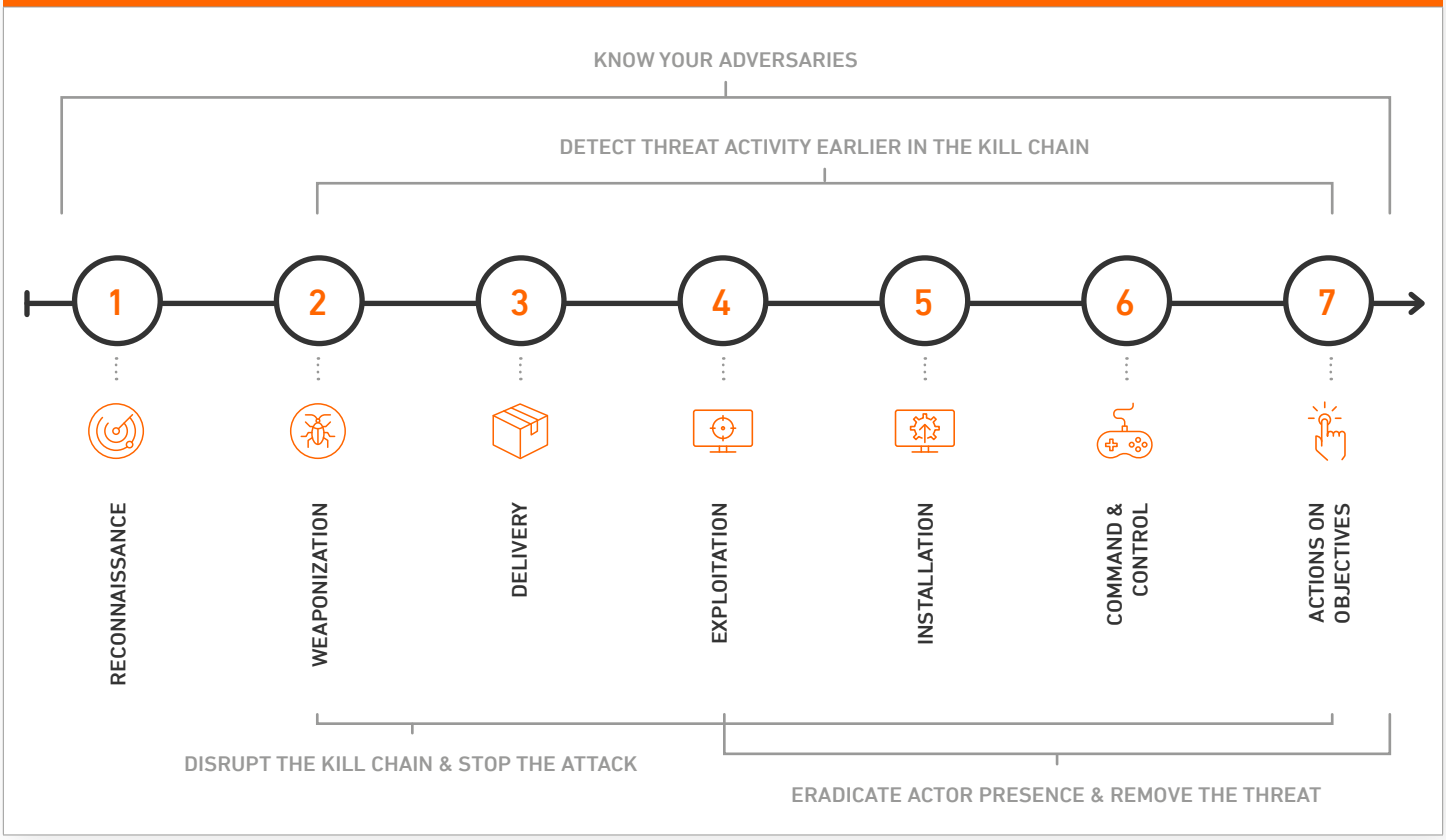
Vulnerability scanning can further identify potential paths and weaknesses to exploitable programs or scripts.

Our **Threat Resistance Unit (TRU)** actively analyzes critical threats to your customers' environments and responds to the most challenging issues. They monitor new threats as they evolve, which are collected from experiences with customers, a variety of the cybersecurity industry's most trusted threat intelligence sources, and other research such as reverse-engineering malware and dark web research. Through our TRU, Armor can identify the latest threats before they are widely known and patched by software vendors.

Ransomware attacks such as those on municipalities or school districts are not always designed to target and encrypt workstations. More sophisticated ransomware threat actors go after the valuable servers within an organization's environment and may often target backups.

When threat actors initially get a foothold within an organization by compromising a corporate workstation (often via a malicious email link or attachment), many are not always trying to inject ransomware onto a single workstation. They are instead looking for infrastructure containing critical data and applications, ones with heavy workloads that, if interrupted, could be devastating. Once cybercriminals find those servers, they will attempt to deliver their payload and, if successful, proceed to deploy ransomware onto the target servers.

BREAKING THE KILL CHAIN



Depending on what stage of the kill chain Armor Anywhere interrupts an attack, our logs would not necessarily indicate that we are blocking ransomware. For example, if we block the attack at the point a threat actor is trying to install a trojan or downloader, then that is all our logs would show. It would not tell us, "by the way, the next stage of the attack, after the downloader is installed, is a family of ransomware."

But by stopping threats further left in the kill chain, and continuously monitoring your environment through automation, Armor Anywhere can greatly reduce the chances ransomware will infect your customers' applications and data. Combined with a comprehensive and ever-changing security posture, one that aims to "secure left" throughout the kill chain, Armor's security controls can help MSPs combat the growing scourge of ransomware.

CONSIDER OFFERING THESE SERVICES TO FURTHER PROTECT YOUR CUSTOMERS FROM RANSOMWARE

PATCHING

Your customers must continuously patch against vulnerabilities, both known and unknown. Minimizing the potential attack surface is critical.

DATA SEGMENTATION

Not all data is critical for business continuity, nor should all data be accessible to everyone. Least privilege access is key to securing critical data.

OFFLINE DATA BACKUPS

Your customers must have multiple backups of their critical data, applications, and application platforms. These backups must be air-gapped from the internet, password-protected, and tested. Best practices include the rule of 3/2/1 (3 copies, 2 storage media, 1 offsite).

WHITE LISTING SOLUTION

Limit the use of applications and processes that are allowed to run in your customers' environment by providing a short list of approved applications and processes. Similar to a VIP list for PC, if it's not on the list, it's not allowed.

OFFER LEAST PRIVILEGE ACCESS CONTROL

Ensure your customers have the least privilege for their job. This also applies to services.

AUDIT/PENETRATION TESTING FROM INDEPENDENT, THIRD-PARTY EXPERTS

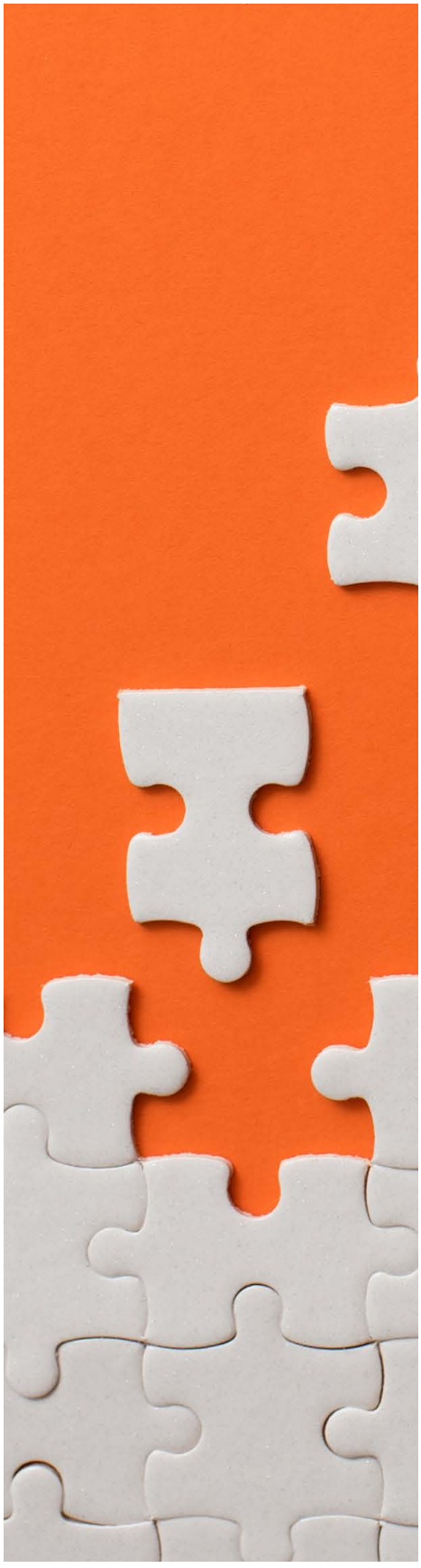
Ensure that your customers are implementing security best practices by outsourcing their audit/penetration testing needs.

CONTINUOUS SECURITY AWARENESS TRAINING

Educate your customers' employees about current and emerging cybersecurity risks and phishing emails. Effective training should actively engage employees and include policies concerning the correct response to suspected phishing attempts.

ARMOR ANYWHERE

Armor Anywhere is a turnkey, enterprise-grade cybersecurity platform purpose-built for managed service providers (MSPs). It helps detect and respond to malicious threats across endpoint, network, server, and cloud environments. MSPs also use the platform to help streamline compliance for their customers. In the event of an attack, our cybersecurity experts are available 24/7/365 to help you respond quickly and effectively.



ABOUT ARMOR

Armor is a global cloud security company. We make cloud security and compliance simple, achievable, and manageable for managed service providers (MSPs) and their customers.

Armor safeguards endpoint, network, server, and cloud environments against malicious threats seeking to infiltrate and disrupt businesses, while providing unparalleled insight into security risks your customers may face. In the event of an attack, our cybersecurity experts are available 24/7/365 to help you respond quickly and effectively.

MSPs who use Armor benefit from an enterprise-grade security platform, cybersecurity expertise, and business growth resources to help you quickly scale your cybersecurity practice.

Armor is all about keeping your customers safe and helping you grow your business. We know security and compliance are complex, but it doesn't have to feel that way.

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167