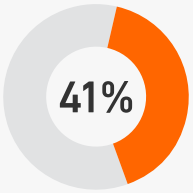
THREAT USE CASE

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.

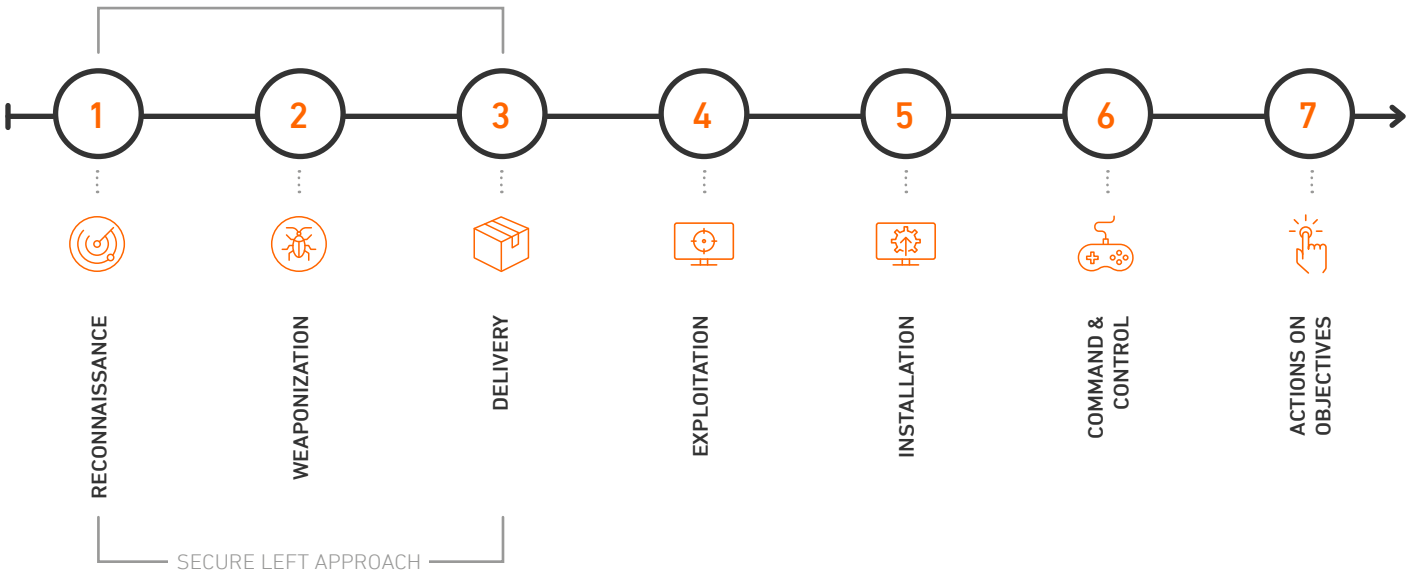
While this malware class isn't new, the number of U.S. infections increased 41% in 2019 with threat actors developing a variety of destructive new applications and techniques. Healthcare organizations, municipalities, and schools have all been victims, along with Managed Service Providers (MSPs) that have sometimes infected hundreds of individual end users.



RANSOMWARE INCREASES BY 41% IN 2019.

Ransomware attacks vary by type and delivery method, but they primarily expose themselves at the last stage of the Cyber Kill Chain: actions on objective. **The key to stopping ransomware lies in a layered "secure left" approach to cybersecurity in which threats are identified and eliminated early, before they are able to carry out malicious actions against their target.** To effectively stop 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.

CYBER KILL CHAIN



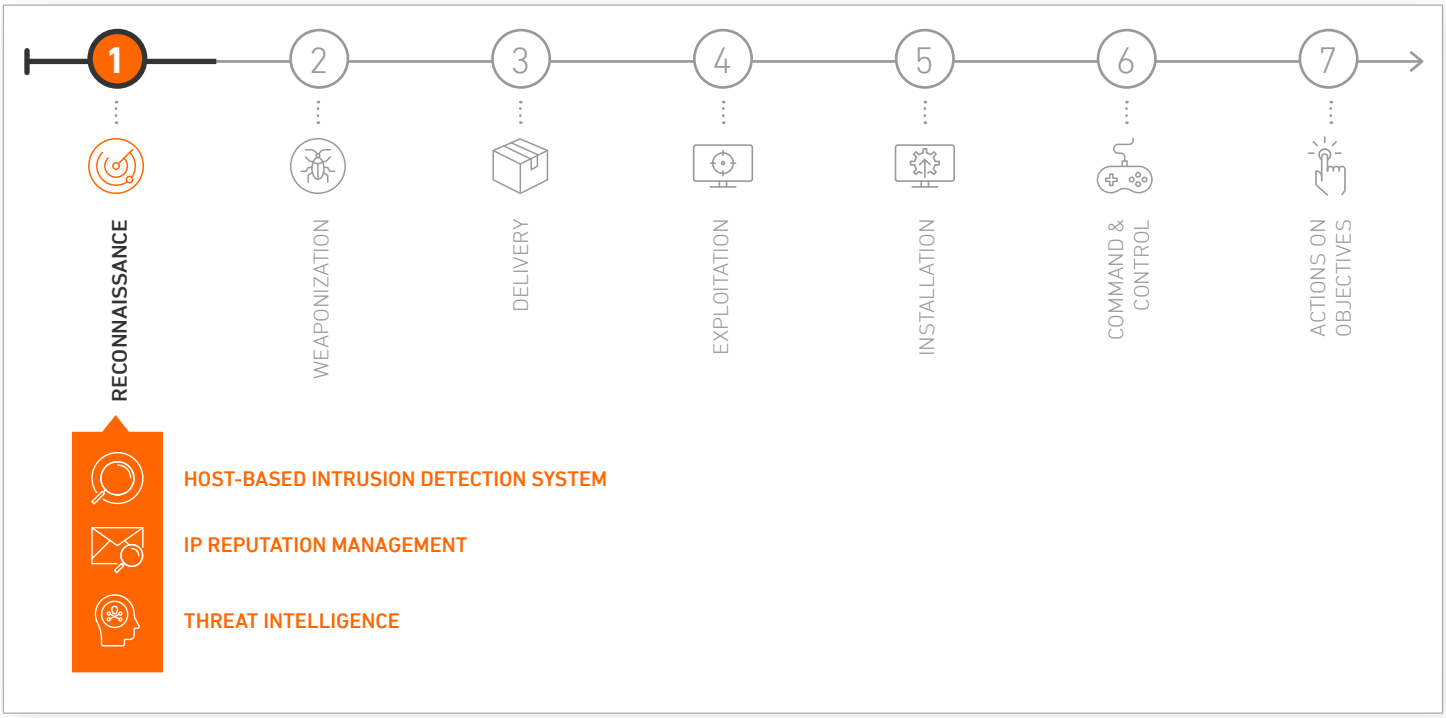
HOW ARMOR DETECTS & RESPONDS TO RANSOMWARE

Armor's cloud security platform, the industry's leading threat detection and response platform, ingests logs from the Armor Anywhere agent and from cloud-native 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 customer environments for known malicious signatures that can signal a ransomware attack at the earliest stage of the Cyber Kill Chain. **Our host-based intrusion detection system (HIDS) and IP reputation management**, coupled with our **threat intelligence**, monitors cloud network traffic during the **reconnaissance stage,** blocking known bad signatures immediately when they are detected.

Armor provides cloud security controls that aim to detect and respond to cyberattacks at various stages of the Cyber Kill Chain. As part of a layered approach to cybersecurity, Armor provides:

- Host-based Intrusion Detection System (HIDS)
- File Integrity Monitoring (FIM)
- Vulnerability Scanning
- Automated Security and Compliance (CSPM)
- Antivirus/Antimalware (AV/AM)
- IP Reputation Management
- 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.

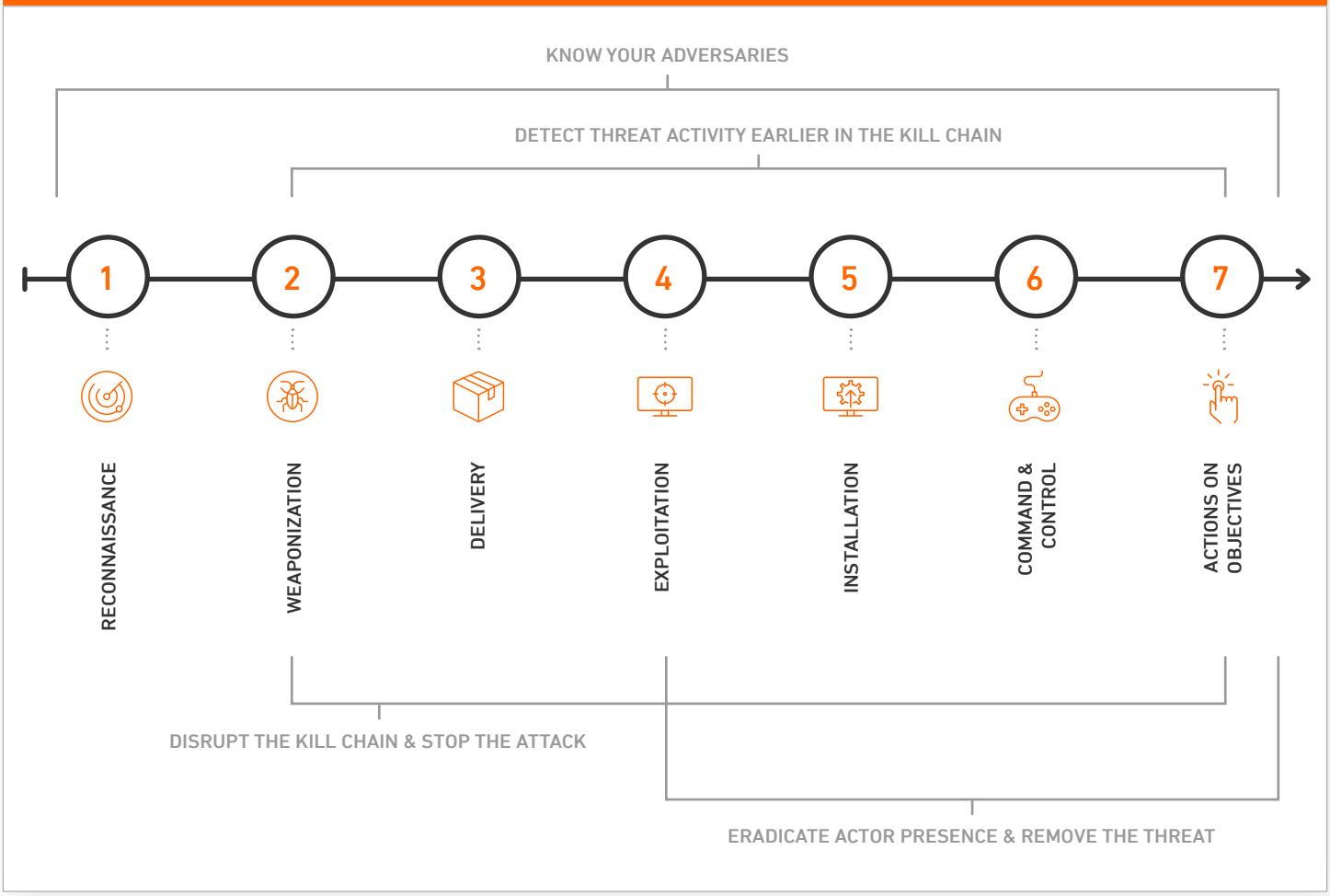
Antivirus/antimalware controls detect, quarantine, and/or block malicious software from executing on networks and workstations. IP Reputation Management filters stop messages based on source and destination IP addresses. Our threat intelligence is constantly updated with known bad IP addresses used by bad actors, such as commonly used command and control servers, malware delivery infrastructure, and other attack infrastructure.

Our **Threat Resistance Unit (TRU)** actively analyzes critical threats to our 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 malware reversing and dark web research. Through our TRU, Armor can sometimes identify the latest threats before they are widely known and patched by software vendors.

Ransomware attacks such as those on municipalities, school districts, and Managed Service Providers (MSPs) 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 into 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 an organization's applications and data. Combined with a comprehensive and ever-changing security posture, one that aims to "secure left" throughout the Cyber Kill Chain, Armor's security controls can help companies combat the growing scourge of ransomware.

ADDITIONAL TIPS FOR PROTECTING YOUR ORGANIZATION FROM RANSOMWARE

PATCHING
Organizations 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
Users 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 environment by providing a short list of approved applications and processes. Similar to a VIP list for your PC, if it's not on the list, it's not allowed.

PRACTICE LEAST PRIVILEGE ACCESS CONTROL
Ensure the user has the least privilege for their job. This also applies to services.

AUDIT/PENETRATION TESTING FROM INDEPENDENT, THIRD-PARTY EXPERTS
Ensure that you are implementing security best practices.

CONTINUOUS SECURITY AWARENESS TRAINING
Educate 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.

ENDPOINT PROTECTION SOLUTION
This solution should include endpoint detection and response capabilities for laptops, workstations, and mobile devices. It utilizes antivirus (AV) and antimalware (AM) to block cyberattacks. It is also used to quickly detect and remediate any malicious activity or infection that has made its way onto the endpoint.

ARMOR ANYWHERE

Armor Anywhere is Armor's flagship technology that provides threat detection and response as well as helps organizations meet compliance. Armor Anywhere combines workload protection, analytics from cloud-native sources, and other security data to provide unparalleled insight into threats facing organizations in any environment.

Organizations with mission-critical applications can choose Armor's high-performance hosting infrastructure and still enjoy the security benefits of Armor Anywhere.

ABOUT ARMOR

Armor is a global cybersecurity software company that simplifies protecting your data and applications in private, public, or hybrid clouds—or in an on-premise IT environment. Armor Anywhere provides technology to detect and respond to threats and can be activated in minutes. Armor also helps organizations comply with major regulatory frameworks and controls. Armor's cybersecurity experts monitor customer environments 24/7/365 and, if an attack takes place, helps customers respond quickly and effectively. Wherever you are on your cloud journey, Armor can help. We make cybersecurity simple.

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