White Paper

Threat Use Case: Defending Against Ransomware

rackspace technology® | ARMOR

Table of contents

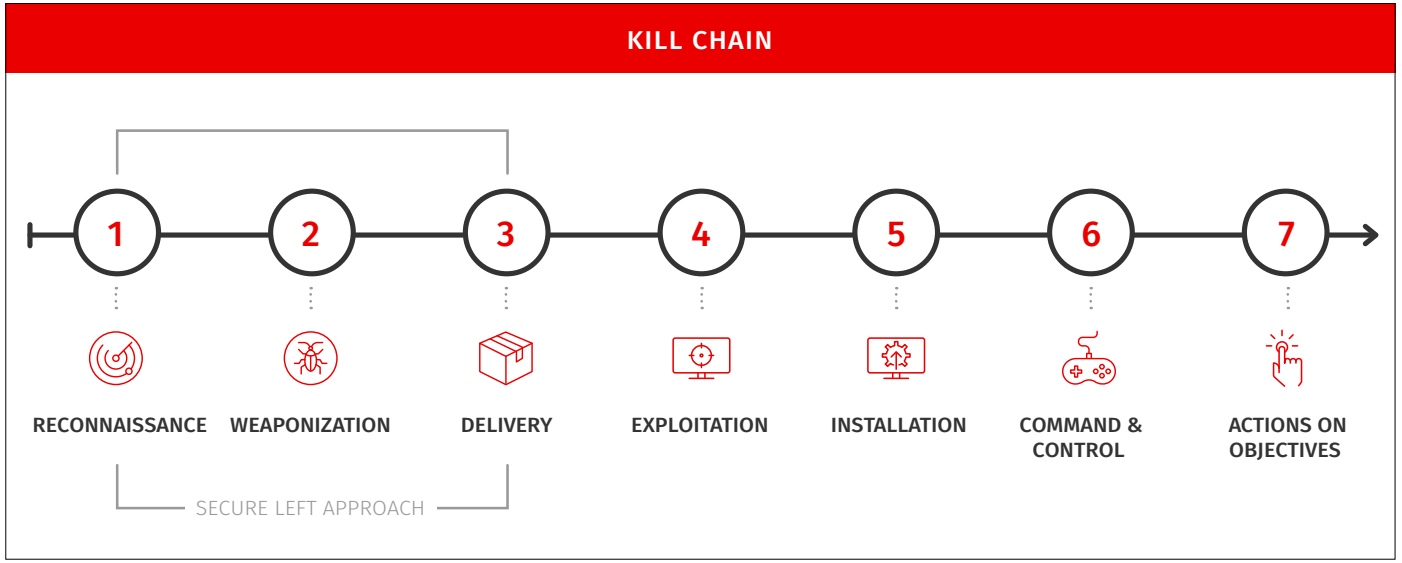
rackspace technology® | ARMOR

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 of a variety of destructive new applications and techniques. In a 2020 study, 51% of organizations indicated they were impacted by ransomware in the last year. 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 attacks vary by type and delivery method, but they primarily expose themselves at the last stage of the 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 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.



rackspace technology. | ARMOR

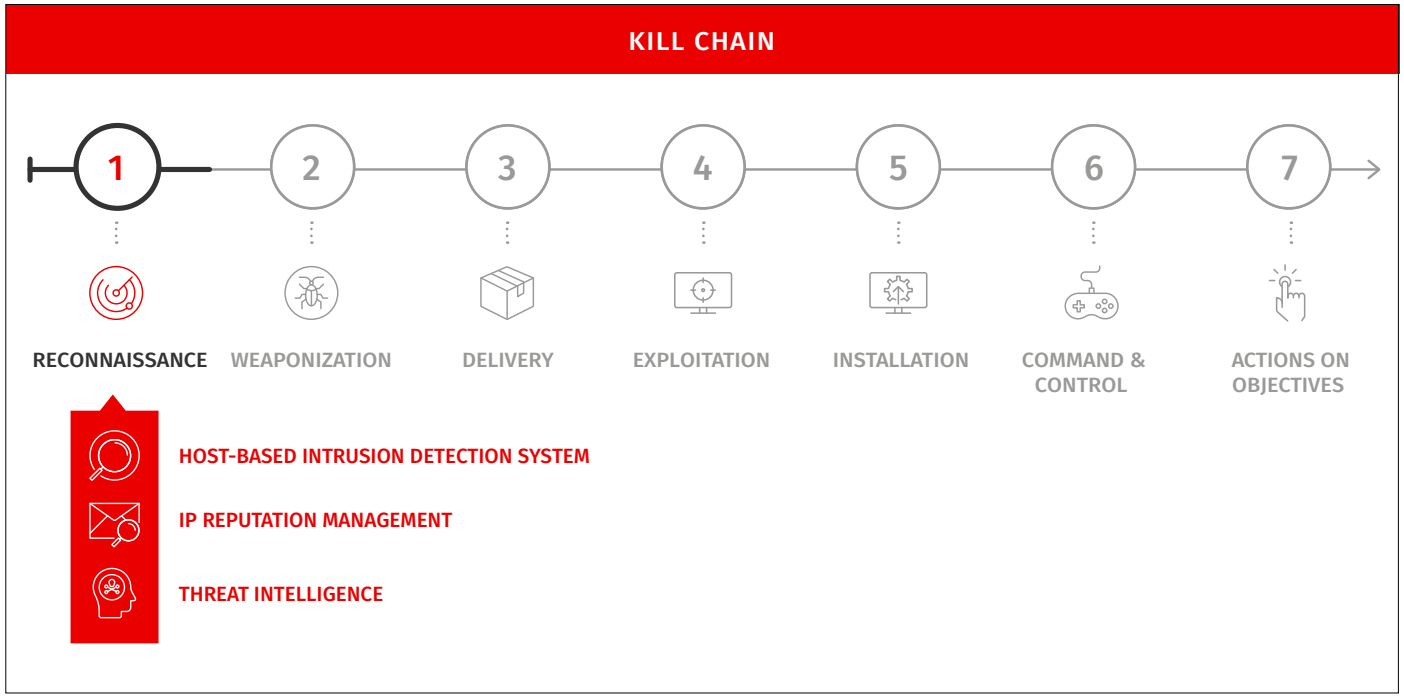
How to detect ransomware

The first and most critical step in the Kill Chain is **reconnaissance**. It's critical to have a security agents deployed into your environment to continuously monitor for known malicious signatures that can signal a ransomware attack at the earliest stage of the kill chain.

Rackspace Security Essentials combines industry-leading global security expertise with the Armor Anywhere cloud security platform that includes a layered approach to cybersecurity:

- 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

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.

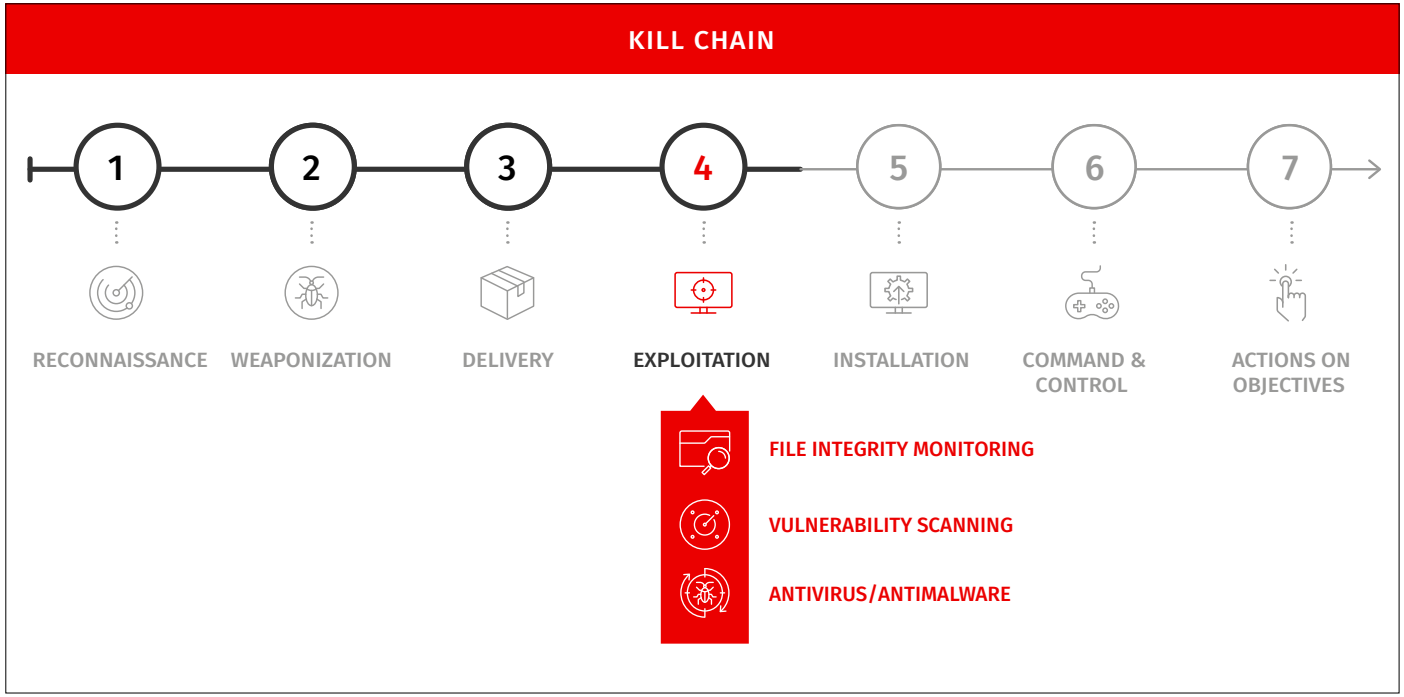


Rackspace Security Essentials provides cloud security controls that aim to detect and respond to cyberattacks at various stages of the kill chain.

Rackspace Security Essentials leverages Armor's industry leading threat detection and response platform which 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.

rackspace technology® | ARMOR

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 targets

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.

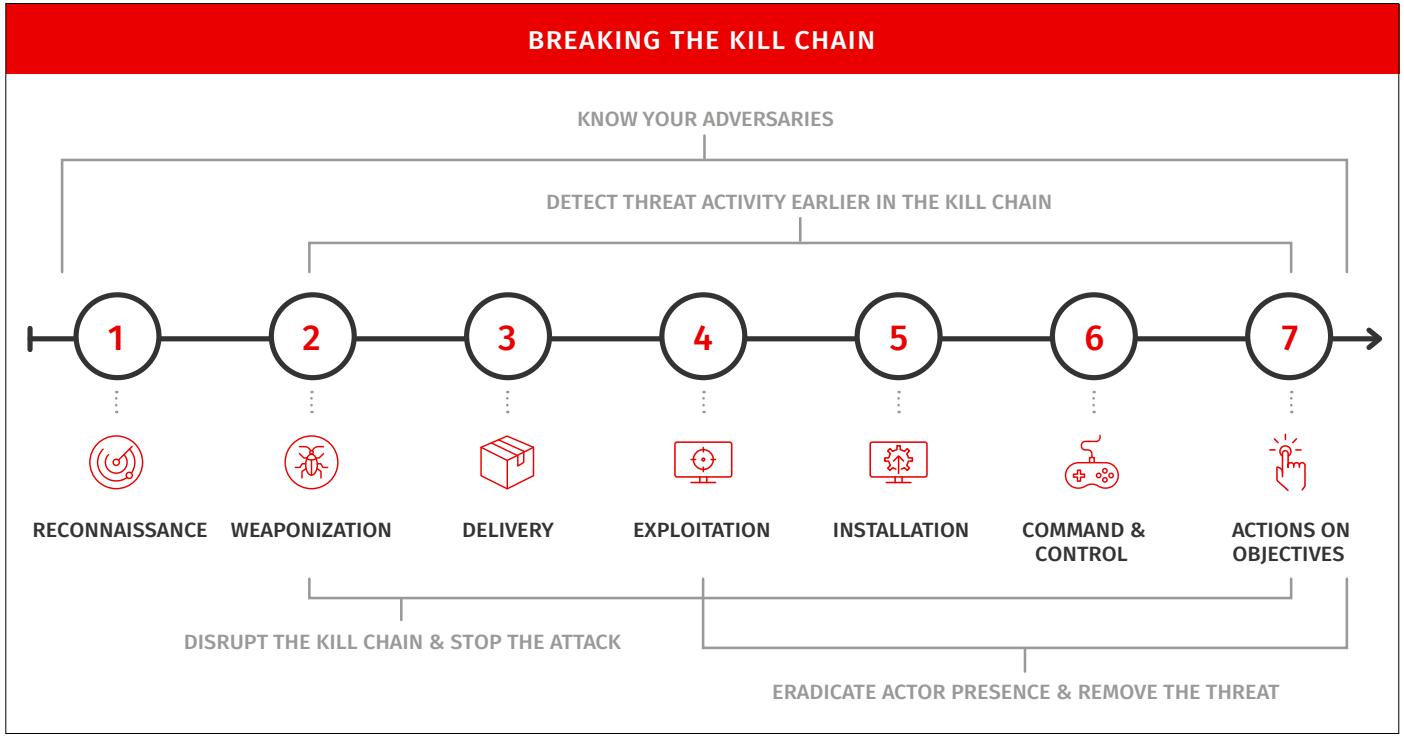
When threat actors initially get a foothold into an organization by compromising a corporate workstation (often via a malicious email link or attachment), many are not always trying to inject ransomware onto a single workstation. They are instead looking for infrastructure containing critical data and 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.

rackspace technology® | ARMOR

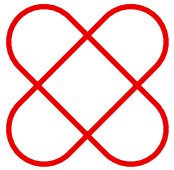
Breaking the kill chain

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.”

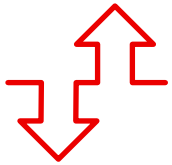
But by stopping threats further left in the kill chain, and continuously monitoring your environment through automation, Armor Anywhere can greatly reduce the chances ransomware will infect an organization’s applications and data. Combined with a comprehensive and ever-changing security posture, one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



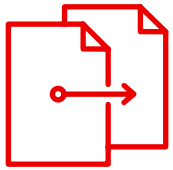
Additional tips for protecting your organization from ransomware



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).

Whitelisting 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.

rackspace technology® | ARMOR

Conclusion

How Rackspace Technology can help

Protect your business with advanced threat detection and incident response services.

Adding security to your environment is now easier than ever. Rackspace Security Essentials combines industry-leading global security expertise with the Armor Anywhere cloud security platform for a service that your business can rely on around-the-clock for advanced threat protection and 24x7x365 incident response.

The lightweight security agents can be swiftly provisioned onto your servers, VMs and public cloud instances, because it doesn't require any hardware or changes to your existing applications — even live workloads.

Here's what's included in Security Essentials:

- **Advanced Threat Detection:** Get advanced protection against cyber threats through an integrated suite of security capabilities that includes an intrusion detection system (IDS), antivirus (AV), malware protection, file integrity monitoring (FIM) and threat intelligence.
- **24x7x365 Incident Response:** Rackspace Technology security experts monitor security alert activity to detect possible compromises and respond to incidents around the clock.
- **Vulnerability Scanning:** Reduce risk and stay ahead of the next threat with increased visibility into technical vulnerabilities, patching and compliance issues.
- **Log and Data Management:** Log data can be stored for up to 13 months to support compliance requirements.
- **Enable Audit-Ready Compliance:** Enable compliance with security controls mapped to mandates such as PCI DSS, HIPAA, HITRUST and GDPR.

For organizations who require a full-scale security service with proactive cyber hunting, guaranteed environment coverage, custom reports, monthly security reviews and more, we also offer the Proactive Detection and Response service.

Learn more at:
www.rackspace.com/lp/rackspace-security-essentials
or call 1-800-961-2888

rackspace technology® | ARMOR

About Rackspace Technology

Rackspace Technology is the multicloud solutions expert. We combine our expertise with the world's leading technologies — across applications, data and security — to deliver end-to-end solutions. We have a proven record of advising customers based on their business challenges, designing solutions that scale, building and managing those solutions, and optimizing returns into the future.

As a global, multicloud technology services pioneer, we deliver innovative capabilities of the cloud to help customers build new revenue streams, increase efficiency and create incredible experiences. Named a best place to work, year after year according to Fortune, Forbes, and Glassdoor, we attract and develop world-class talent to deliver the best expertise to our customers. Everything we do is wrapped in our obsession with our customers' success — our Fanatical Experience® — so they can work faster, smarter and stay ahead of what's next.

Learn more at www.rackspace.com or call 1-800-961-2888.

TSK-6121 Ransomware White Paper v6a :: May 26, 2022