SOLUTION BRIEF

RANSOMWARE PROTECTION

Workloads Are the New Attack Surface

Ransomware, espionage, sabotage, theft, fraud and other exploits are proliferating exponentially. The most insidious threats bypass traditional defenses and execute at the speed of code, often going undetected for days, weeks, months or even years. Organizations must assume that their networks already have the precursors to the next ransomware attack inside it.

The workloads themselves are the new attack surface. To effectively protect them, security solutions must include system assurance, application control and memory protection. Code that executes during runtime can be almost undetectable, and the traditional blacklisting approach cannot possibly detect all the malware that is generated each day. Adopting a positive security model and arming the workloads to defend themselves is the best protection against the most sophisticated and evasive ransomware attacks.

Ransomware Techniques

Ransomware attacks can use a wide range of techniques to break into systems, access sensitive data, hijack operations, deploy encryption tools, encrypt data, and demand a ransom in exchange for retrieving encryption keys.

The encryption/ransom step is usually the final objective, which only executes after multiple other hacking steps. These steps typically include:

- **Initial Infiltration –** exploiting web-based attacks such as a SQL injection or stealing credentials through phishing or social engineering to gain initial access.
- **Command & Control –** deploying shell code and escalating privileges to remotely hijack control over internal servers or resources.
- **Weaponization –** remotely executing commands to locate critical assets, overtake operations, exfiltrate or encrypt data, and demand ransoms.

VIRSEC

"Virsec understands what's happening to applications at runtime, effectively making them self-defending."

CISCO

"Real-time memory protection on servers is the single most important protection upgrade a company can make."

AITE Group

"Virsec monitors how code executes at the lowest level and instantly detects when an adversary is doing something bad."

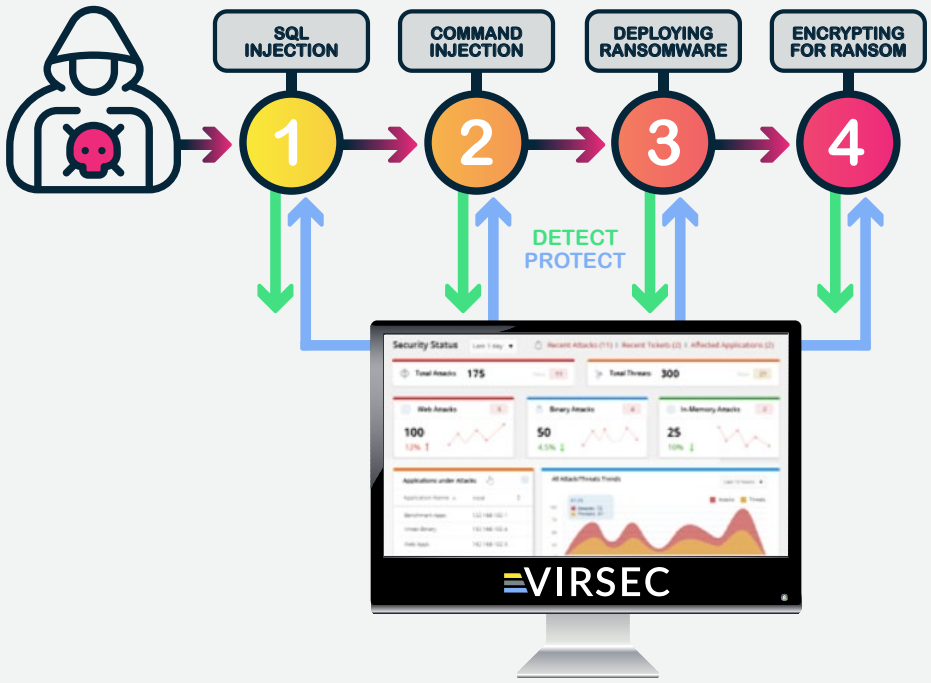
Raytheon

 • 226 Airport Parkway, San Jose, CA 95110 • VIRSEC.COM

Advanced Ransomware Protection

Virsec is unique in its ability to precisely detect each step of a complex attack within milliseconds and instantly take actions to surgically stop attacks without disruption. By protecting the full attackable surface of an application, Virsec provides application defense-in-depth to stop ransom attacks immediately, regardless of the specific sequence used.

Following is an example of a multi-step ransomware attack and how Virsec can protect at each step:

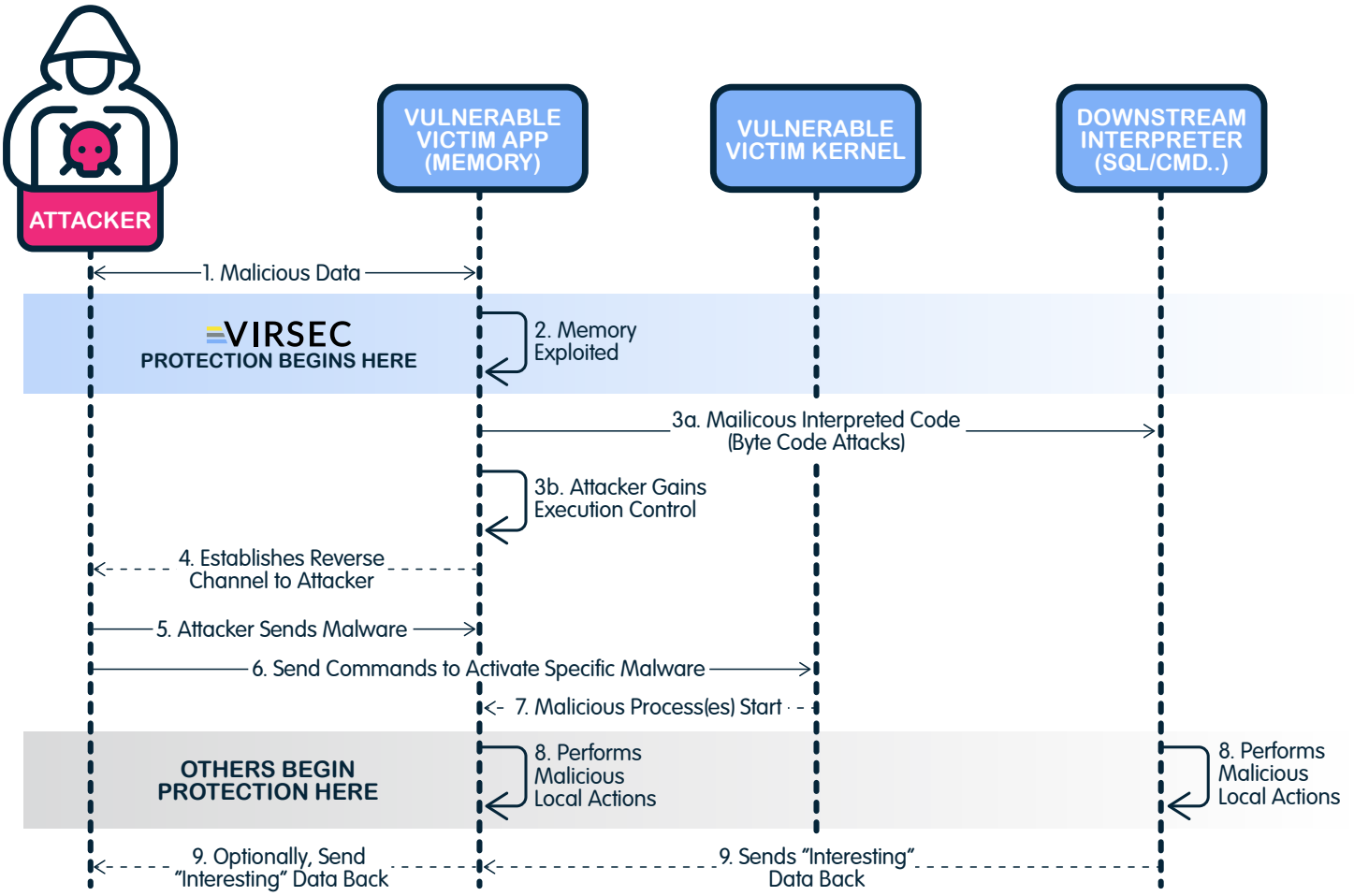


Virsec protects against the most sophisticated and evasive multi-step ransomware attacks.

- **Web Attacks –** detects and stops the widest range of SQL injections and other web attacks.
- **Command Injections –** instantly detects and stops illicit command injections used to hijack control.
- **Deploying Ransom Tools –** detects downloads and stops unauthorized processes from executing.
- **Encryption –** detects attempts to encrypt data and quarantines and restores sensitive files.

Precise Actionable Forensics

Because of Virsec's unrivaled visibility and accuracy, it delivers precise forensics with extensive, detailed information including the precise time, threat ID, victim's and attackers' IP addresses, and session tokens. Virsec also captures the full HTTP request that triggered the attack, and the complete attack payload. This data can be invaluable in finding system vulnerabilities, alerting SIEMs, or triggering other network tools to disable attacker access and prevent future attacks.



Host, Memory and Web Protection

Virsec is the first and only application-aware workload protection platform that provides System Integrity Assurance, Application Control and Memory Protection in a single solution. This technology delivers in-depth visibility into the entire workload – no matter where it resides. Unlike heuristic or endpoint solutions, Virsec technology identifies threats the moment they happen – without latency, probabilistic detection models, prior threat knowledge, analysis, or threat hunting. Virsec's deterministic defense enacts a kill chain process the moment an application, OS, file library or process deviates from the norm, with zero dwell time, zero tuning and zero noise.

Complete Runtime Visibility

Most security tools are stuck at the perimeter and guess at what threats look bad. Virsec is instrumented in the workload and delivers complete visibility across the application stack from the inside.

Application Awareness

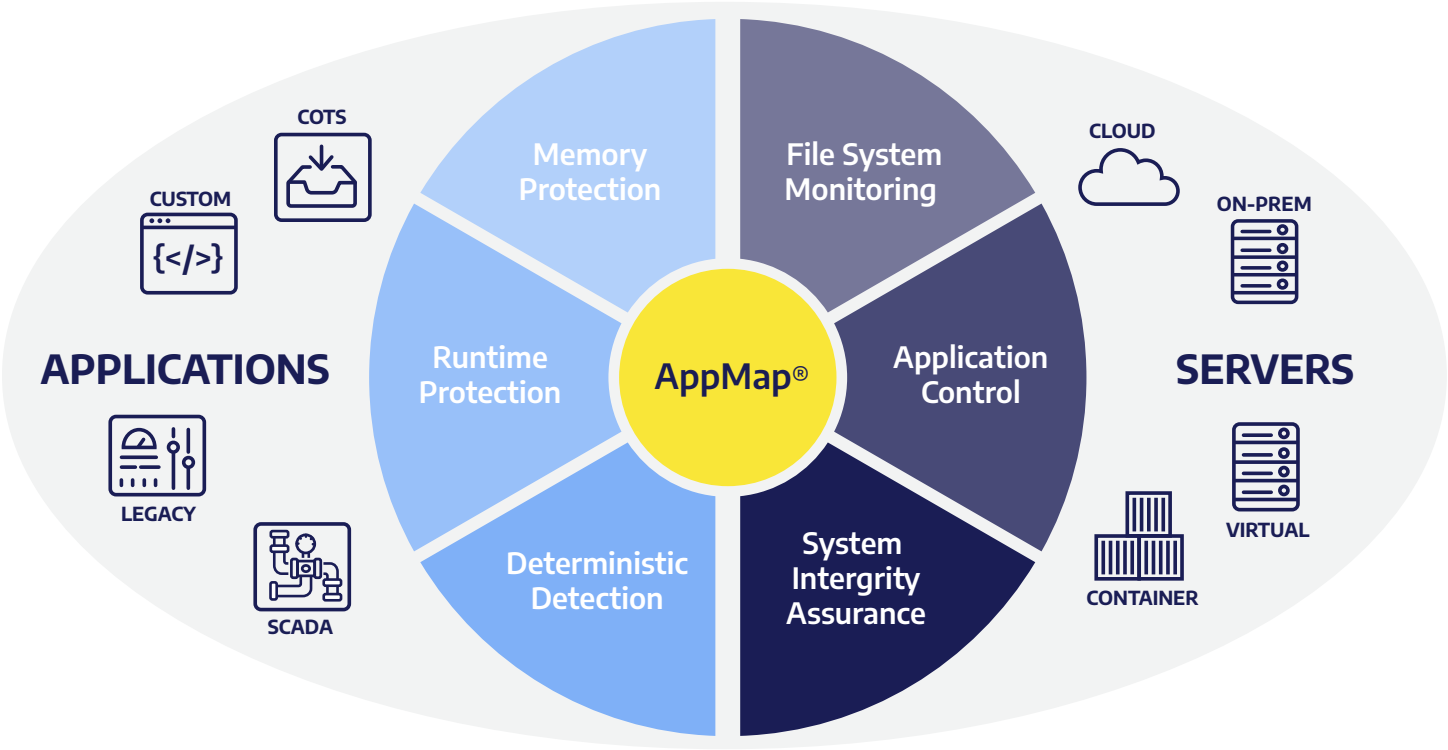
Patented AppMap® technology maps acceptable files, processes, libraries, web input, memory usage, control flow and more. This enables Virsec to instantly detect and stop any deviations, preventing attacks at the first step before damage occurs.

Application-Aware Workload Protection

Virsec provides application-aware workload protection against the widest range of evasive cyberattacks – known and unknown – and secures applications from the inside. Virsec protects all your applications, including custom, COTS, third-party, legacy, SCADA and more. And the Virsec solution protects across any environment, including on-prem servers, virtual, cloud, hybrid, container, and edge.

ANYWHERE	ANYTHING	ANYTIME
On-prem, public/private cloud, hybrid, container	*Custom, legacy, COTS and air gapped applications*	*Deploys in minutes, protects continuously in real-time*

"Do not use an offering designed to protect end-user endpoints and expect it to provide adequate protection for server workloads." Gartner



Securing the World's Most Critical Applications

Virsec is deployed globally protecting mission-critical applications and infrastructure in industries including financial services, healthcare, government, defense, power, oil & gas, transportation, telco, technology, and more.

Recognition

Cyber Catalyst · CRN · Cyber Defense Global Awards 2019 Winner · Gartner · Cyber Security Excellence Awards Winner 2020 · MITRE · Info Security Products Guide 2020 Global Excellence Gold · Ovum

Partners & Customers

Cisco · Tech Mahindra · NCUA · Raytheon Technologies · Godrej · Schneider Electric · Yotta · Nutanix · du · AVEVA · Broadcom · inspirage · etisalat · GDIT

VIRSEC