RANSOMWARE PROTECTION
SOLUTION BRIEF

virsec®

The Ransomware Epidemic

Virsec delivers unrivaled protection against the most advanced cyberattacks, including those that attempt to encrypt sensitive data and hold it hostage for ransom payments. By protecting the full application stack at the web, memory, and host layers, Virsec can detect and stop ransomware attacks at the first step before damage is done.

Ransomware has become a widespread scourge because it is relatively easy for attackers to execute and can cause significant disruption and business damage, without hackers having to exfiltrate data. Because many organizations are willing to pay ransoms to retrieve lost data, and many insurance policies cover ransom payments, the wave of ransom attacks continues to accelerate.

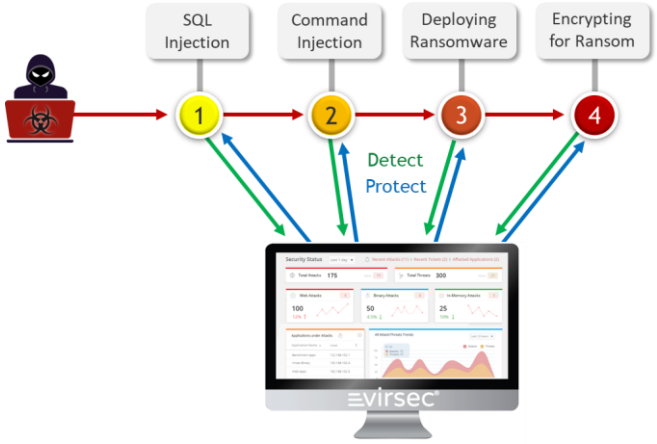
Ransomware Attack Kill Chain

Ransomware attacks can use a wide range of techniques to break into systems, find sensitive data, deploy encryption tools, encrypt data, and demand a ransom in exchange for retrieving encryption keys. In fact, the encryption/ransom step is usually the final objective, that 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, deploy encryption tools, and execute encryption to demand ransoms.

Virsec Stops Attacks at Each Step

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:

- **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 can quarantine and restore 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.