

# REDPRO SERVER: ENTERPRISE DATA PROTECTION AND RESILIENCY

## KEY FEATURES

- Zero-day server protection
- Ransomware protection
- Deception capabilities
- Secure, resilient storage data and user access rights
- Multilevel system monitoring, orchestration and automated response

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. REDPro Server 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, REDPro can detect and stop ransomware attacks at the first step before damage is done.

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. The encryption/ransom step is usually the final objective and only executes after multiple other hacking steps, such as:

- **Initial infiltration** — Exploiting web-based attacks such as a SQL injection or stealing credentials through phishing or social engineering to gain initial access.
- **Command and 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.

## BENEFITS

- Extensible cybersecurity platform for enterprise-scale data protection and cyber resiliency
- Integrates best-in-class hardware, software, network, data and user security
- Multilevel data security binds data to users, devices, locations, applications and time to contextually control data access — know who, where, when, what and how
- Risk-based, dynamic data access controls
- Integrates advanced system, storage and user behavioral analytics and data loss prevention
- Zero-trust enforcement continuously verifies and enforces system, network, application, data and user access rights
- Multilevel system monitoring, orchestration and automated response

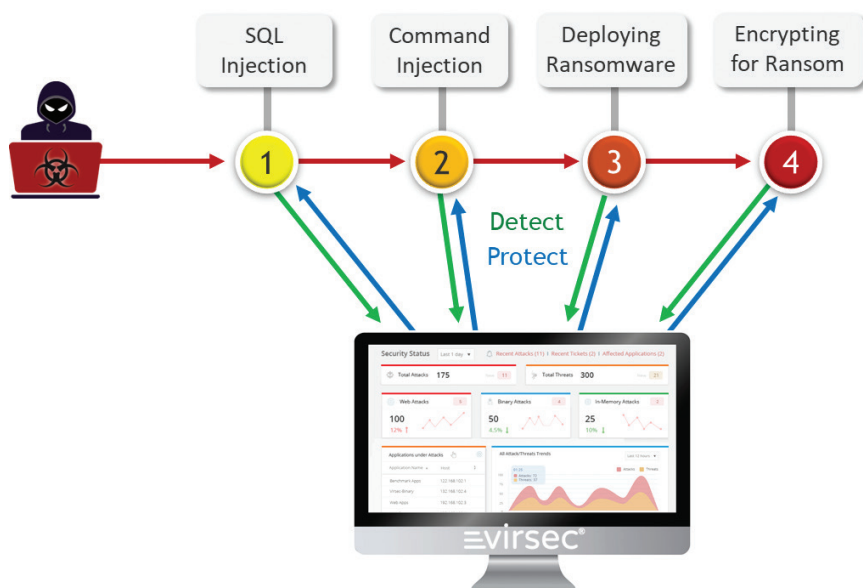
## REDPRO SERVER

### CAPABILITIES

REDPro Server 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, REDPro provides application defense in depth to stop ransom attacks immediately, regardless of the specific sequence used.

The following is an example of a multistep ransomware attack and how REDPro 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.



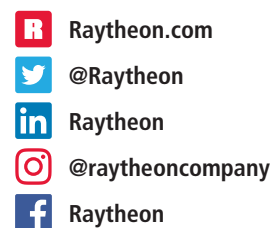
### PRECISE ACTIONABLE FORENSICS

Because of REDPro'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. REDPro 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.



For further information, contact  
luigi.valentini@raytheon.com  
raytheon.com/cyber

**Raytheon**  
**Intelligence, Information and Services**  
22260 Pacific Blvd.  
Dulles, Virginia  
20166 USA



**Raytheon**