FORTIS By Sentinel

Advancing Your Protection

Ransomware Attacks Continue to Rise

A recent report from Sophos surveyed 5,400 IT professionals from mid-sized organizations. 37% reported they had experienced a ransomware attack, and 54% confirmed their data had been encrypted. The average overall cost of these attacks was $1.85 million. Another study by Palo Alto Networks Unit 42 showed the average ransom demand for cases they consulted on increased 144% over the last year to $2.2 million, while the average payment rose 78% to $541,010. The impact of such an attack can devastate a business.

Keep Your Data Safe From Ransomware With Fortis Knox!

Fortis Knox combines Sentinel's CloudSelect® Backup as a Service (BaaS) and Fortis by Sentinel's ActiveDefense™ Security Operations Center (SOC) monitoring in a platform to protect and recover your data. Your organization receives a cyber vault that can be connected to your data center or cloud where it will store immutable backups (optional all-flash safe mode appliances also available). Even if a ransomware attack is successful and bad actors manage to access to your cyber vault, immutable backups prevent the deletion or encryption of the data.

The Fortis Knox vault is protected by a virtual air gap that includes firewalled connection protection and 24x7x365 monitoring by the Fortis ActiveDefense™ SOC. Our SOC continuously scans for any indicators of compromise, including unusual traffic, scanning, backup job changes, attempts to delete files, and other atypical activity. Alerts are issued at the first sign of trouble so Fortis by Sentinel's award-winning ActiveRecovery™ incident response experts can take immediate action. Regular penetration tests are also conducted by Fortis Advisory Services to ensure all strict vault policies remain enforced.

Protection, Detection and Response

Most organizations won't even identify a breach until it's too late. According to Mandiant® M-Trends 2022, ransomware-related intrusions had a median dwell time of five (5) days, compared to 36 days for non-ransomware intrusions. Fortis Knox offers full-fledged data backup protection plus rapid detection and response, so your organization can effectively and efficiently recover from an attack without paying any ransom.

Benefits

Immutable Recovery – hardened appliances powered by Veeam with secure network connections, ALWAYS CONNECTED to the Sentinel NOC & SOC

Rapid Recovery – many hardware options, from spinning disk to all-flash recovery

Local and Cloud Recovery – designed on premises or in the cloud for cloud native workloads, your vault ships to your primary data center sized to protect your workloads, with optional CloudSelect® connections to Sentinel's VMware hosting or public clouds (including AWS and Azure)

Monitored by Fortis ActiveDefense™ SOC 24x7x365 – provides constant insight that jobs, backups, snapshots, and hardened ports are all functioning as expected

Validated by Fortis ActiveRecovery™ Incident Response Teams – quarterly testing of operations and recovery readiness delivered by Sentinel's award-winning ActiveRecovery™ incident response experts

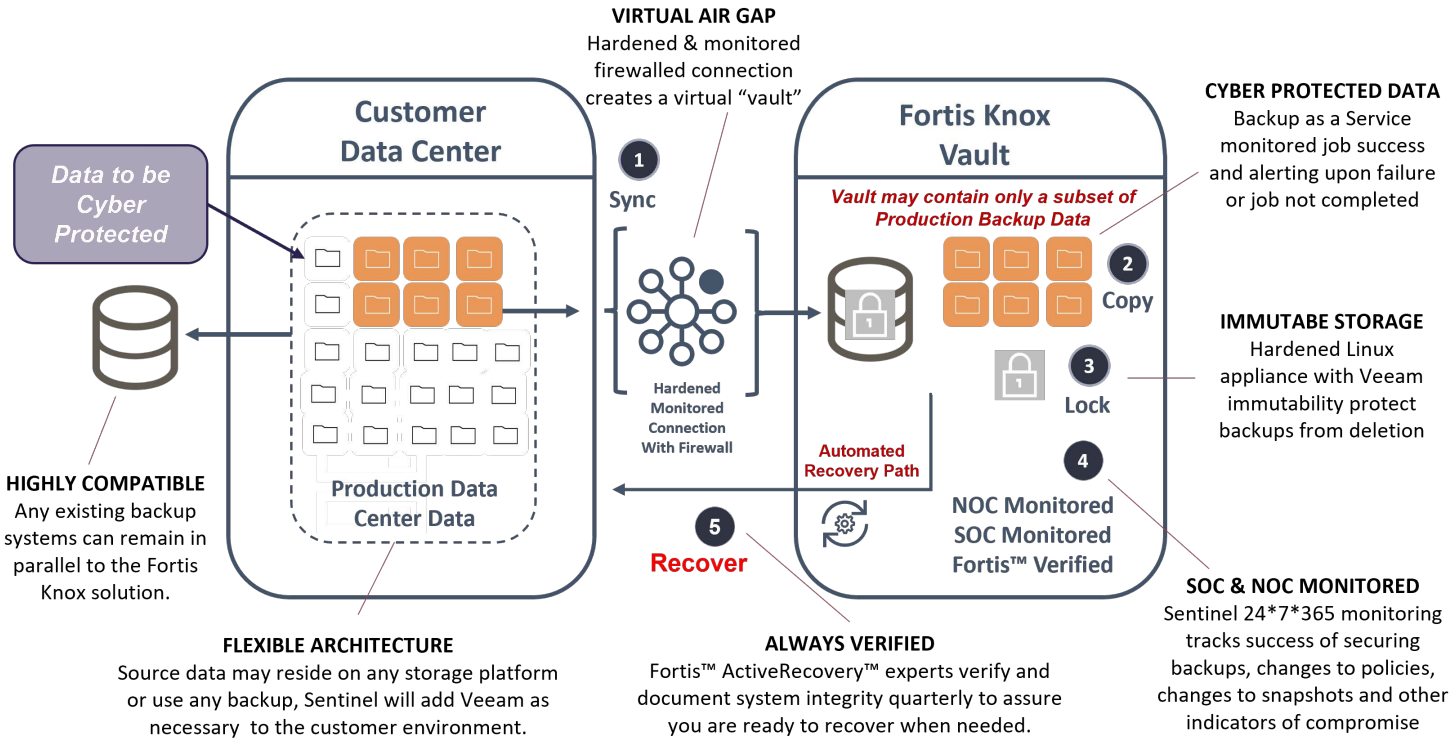
Delivered as a Service – complete solution delivered as a Service by Sentinel CloudSelect® and Fortis by Sentinel experts for the life of the contract – purchase options up-front or monthly recurring over the duration of the contract

Flexible Pricing Options – monthly, pre-paid annual, pre-paid in full and bring your own options available with "flex" retainer services useful for any Sentinel or Fortis service offering

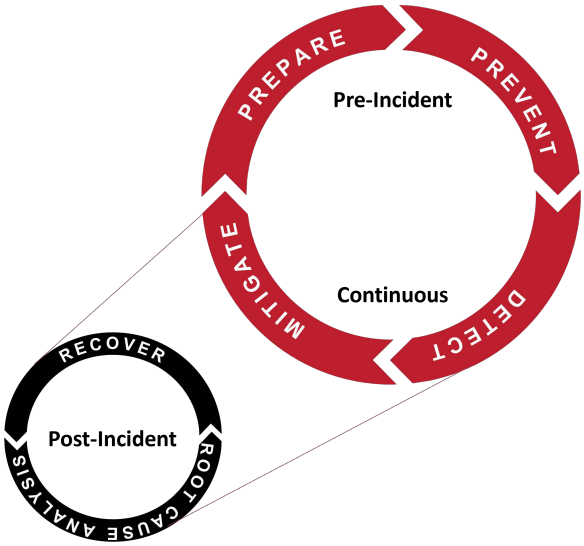
FORTIS By Sentinel

Advancing Your Protection

Fortis Knox Elements



Ransomware Circles Test



Pre-incident

Prevent ransomware by adopting a Zero Trust approach to cybersecurity. Combine this with technologies like endpoint & data protection, immutable backup, asset management, end-user awareness, strong identity, and access management to solidify your security posture.

Continuous

Ensure your environment remains always protected with 24x7x365 monitoring, alerting, risk investigation and containment. Further enhance protection by continuously measuring your cybersecurity maturity across NIST CSF, CIS and other advanced frameworks.

Post-Incident

Develop and execute a ransomware response playbook with experienced experts, schedule regular training exercises, and reserve the Fortis ActiveRecovery™ cyber response team today!

Contact Us Today for More Information!

www.fortisbysentinel.com
1.800.769.4343 (main)
1.844.297.4853 (Incident Response Hotline)
infoSENter@sentinel.com