DATA SHEET

RANSOMWARE DEFENSE

Defend your critical infrastructure against the threats of targeted and non-targated ransomware with comprehensive protection

VERVE SECURITY CENTER

The Verve Security Center was designed to provide comprehensive cyber defense. To defend against ransomware in OT, organizations need to deploy multiple layers of overlapping protective and detective measures.

Verve's integrated and open platform enables operators to understand risk posture, rapidly identify most effective remediation strategies, and rapidly take action to defend against a potential attack. No other tool enables integrated layers of defense and response against ransomware in OT/ICS.

RANSOMWARE REQUIRES LAYERS OF PROTECTION

95% of OT/ICS attacks occur through the commofity IT equipment in the environment	Defense requires visibility into all assets, robust patching strategies, measurable compensating controls, as well as confirmed backups in case of emergency	Verve integrates these components to provide simple, but comprehensive coverage

VERVE

ICS/OT RANSOMWARE CHALLENGES

- Ransomware often hits untargeted organizations as it spreads - you don't need to be a critical asset to be impacted
- Most ransomware attacks take advantage of unpatched commodity systems and patching is difficult in critical operational environments
- Vulnerabilities and missing patches are only one axis an attack. Dormant users, insecurely configured devices, insecure password settings, open ports and services all also offer potential for ransomware infiltration
- Defense requires multiple layers of compensating controls: network protection, application whitelisting, etc. and strict monitoring of maintenance that those controls are in place
- Ransomware quickly spreads horizontally in non-segmented networks can rapidly cripple an organization
- Response must be very rapid to stop the spread, but false positives can cause expensive shutdowns
- Recovery in case of successful attack requires robust, updated backups stored in offline repositories - which are not often present in OT/ICS environments
- The cost of recovery is in addition to a cost of disruption and can into the hundreds of millions for large organizations

BENEFITS

- Improved visibility of potential ransomware risks
- Lower cost protection with integrated assessment and remediation in same platform
- Faster time to remediation and response with limited actions
- Better defense visibility with integrated compensating control information
- More comprehensive defense by reducing risk in configuration, user access, network defense, etc.

FEATURES

- Comprehensive IT and OT asset inventory to identify all potential targets of ransomware
- Detailed vulnerability and patch assessment to discover potentially vulnerable devices
- Full 360-degee risk assessment of the asset allows identification of comprehensive risks, not just the missing patches (e.g. users & accounts, insecure configurations, etc.)
- Full visibility into network connectivity and running configurations on switches enables view of potential network protections
- Integrated actionability to automate remediation of patches, configuration hardening, etc.
- Integration with third-party defense tools, such as next-gen antivirus and application whitelisting to allow for data-based monitoring of compensating controls
- Machine learning engine identifies potential anomalous indicators of ransomware spread
- Integrated response actions to speed response times