DATA SHEET

RISK SCORING AND PRIORITIZATION

Reduces cost and complexity of OT/ICS security

SUMMARY

Risk scoring is the process of calculating a score based on a number of risk and protection factors that enable the prioritization of risks that require remediation.

Key elements include:

- Gathering detailed endpoint system status information
- Understanding asset criticality to determine potential impact from an event
- Understanding how different security risks and protective measures work in concert to make an asset more or less risky
- Assigning scores to different risks and criticality. Calculating an overall score for vulnerability and impact.

Every critical vulnerability doesn't present the same security risk to operational systems. Vulnerability scanning and analysis is only one lens into the risk of an asset.

To prioritize remediation of security efforts and reduce cost and complexity, organizations need ICS/OT risk assessments that include comprehensive risk scoring.

Verve Security Center's agent-agentless platform approach creates a 360-degree risk view of each asset to streamline remediation and get the greatest ROI on their security dollars.

BENEFITS

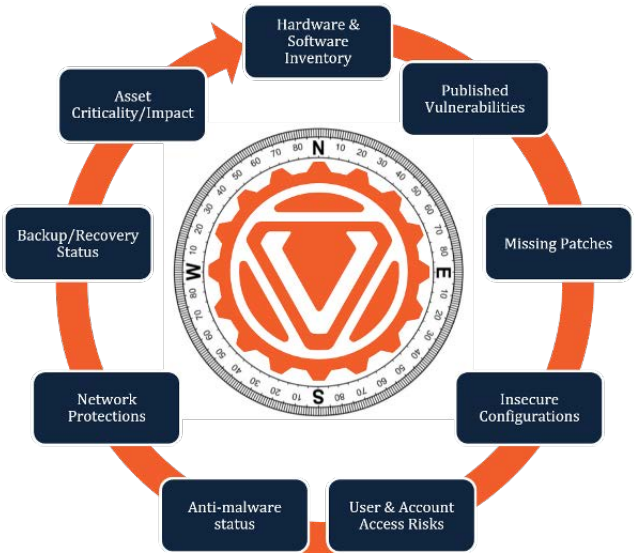
A 360-degree view of an asset's risks and potential impacts of that risk on the process provides prioritization for a timely and cost-effective remediation strategy.

- Comprehensive view of the risk to an asset because of the agent-agentless platform approach for the deepest asset risk visibility available
- Comprehensive view of all potential defenses through integration of third-party tools, such as antivirus and whitelisting, firewalls, etc.
- Real-time update of scores without risky scanning
- Customized to each specific operational process by integrating data from clients own PHA, disaster recovery plans, etc.
- Increased ROI of remediation based on prioritized actions

VERVE
A ROCKWELL AUTOMATION COMPANY

360-DEGREE RISK ASSESSMENT

- **Asset inventory:** Gather 100% views of all hardware and installed application software to identify all potentially risky software
- **Vulnerabilities:** Comprehensive IT OT device vulnerabilities with ratings
- **Missing patches:** All missing patches - not just those approved by vendors - without scanning
- **Insecure configuration settings:** Over 100 ICS/OT specific configuration checks from password settings to ports and services
- **Users and accounts:** Inventory of all users and accounts on the system including dormant, shared, service accounts, etc.
- **Anti-malware status:** AV and application whitelisting protections and recency
- **Network connectivity and protection:** What is communicating (and can communicate) based on network rules and connections
- **Backup status:** Availability of recent confirmed backups



- **Device functions:** Domain server, HMI, core switch, etc.
- **User-defined criticality data:** Based on PHA, disaster planning, etc.
- **System process identification:** Determine criticality of steps in a process controlled by an individual device