DATA SHEET

VULNERABILITY ASSESSMENT

Prioritize risks with 360-degree assessments

SUMMARY

OT/ICS Vulnerability Assessment is complicated. Older devices, embedded devices which cannot be scanned with traditional IT solutions, lack of comprehensive asset inventory, policies and procedures not designed for OT/ICS, all create challenges to robust vulnerability analysis.

Verve addresses these challenges with a unique tech-enabled assessment approach that leverages our 25+ years of experience and Verve Security Center software platform.

This combination of “man and machine” ensures a comprehensive assessment in the least time and cost possible. It also offers the advantage of a real time ongoing assessment, rather than a one-off manual process.

> “The ability to use Verve to see the full range of vulnerabilities from missing patches to insecure configurations on endpoints, to inappropriate network design and firewall rules in a single platform allows us to rapidly prioritize critical remediation steps.”
>
> **USA CISO** | FORTUNE 100 PHARMACEUTICAL COMPANY

VERVE

THE VERVE DIFFERENCE

Expertise

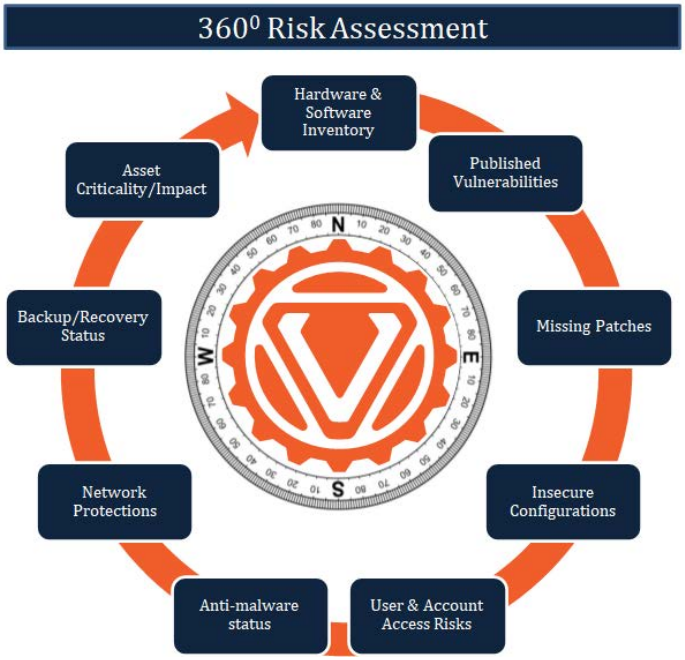
Verve's 25+ years of OT/ICS experience provides deep expertise both in assessing the risks to the critical processes, but also designing the right remediation strategies – from patching to deploying compensating controls depending on the cost and sensitivity of the system.

Technology

Verve's tech-enabled approach, leveraging the Verve Security Center ensures 100% asset visibility into OT/ICS networks, deeper endpoint level assessment, and ability to conduct real time assessments going forward, rather than one-time manual efforts.

360° Risk Analysis

Verve offers network design and segmentation implementation, including firewall deployment, switch and subnet configuration, endpoint re-IP'ing as necessary, etc. Leverage our cross-vendor controls systems expertise for a single partner in your journey.



FEATURES

- Gather vulnerabilities across all assets on OS, application software and firmware with no need for scan-based tools or manual processes
- Add asset criticality metrics based on criticality of asset to the process or safety
- Gather and integrate dozens of other risk metrics on the asset: enabled users and accounts, configuration settings, password settings, backup status, antivirus or whitelisting status, network security configurations, etc.
- Closed-loop actions to immediately pivot from risk to remediation in the same platform

BENEFITS

- Ongoing real-time risk updates as remediation takes effect
- Less expensive and faster than manual solutions
- No risk from scanning like IT tools
- Enables risk prioritization across dozens of risk and asset criticality variables
- 100% software-based with no need for hardware or span taps/ports
- Expert resources to assess risks and remediation strategies