



Verve Capabilities Overview

Achieve Comprehensive OT Visibility

Complete asset visibility is essential for OT/ICS cybersecurity. By understanding each asset's context, organizations can assess vulnerabilities, manage configurations, and prioritize risks effectively, forming a strong defense against security threats.

The Verve Difference

Verve®'s approach to asset inventory integrates contextual data with deep asset visibility, allowing organizations to prioritize risks and address vulnerabilities efficiently, all without the operational impact of traditional network scans.

Hybrid Technology:

Combines agent-based and agentless approaches, collecting deep asset data without network interference.

Detailed Data

Collection: Profiles each asset, including IP, patch status, user accounts, and antivirus details, without active scans.

Automated

Monitoring: Alerts on new asset connections and changes, delivering quick responses to unauthorized activity.



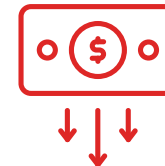
Enhanced Visibility with

Contextual Data: Collects over 1,000 data points per asset, including software, firmware, configurations, and critical contextual information that enables risk prioritization.



Efficient Compliance:

Simplifies regulatory reporting with extensive, centralized asset tracking.



Cost Savings: Deploys quickly and inexpensively with a 100% software approach—no need for costly infrastructure such as spans, taps, or custom scripts.

Case Study I

Asset Inventory

A global top 10 Industrial Gas manufacturer with over 700+ sites needed a solution to achieve complete visibility into its OT assets. The client's sites spanned various geographies, and many locations were unmanned, making it challenging to maintain accurate asset data for cybersecurity and operational management.

APPROACH



Rapid Deployment and Comprehensive Visibility:

The Verve Security Center provided deep asset visibility across all sites. Verve's agent-agentless technology enabled deployment to over 500 locations within 3 months without additional hardware, which was critical for unmanned and remote sites.



Centralized, Cloud-Based Management:

Verve's platform centralized data collection and reporting, allowing the client's IT/OT teams to monitor asset inventory, detect changes, and identify risks in real time across its entire global footprint.

OUTCOME

The manufacturer achieved complete asset visibility across 500+ sites, significantly advancing their ability to manage risks and proactively secure their OT environment without operational disruption.

Proactively Manage OT Vulnerabilities

Older and embedded devices often lack traditional patching options, making it crucial to identify and mitigate vulnerabilities efficiently. Effective vulnerability management helps protect critical systems, reduce cyber risks, and ensure operational safety.

The Verve Difference

Verve's approach integrates OT-safe, real-time vulnerability management with contextual risk prioritization, enabling focused, efficient remediation in a single, cost-effective solution.

OT-Safe, Agent-Agentless Monitoring:

Gathers deep risk data safely, avoiding the disruptions common in IT-based scanning tools.

360-Degree Risk Assessment:

Provides a full view of vulnerabilities and generates a tailored remediation roadmap aligned to your OT environment's needs.

Closed-Loop Remediation:

Automates mitigation actions directly from the platform, streamlining risk response without requiring separate tools.



Comprehensive Risk Insights:

Continuous visibility across OS, firmware, configurations, and network vulnerabilities.



Faster Remediation:

Integrated platform enables immediate action from identification to mitigation, reducing remediation time.



Improved Security Posture:

Prioritizes risks based on asset criticality, supporting focused remediation that enhances resilience.

Case Study I Vulnerability Management

A leading Consumer Packaged Goods (CPG) manufacturer with a global presence required a way to rapidly assess and remediate vulnerabilities across its diverse OT environments. The company's infrastructure was complex, with multiple plants acquired over time, each following different security practices and OT maturity levels.

APPROACH



Comprehensive Risk Visualization and Prioritization:

Verve's Security Center provided an in-depth vulnerability assessment across all sites, allowing the CPG manufacturer to visualize risks and prioritize remediation efforts across its global footprint.



Closed-Loop Remediation:

With Verve's closed-loop architecture, the company could initiate immediate remediation actions upon identifying vulnerabilities. Verve's centralized management console allowed the IT/OT teams to plan and execute vulnerability mitigation steps at each site based on real-time data.

OUTCOME

Within 12 months, the CPG manufacturer achieved substantial improvements in its security posture. The streamlined vulnerability management approach enabled the company to maintain a consistent security standard across regions, reducing operational risks and enhancing compliance.

Streamline OT Patching

Patching in OT environments is complex and often delayed due to safety concerns, manual tracking, and compatibility checks. Effective patch management reduces vulnerabilities, enhances compliance, and minimizes manual workload.

The Verve Difference

Verve's patch management integrates discovery, prioritization, and deployment in a single platform, enabling automated, OT-safe patching without relying on complex manual processes.

Automated Patch Identification:

Identifies missing patches and filters by relevance to specific OT assets.

Flexible Deployment Options:

Schedules and deploys patches with rollback capabilities and options to disable services if a patch isn't supported.

Integrated Change Management:

Verifies and documents all patching actions, including pre-patch backups and post-patch changes.



Lower Labor Costs:

Automates patch discovery, evaluation, and deployment, reducing the need for manual tracking.



Faster Remediation:

Prioritizes and deploys patches efficiently, shortening mean-time-to-remediate.



Simplified Compliance:

Centralized tracking and reporting make it easier to document patch status across assets.

Case Study I

Patch Management

One of Verve's clients, a small energy provider regulated under NERC CIP standards, was spending nearly 40 hours each month manually managing patches across their OT systems. With a limited team and stringent compliance requirements, this process was both exhausting and time-consuming, leaving them constantly scrambling to meet federal standards. The team needed a solution that would not only help them stay compliant but also alleviate the heavy workload on their already stretched resources.

APPROACH



Automated Patch Identification and Collection:

Verve's platform took over the heavy lifting of patch management, automatically spotting missing patches and handling the analysis, file collection, and pre-staging needed for deployment. With Verve managing these steps, the team no longer had to track patches manually or prepare files one-by-one, freeing them up to concentrate on higher-priority tasks while Verve readied patches in the background.



Controlled, Compliant Deployment:

With Verve, the team could safely roll out patches during scheduled maintenance, zeroing in on the critical updates that mattered most for their core systems. Each patch deployment was verified in real time, helping them stay confidently in line with NERC CIP compliance without a hitch or disruption to their day-to-day operations.

OUTCOME

With Verve's automated patching process, the client reduced their patching effort from 40 hours per month to just 12, achieving a 70% time savings. This streamlined approach allowed the client to maintain NERC CIP compliance with fewer resources and focus on other critical tasks while mitigating security risks across their OT environment.

Enhance OT Security with Configuration Management

In OT/ICS environments, many systems lack secure configurations by default, leading to increased risks. Effective configuration management reduces vulnerabilities, achieves compliance, and helps prevent unauthorized changes that could disrupt operations.

The Verve Difference

Verve's platform offers deep, OT-specific configuration management that combines visibility, automated checks, and integrated response, securing devices in a single, user-friendly interface.

Comprehensive Visibility: Tracks configuration settings across all OT assets, providing in-depth insights into both IT-based and embedded OT devices.

Automated Compliance Checks: Verifies configurations against industry standards, allowing proactive adjustments to reduce risk.

Closed-Loop Remediation: Enables immediate action on insecure configurations directly from the Verve console, minimizing time-to-remediation.



Improved Security Posture:

Identifies and corrects insecure settings across devices, from PLCs to protective relays.



Streamlined Compliance:

Monitors configurations against standards like DISA STIG and OT-specific guidelines, ensuring regulatory alignment.



Rapid Response to Changes:

Real-time alerts on configuration modifications help prevent potential security or operational issues.

Case Study I Configuration Management

A large U.S.-based power generation company needed to improve its OT security by ensuring consistent and secure configurations across various assets, including critical infrastructure systems. With regulatory pressures and the complex nature of OT environments, the company sought a solution that could manage and monitor configuration settings to help prevent security gaps and misconfigurations.

APPROACH



Centralized Configuration Oversight:

Verve's Security Center provided a centralized platform to monitor and enforce secure configuration baselines across all OT assets. This allowed the company to maintain control over configurations in a scalable, efficient manner.



Automated Compliance Checks and Change Detection:

Verve's platform continuously checked configurations against regulatory and company-defined standards, detecting unauthorized changes in real time and alerting the team to deviations from secure setting.

OUTCOME

With Verve, the power company achieved consistent, secure configurations across critical systems, reducing misconfiguration risks and improving regulatory compliance. The centralized oversight and automated compliance checks saved time and enhanced the reliability of their OT security posture.

Tailored OT SIEM

Traditional SIEM tools lack the specialized capabilities to detect and respond to process-specific threats. A targeted OT SIEM integrates process data and device performance metrics, allowing for more effective threat detection and response.

The Verve Difference

Verve's OT SIEM combines endpoint data with process-level insights, providing true OT-specific security intelligence. The integrated platform enables real-time alerting, investigation, and immediate response actions—all from one interface.

Endpoint-Focused Data Collection:

Directly gathers logs, syslogs, and NetFlow data from OT assets, enabling detailed host-level analysis.

Integrated Process Alarms:

Incorporates DCS/ICS alarm data, enhancing context for accurate threat detection and response.

Advanced Analytics:

Machine learning identifies anomalous patterns and tracks incident timelines, supporting forensic analysis.



Enhanced Threat Detection:

Combines logs, process alarms, and endpoint data for comprehensive threat visibility.



Faster Incident Response:

Integrated response actions within Verve reduce mean time to remediate threats.



Improved Compliance: Built-in detections for frameworks like MITRE ATT&CK and NERC CIP streamline regulatory reporting.

Case Study I

OT SIEM

A top 10 North American oil and gas producer needed a way to monitor its highly segmented, complex OT network for potential threats in real time. With a mix of different OEM systems and numerous NAT routers and subnets, the client required an OT-specific SIEM solution that could integrate with their existing infrastructure without disrupting operations.

APPROACH



Integrated OT Data Collection and Analysis:

Verve's SIEM aggregated data from various OT sources, including syslogs, alarms, and network activity logs across multiple OEM systems, providing a holistic view of security events. This comprehensive data ingestion allowed for detailed threat analysis within the OT environment.



Automated Compliance Checks and Change Detection:

Verve's SIEM provided continuous monitoring and alerted the team to suspicious behavior, such as unauthorized access attempts or unusual activity, enabling rapid response to potential threats.

OUTCOME

Within 6 months, the oil and gas company significantly improved its real-time monitoring and response capabilities. The Verve SIEM helped them detect, prioritize, and act on critical threats across the network, reducing response times and strengthening their overall OT security posture.

Secure OT Environments with Account Management

Unmanaged user accounts pose significant security risks, especially in systems designed without stringent access controls. Effective account management reduces unauthorized access, enforces compliance, and secures critical assets.

The Verve Difference

Verve's platform integrates OT-specific account management with security controls, providing full visibility and control over user access across critical systems. This enhances compliance and reduces the risk of unauthorized access.

Comprehensive Access Controls:

Enforces least-privilege access, confirming users have only the permissions necessary for their roles.

Centralized User Management:

Tracks and manages accounts across OT environments, simplifying account provisioning and deactivation.

Real-Time Alerts:

Automated notifications for new accounts, permission changes, or unauthorized access attempts enable rapid response.



Reduced Insider Threats:

Enforces access controls, minimizing unauthorized access across OT systems.



Streamlined Compliance:

Centralized tracking sustains compliance with regulatory standards for account management and audit requirements.



Enhanced Security Posture:

Regular monitoring and immediate alerts for changes in user accounts help prevent potential misuse.

Case Study I

Account Management

At a large Canadian oil sands refinery, a routine security review revealed a critical yet often-overlooked vulnerability—dozens of dormant administrative accounts lingering in their OT environment. Many of these accounts, created for temporary contractors or former employees, still had elevated access privileges, providing potential backdoors into critical systems. In complex OT environments like this, it's all too easy for dormant accounts to accumulate, especially with high turnover and decentralized management processes. Each forgotten account represented an unchecked access point, heightening the risk of unauthorized entry and underscoring the need for proactive, ongoing account management.

APPROACH



Identifying Dormant Accounts:

Verve's platform quickly flagged the inactive administrative accounts, bringing immediate visibility to this overlooked risk and allowing the refinery to take swift action to deactivate them.



Improving Access Review and Tracking:

With insights provided by Verve, the refinery adjusted its account tracking and review processes, establishing a proactive, regular review protocol. This change enabled more rigorous oversight, helping prevent similar issues from arising in the future.

OUTCOME

Powered by Verve's insights, the refinery minimized a major security gap, significantly reducing potential access points for unauthorized entry. The refinery's updated account management approach now includes continuous monitoring, confirming only authorized users have access to critical OT systems.

Strengthen OT Security with Hardening Solutions

OT environments, especially legacy systems, are often “insecure by design.” Effective system hardening reduces the attack surface, securing endpoints and networks against unauthorized access and minimizing operational risks.

The Verve Difference

Verve’s all-in-one platform combines OT-specific hardening with automated tools, delivering secure configurations and minimal operational impact. Our approach leverages a “Think Global, Act Local” model for scalable, efficient analysis and tuning.

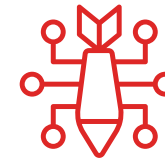
Comprehensive Hardening Tools:

Automates patching, configuration, anti-malware, and access control across all OT assets.

Network Segmentation and Secure Configuration:

Enforces segmentation, restricts ports/services, and updates policies to limit vulnerabilities.

Automated Management: Centralized platform providing a turnkey solution for reliable and consistent hardening.



Reduced Attack Surface:

Implements secure configurations, removes unnecessary services, and enforces access controls across devices.



Enhanced Operational Security:

Segments networks and applies anti-malware and allowlisting, helping protect critical systems from disruptions.



Lower Cost and Complexity:

Integrated approach reduces the need for multiple vendors, streamlining deployment and reducing risk of error.

Case Study I

System Hardening

Verve has established itself as a trusted provider for proactive system and network hardening, validated by the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA). Verve's inclusion on the DHS Continuous Diagnostics and Mitigation (CDM) Approved Products List (APL), along with its unique third-party validation, underscores Verve's alignment with rigorous federal cybersecurity expectations.

APPROACH



Comprehensive Hardening Aligned with Federal Standards:

Verve's platform was recognized for addressing critical CDM areas—Hardware Asset Management (HWAM), Software Asset Management (SWAM), Configuration Settings Management (CSM), and Vulnerability Management (VUL). These capabilities meet CISA's stringent standards, providing federal entities with the tools needed for real-time diagnostics and secure network segmentation.



Validated by DHS and Third-Party Evaluation:

Verve's platform not only met the CDM criteria but exceeded expectations through a thorough third-party evaluation. This sets Verve apart as one of the few OT cybersecurity providers capable of achieving and maintaining federal compliance standards for critical infrastructure.

OUTCOME

This recognition by DHS reinforces Verve's role as a proactive cybersecurity partner for the federal government, delivering continuous diagnostics, vulnerability management, and secure asset configurations for critical OT environments.