framatome cybersecurity

Sentrigard Patch

Streamline patch management to focus on your priorities

Enhance flexibility, adaptability, and security in complex Industrial Critical System (ICS) environments.

Challenge

Despite the importance of patch management for OT cybersecurity, some industrial companies are reluctant to implement it due to the challenges of little downtime, complex system architecture, thousands of assets and vendors, and high security and safety standards. However, the risks of not patching are high. Unpatched systems are vulnerable to cyberattacks, which can lead to data breaches, operational disruptions, and physical damage.

Solution

Increase visibility into your patch status across your environment from a single management point, ensuring compliance with company-specific and regulatory requirements. Sentrigard Patch is an on-premise platform that simplifies patch distribution, orchestration, and deployment for IT and OT assets using industry-proven automation tools.

Sentrigard supports both agentless and agent-based deployment, offering manual, semi-automated, and fully automated installation options. It provides granular control over installations and reboots, including end-user notifications and optional delay windows, ensuring smooth integration and minimal disruption

Customer benefits

- **Simplify internal distribution** Streamline patch deployment by simplifying the process of integrating, verifying, and distributing patches to your OT environment.
- **Align with vendor approvals:** Minimize the risk of unexpected issues, poor performance, and downtime by using our customizable patch deployment policy templates to deploy only OEM-approved patches.
- **Minimize manual processes:** Save time by avoiding manual, one-by-one patching with efficient bulk operations. Customize deployment schedules and installation behaviors to align with your operational needs.
- **Reduce operational friction:** Schedule deployments during maintenance windows to reduce disruption. Configure automation to align with risk tolerance and system needs for a seamless user experience.

Your performance
is **our** everyday **commitment**

Technical Highlights

- **Adaptable to your needs:** Our solution offers flexibility for various deployment models, from single servers to large fleets.
- **Increase Patch Status Visability:** Leverage the fully integrated reporting engine of our platform to attain patch status information
- **Extensive Patch Catalog support:** enabling quick and easy updates:
  - Operating systems
  - Software libraries and component frameworks
  - Application software
  - OEM vendor approved patches
  - Custom / proprietary applications

Key figures

80% of companies that experienced a breach or failed security audit could have avoided it by keeping their operating systems up to date.

Microsoft, 2023.

90% of OT cyberattacks are successful.

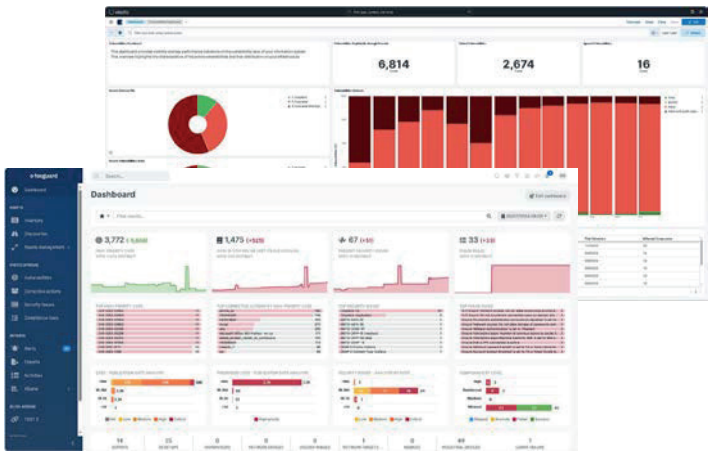
OT Security: The State of Play by SecurityScorecard

Contact: cyber-services@framatome.com
https://framatomecybersecurity.com/

framatome cybersecurity

Vulnerability & Compliance Management Software

Discover a simple and complete platform to improve your cybersecurity posture



Challenge

With over 80 new vulnerabilities emerging daily, risk prioritization is a critical challenge for IT and OT security teams. It's not just about identifying alerts but determining which ones require immediate action.

Solution

From detection to remediation, manage all your vulnerabilities and enhance your cybersecurity posture.

Identify: Consolidate your asset inventory through various passive and active collection techniques ensuring a complete overview of your ICS assets with our advanced hybrid approach.
Prioritize: Our innovative 3D prioritization technology provides a list of the most vulnerable assets in your context andsends targeted alerts.
Remediate: Using prioritization inputs, our advanced risk exposure dashboards help you select the adapted remediation, whether it's mitigation or patching considering your business constraints.
Monitor Compliance: Ensure asset configuration remains compliant with your defined cyber standards and system hardening guidelines through our integrated compliance module.

Maintain data privacy and sovereignty. Our platform ensures that sensitive information, such as asset details, vulnerabilities, and missing patches, stays on your premises.

Technical Highlights

Cyberwatch covers the following scope:

- Desktops: PCs,Laptops
- Servers: Virtual Machines, Physical Machines, Hypervisors, Mainframes
- Network devices: Routers, Switches, Firewalls
- Cloud & Containers: Docker, Kubernetes, Azure, AWS, GCP
- Web applications: URLs, IP addresses
- Industrial devices: Firmwares
- Software libraries: Development modules

Customer benefits

- **Gain 100% visibility** by consolidating your asset inventory into one platform
- Manage the entire lifecycle of vulnerabilities from detection to remediation, **all within the same platform**
- **Use a unified cross platform** to support patch management
- Deploy and **integrate with flexibility** whether on-premise, self-hosted or in the cloud
- **Generate customizable operational reports** with pre-built and modifiable templates
- Ergonomic and **easy-to-use** interface

Key figures

$3.8 million is the average cost of a data breach in an OT environment.

IBM

Only **30%** of organizations are fully compliant with OT cybersecurity standards.

Ponemon Institute

Your performance
is **our** everyday **commitment**

Contact: cyber-services@framatome.com
https://framatomecybersecurity.com/

framatome cybersecurity

Patch Management PAR/PBA

Boost remediation efficiency with patch intelligence

We are a one-stop shop to define, source, integrate, and deploy solutions specific to standards and cybersecurity frameworks within OT environments.

Challenge

Vulnerabilities in critical infrastructure and industrial systems present significant risks, including safety incidents, production downtime, and ransomware attacks. Prompt and effective remediation is crucial.

Solution

Our scalable patch intelligence and acquisition solutions help you quickly identify and address vulnerabilities, improving your patch management and reducing time to remediation.

Technical Highlights

- **Detailed Intelligence Information:** have the detailed patch information you need in one place to make informed decisions right at your fingertips.
- **Evidence to support the data at each step along the way:** including your internal and external regulatory audit requirements, patch authenticity review and integrity verification on every patch we supply.
- **Multiple Delivery Formats:** including human-readable and machine-readable datasets, for easy integration with your enterprise systems. We deliver consistent, structured data and binary files to simplify import into your tools and support standard integrations with popular platforms.
- **Diverse Asset Catalog support:** take the complexity out of the equation with a consistent, structured approach to shield you from many of these intricacies.

Customer benefits

- **Save valuable time and resources** by emiminating the hassle of checking multiple sources for new patches
- **Enrich existing processes** with our detailed information and content, enabling faster and more efficient decision-making and remediation
- **Feel confident** that you have clear visibility to all security related patches for your assets, including those not listed with CVE identifiers
- **Ensure compliance** with your OEM vendors' approved patch lists for your OT assets
- **Streamline your compliance efforts** with our proven solution, which provides all the information and documentation needed to effectively meet internal and external regulations, such as NERC-CIP

Key figures

90% of OT cyberattacks are successful

OT Security: The State of Play by SecurityScorecard

17% of industrial organizations have a mature and systematic approach to patch management.

SANS Institute Industrial Control Systems Security Survey

Your performance
is **our** everyday **commitment**

Contact: cyber-services@framatome.com
https://framatomecybersecurity.com/