

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.

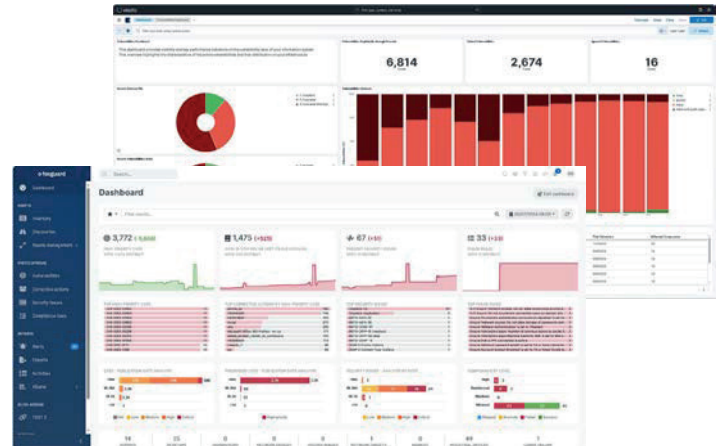
Identify: Consolidate your asset inventory through various passive and active collection techniques ensuring a complete overview of your ICS assets with our advanced hybrid approach.

Prioritize: Our innovative 3D prioritization technology provides a list of the most vulnerable assets in your context and sends 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

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

The data and information contained herein are provided solely for illustration and informational purposes and create no legal obligations by Framatome. None of the information or data is intended by Framatome to be a representation or a warranty of any kind, expressed or implied, and Framatome assumes no liability for the use of or reliance on any information or data disclosed in this document. Property of Framatome or its affiliates.

© 2024 Framatome. All rights reserved.

Your performance
is our everyday **commitment**