ÆGIS
TRUST THE EDGE

INDUSTRIAL-GRADE CYBERSECURITY FOR OPERATIONAL ENVIRONMENTS

OVERVIEW

To protect industrial environments from cyber threats and maintain uninterrupted access to essential OT systems, organizations must adopt and uphold an expanding set of critical security measures. Yet, as these requirements grow in scope and complexity, constrained budgets and limited personnel make it increasingly challenging to keep up.

CYBER THREATS IN OT

Over the past year, **77% of organizations experienced a successful cyberattack** that either compromised sensitive data or disrupted OT operations. Alarmingly, **62% of these incidents went undetected for over a month,** and the average time required to fully recover was nearly seven months. In nearly a quarter of the cases, these breaches led to a **complete halt of operational workflows.**

The manufacturing sector has been particularly affected, with a **71% increase in cyberattacks** recorded between 2024 and the first quarter of 2025. Researchers identified **29 active threat** actors targeting this sector, the vast majority of which were organized **cybercriminal groups (79%)**, with **45% linked to ransomware operations** specifically aimed at industrial control systems.

Adding to the concern, **nearly 70,000 OT devices** worldwide, including PLCs, HMIs, and remote access interfaces, are currently **exposed to the public internet.** Many of these devices are running **outdated firmware,** reveal critical **system information,** and lack basic protections, making them highly vulnerable to exploitation by malicious actors.

CHALLENGES

Organizations today face an escalating landscape of sophisticated and constantly shifting cyber threats. While deploying security controls is essential, it is merely a starting point. As threats evolve, so too must the tools and strategies used to defend against them. This requires continuous tuning, monitoring, and proactive management of cybersecurity systems, a task that overwhelms many security teams struggling with limited time, resources, and specialized expertise. In this context, many companies are confronted with a difficult dilemma: either commit substantial investment into building and maintaining a comprehensive cybersecurity program, or risk falling behind, exposing their critical systems to growing threats and regulatory consequences.

Organizations today face an escalating landscape of sophisticated and constantly shifting cyber threats. While deploying security controls is essential, it is merely a starting point. As threats evolve, so too must the tools and strategies used to defend against them. This requires continuous tuning, monitoring, and proactive management of cybersecurity systems, a task that overwhelms many security teams struggling with limited time, resources, and specialized expertise. In this context, many companies are confronted with a difficult dilemma: either commit substantial investment into building and maintaining a comprehensive cybersecurity program, or risk falling behind, exposing their critical systems to growing threats and regulatory consequences.

INTELLIGENCE & STRATEGY

Understand before you defend

- Risk Assessments
- Security Audits
- Compliance Mapping
- Threat Modeling
- Gap Analysis
- Architecture Design
- Policy Review
- Maturity Scoring
- Roadmap Planning
- Executive Reporting

TECHNOLOGY & AUTOMATION

Equip your infrastructure with smart defense

- Antivirus & EDR
- SIEM Integration
- Vulnerability Scanning
- Zero Trust Access
- MFA Enforcement
- Segmentation
- Network Monitoring
- Firewalling
- Device Control
- Analytics Dashboads

UNIFIED.
SCALABLE.
TRUSTED.

MANAGED & PROFESSIONAL SERVICES

Deliver protection continuously

- 24/7 Monitoring
- Incident Response
- Secure Patch Management
- Asset Discovery
- User Awareness Training
- Managed Backup
- DR Testing

Three lintegrated pillars. One powerful cybersecurity ecosistem: ÆGIS delivers security that scales with your ambition.

ADVANTAGES

ÆGIS offers you a next-generation platform with the following core strengths:

Broad and Adaptive Coverage

Seamlessly integrates with a wide variety of operating systems and is specifically refined for industrial control and OT environments.

Designed for Real-World OT Systems

Built to align with complex OT ecosystems used in power generation and critical infrastructure.

Intelligent Automation

Streamlines operational security through automated patching, enforcement of configuration policies, scheduled backups, and more, reducing manual effort and errors.

Pre-Integrated and Ready to Deploy

Delivers a set of fully tested, fine-tuned applications, services, hardware, and configuration elements, minimizing deployment times and complexity.

Modular Scalability and Future Readiness

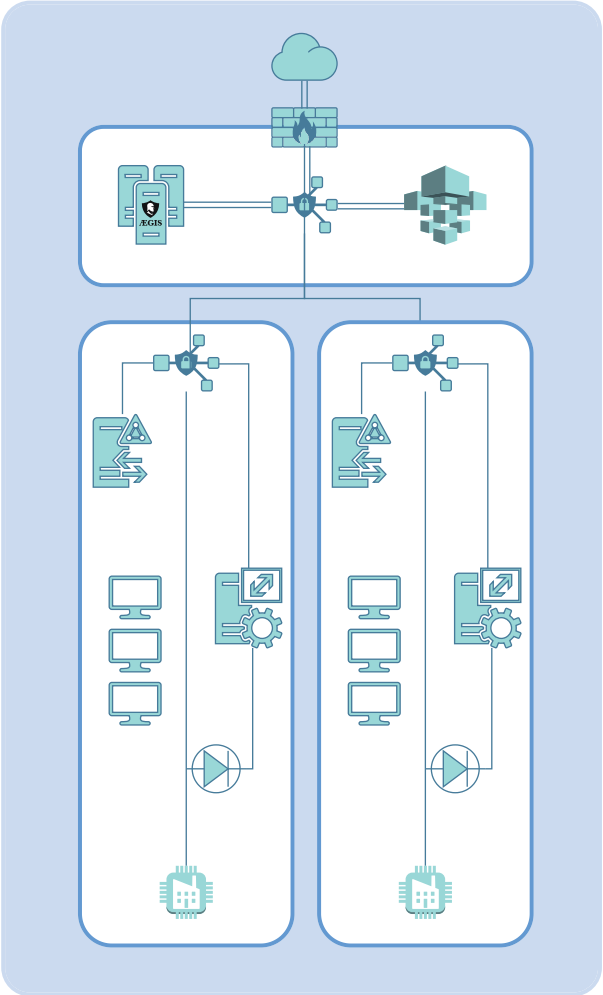
Enables organizations to scale their security posture over time thanks to a flexible, modular architecture. Supports integration with SOC environments and accommodates the evolution of future technologies with ease.

SOLUTION

ÆGIS delivers a fully integrated cybersecurity platform that empowers industrial organizations to implement robust, defense-in-depth protection across their operational environments.

By consolidating essential security functions into a single, ready-to-deploy solution, ÆGIS eliminates the complexity, time, and cost typically associated with assembling and integrating disparate tools and technologies.

The platform provides native support for a wide range of OT systems, including PLCs, DCSs, and industrial controllers, offering centralized tools for both cybersecurity enforcement and operational maintenance.



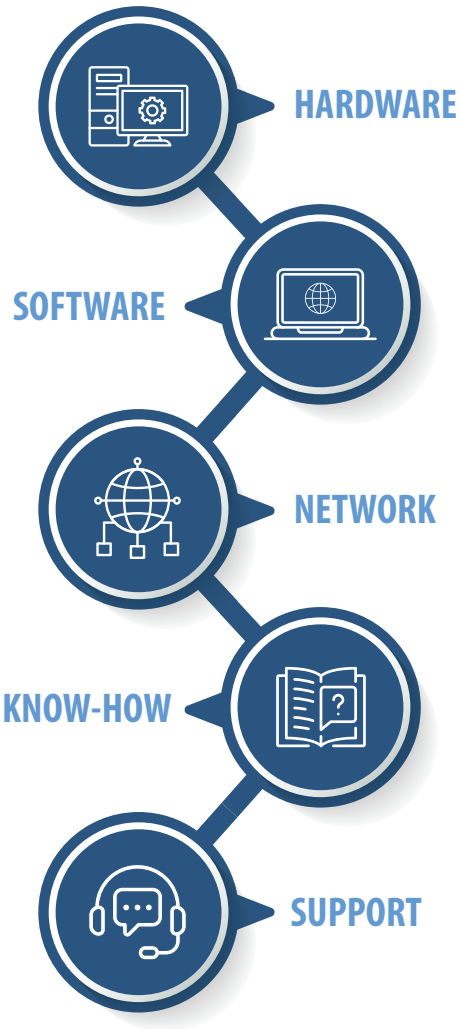
ÆGIS simplifies security operations by collecting, correlating, and presenting logs and events in an intuitive, actionable format. It includes built-in features for identity and password management, and can be seamlessly integrated into your existing ecosystem, including SIEM platforms, antivirus solutions, backup infrastructures, and log management systems.

CORE COMPONENTS OF THE ÆGIS PLATFORM

» Secure hardware appliance and operations console
» Hardened server infrastructure with thin-client access
» Optional industrial-grade firewall
» Secure-by-design architecture
» Support for international certifications and compliant hardware

In addition to its core platform, ÆGIS includes a full suite of integrated applications and services for:
» Access control
» Centralized patch management
» Log aggregation and threat correlation
» Vulnerability reporting

All deployments are supported end-to-end by Sysware's professional services, including planning, configuration, asset integration, and ongoing technical support.



KEY BENEFITS OF THE ÆGIS PLATFORM

Implementing the ÆGIS platform allows your organization to unlock immediate and long-term value across operational and cybersecurity domains. Here's how:

Reduce Operational Overhead

ÆGIS consolidates a broad set of cybersecurity tools, including patch management, anti-malware, backup and recovery, and identity services, into a single, unified platform.
This eliminates the need to source, integrate, and manage multiple solutions separately, reducing both complexity and cost. Automation and advanced orchestration features further streamline routine tasks, helping your teams operate more efficiently with fewer resources.

Strengthen Cyber Risk Posture

Gain real-time visibility into the health and security of your OT environment. ÆGIS enables the rapid implementation of comprehensive security controls designed to prevent cyber attacks and avoid compliance failures.
The platform helps your organization align with key cybersecurity standards such as IEC 62443, NERC CIP, and NEI 08-09, simplifying adherence to regulatory frameworks.

Enhance System Availability

ÆGIS ensures that security does not come at the expense of operational continuity. The platform supports the deployment of governance processes and maintenance strategies that safeguard critical assets while aligning with production requirements.
Security measures are implemented in harmony with plant operations, protecting uptime as well as infrastructure.

KEY CAPABILITIES

Identity & Access Governance

ÆGIS provides centralized identity and access control tailored for OT environments, allowing you to enforce least-privilege principles for both local and remote users. It enables secure credential policies, including complex password enforcement and default credential blocking. Role-based access control (RBAC) ensures users only interact with the systems and data relevant to their roles. The platform supports certificate-based authentication and encrypted communication between HMIs and field controllers, securing access even across segmented networks. These controls support regulatory compliance while reducing insider threats and operational risk.

Advanced Malware Defense

The platform integrates antivirus protection with dynamic signature updates and behavioral monitoring to detect, block, and quarantine malware across endpoints. Application allow-listing restricts execution to only trusted programs, preventing unauthorized or rogue software from compromising critical systems. This multi-layered approach enhances system integrity without impacting performance. Whether on engineering workstations or HMIs, ÆGIS ensures that only verified software runs, improving reliability and reducing operational disruptions caused by malware infections or unauthorized changes.

Secure System Configuration

ÆGIS strengthens system resilience through hardware and software hardening. The platform includes a secure-by-design appliance with protective casing, mounting hardware, and port blockers to prevent physical tampering. On the software side, it enforces least-privileged access and monitors configuration changes across all managed assets. It automatically restores unauthorized modifications and provides agentless deployment for easier lifecycle management. These configuration controls help maintain a known-good state across the infrastructure and align with best practices from standards like IEC 62443.

Host-Level Intrusion Detection

For both Windows and Linux systems, ÆGIS integrates host intrusion detection capabilities including log monitoring, file integrity checks, rootkit scanning, and real-time alerting. The system captures unauthorized changes, failed login attempts, or abnormal activity directly at the endpoint. This deep visibility enables proactive threat response and ensures any compromise is detected before it can spread. The platform also supports automatic remediation workflows and seamless integration with central SIEM dashboards for full-spectrum situational awareness.

Backup & Rapid Recovery

ÆGIS automates backups of key configuration files and operational data, ensuring fast and reliable recovery in the event of system failure, malware compromise, or accidental misconfiguration. Its lightweight deployment model allows quick adaptation to diverse environments without the need for extensive infrastructure changes. Backup policies are centrally defined, executed on schedule, and can be restored in minutes, reducing downtime and preserving system continuity across OT infrastructures where availability is critical.

Centralized Log Intelligence

The platform features a built-in SIEM that aggregates logs from across your OT network, including Windows event logs, syslog sources, network devices, embedded systems, and applications. Logs are enriched, correlated, and presented through customizable dashboards that offer real-time visibility into system state, alarms, and trends. ÆGIS also supports forwarding logs to third-party SIEMs for broader analysis. This enables forensic investigation, compliance reporting, and rapid detection of anomalies, all from a centralized, operator-friendly interface.

Network Configuration Management

ÆGIS supports automated backup and restoration of network equipment configurations, including routers, switches, and firewalls. This ensures quick recovery in case of device failure, misconfiguration, or cyber incidents. Backups are securely stored and versioned, allowing rollback to known-good states. This feature reduces operational risk and downtime, while simplifying management in environments with limited IT resources. Combined with change detection and alerting, it supports governance and continuous protection of critical networking infrastructure.

Patch Validation & Delivery

The optional patch validation program ensures that operating system updates, antivirus definitions, and intrusion detection signatures are thoroughly tested before deployment. Updates are securely delivered through a dedicated portal as pre-packaged, scripted bundles, ensuring consistency and minimizing human error. ÆGIS supports centralized scheduling and deployment of these patches, allowing teams to remain current without risking operational disruption. This service is particularly valuable in OT environments, where change management is tightly controlled.

Controlled Remote Access

ÆGIS enforces secure remote access using a layered approach that includes Multi-Factor Authentication (MFA), VPNs, read-only modes, lockboxes for credential isolation, and unidirectional gateways (data diodes). Access policies are segmented by enforcement zones, enabling precise control over who can connect, when, and to what. These controls are essential in industrial contexts where external vendors and remote teams require limited, auditable access without compromising internal security boundaries or asset availability.

Application Control Whitelisting

Through application allow-listing, ÆGIS prevents unauthorized or malicious software from running on OT endpoints. The platform builds and maintains a trusted list of approved applications, blocking all other executables by default. This significantly reduces the attack surface, limits the spread of malware, and ensures that only operationally validated tools are used. It is particularly effective for securing HMIs, SCADA workstations, and engineering terminals where software consistency is key to safe operations.

Network Threat Detection

ÆGIS offers intrusion detection and prevention at the network layer, using customizable IDS/IPS engines that perform deep packet inspection (DPI), traffic analysis, and pattern-based attack recognition. Suspicious behavior, from lateral movement to port scanning, is logged, alerted, and can trigger automated responses. This provides real-time protection for control networks against external attacks and internal misuse, supporting proactive defense strategies and strengthening perimeter resilience.

Full Asset Visibility

The platform continuously scans the network to detect all connected devices and map data flows between them. It analyzes traffic patterns, inspects packet content (PCAP), and builds behavioral baselines that can later be used to detect anomalies. This comprehensive asset inventory and traffic understanding is critical for managing complex OT environments, identifying rogue devices, and maintaining network integrity over time.

Cyber Intelligence Reporting

ÆGIS provides periodic reports on vulnerability exposure, patch status, and security posture across all managed assets. These reports highlight outdated components, unpatched systems, and areas at elevated risk, enabling data-driven decision-making. Designed for both technical and management audiences, reports offer intuitive visualizations and actionable insights, supporting audit readiness, strategic planning, and continuous improvement of your cybersecurity program.

A FLEXIBLE PLATFORM, TAILORED TO YOUR NEEDS

The ÆGIS platform is available in three distinct editions, each designed to address the specific cybersecurity challenges of different industrial contexts, from small businesses to large-scale, multi-site operations.

ÆGIS Enterprise is a full-scale, turnkey solution that includes both hardware and software components. It provides centralized management, high-availability architecture, and comprehensive protection for complex OT environments spread across multiple facilities. Ideal for large industrial groups, it ensures seamless migration from legacy systems and supports regulatory compliance at scale.

ÆGIS Small Business is a compact yet powerful solution for smaller companies looking to enhance their cybersecurity posture without disrupting existing IT systems. Delivered as a single-server deployment, it integrates smoothly with current infrastructure and delivers enterprise-grade protection, including backup, antivirus, vulnerability management, and compliance reporting, in a simplified, cost-effective package.

ÆGIS Appliance offers maximum flexibility by delivering the full platform as a pre-configured virtual appliance, ready to be deployed on the client's existing hypervisor infrastructure (e.g., VMware ESXi). This edition is perfect for organizations that want to avoid hardware changes and prefer a modular, scalable implementation. All services are activated remotely, ensuring a fast, non-intrusive deployment.

EXPERT SERVICES AND A COMMITMENT TO EXCELLENCE

Deploying a cybersecurity platform in an operational technology (OT) environment demands more than just robust software, it requires expert guidance, seamless integration, and long-term reliability. The ÆGIS platform is not only a powerful cybersecurity solution, but also a fully supported system backed by a comprehensive service ecosystem designed to ensure success from day one.

Our team of specialists manages the full setup process within your environment, including installation, commissioning, and functional startup of all platform components, applications, and services. Every deployment is approached with precision, tailored to the specific requirements of your infrastructure, and executed in close collaboration with your technical team to ensure full alignment with your operational objectives.

To support operational autonomy, ÆGIS includes on-site training, during which your staff will become familiar with system operation, monitoring, and basic troubleshooting procedures. Additionally, detailed documentation is provided, covering architecture, configuration, maintenance, and response procedures, enabling structured governance and simplifying compliance reporting.

For organizations seeking additional assurance, optional Factory Acceptance Testing (FAT) is available to validate the configuration and performance of the platform prior to final deployment. Ongoing maintenance services can also be provided under tailored service agreements, ensuring that the platform remains continuously updated, supported, and responsive to the evolving threat landscape.

At Sysware, we are committed not only to delivering high-quality technologies, but also to building strong relationships grounded in trust, responsiveness, and expertise. Our support culture is deeply customer-centric: each team member is empowered to make quality and client satisfaction their top priority. With ÆGIS, you're not just adopting a solution, you're gaining a reliable partner dedicated to securing your critical operations.

ÆGIS
TRUST THE EDGE

aegis-ot.com

Information contained in this document is indicative. No representation or warranty is given or should be relied on. Information provided is subject to change without notice.
© 2025 SYSWARE and/or its affiliates. All rights reserved.