Aegir

A Cyber PARM EndPoint solution
powered by Arc4dia

Aegir is an endpoint defense capability originally engineered for national security. It was designed to protect military operations and critical infrastructure under conditions where compromise was not possible. The same standard is now extended to a select circle of private institutions, those whose stature and obligations require the highest level of assurance.

It is a system built to address the complexity of contemporary threats with precision, discretion, and resilience.

Beyond IT, **Aegir** provides corporate security leaders with a counterintelligence-grade capability: protecting not only systems and data, but also the integrity of executives, strategic operations, and sensitive environments. As part of an organization's broader security and risk framework, it becomes a discreet shield against the exploitation of metadata, targeted surveillance of business travel, and hybrid threats that combine cyber intrusion with reputational or geopolitical pressure.

PROVEN IN CRITICAL AND HIGH-SECURITY ENVIRONMENTS

Aegir operates in environments where demands are absolute and margins for error do not exist. It demonstrates its value daily across defense, government, and private-sector deployments of strategic importance.

- ➔ Validation of superior detection and containment across classified infrastructures.
- ➔ Recognition as a pragmatic and effective defense capability against advanced malware.
- ➔ Adoption as a trusted partner within multinational defense initiatives.
- ➔ Deployment within enterprises handling billions in sensitive assets and high-value transactions.

These references are ongoing. They represent active performance in environments defined by risk and complexity.

For corporate security executives, this means Aegir has already been validated in conditions where failure is not an option. It directly supports the duty of care for senior leadership, protection of sensitive negotiations, and the preservation of corporate legitimacy under pressure.

ProActive Risk Management
PARM

info@parminc.com - PARMINC.COM

ARCHITECTURE AND CORE CAPABILITIES

The architecture of **Aegir** is engineered for endurance, discretion, and operational clarity. It integrates seamlessly into complex infrastructures while maintaining minimal impact on performance.

■ Comprehensive Coverage

Operates across Windows, macOS, Linux, Android, ARM, MIPS, industrial controllers, point-of-sale systems, and IoT. Protection extends to legacy and specialized environments that adversaries target for their weaknesses.

■ Stealth by Design

Lightweight sensor deployment requires no reboots, introduces no operational friction, and remains undetectable to adversaries.

■ Real-Time Telemetry and Visibility

Continuous low-level telemetry is consolidated into a single, intuitive view. Analysts can reconstruct entire attack chains, trace lateral movements, and identify root causes within seconds.

■ Counterintelligence-Grade Detection

Advanced heuristics and anomaly analysis expose behaviors that diverge from legitimate system activity. This enables the detection of zero-days, bespoke malware, and long-term persistence.

■ Actionable Response

Threats can be neutralized instantly: compromised machines isolated, malicious processes terminated, persistence removed. Actions are precise and scalable to thousands of endpoints simultaneously.

■ Integration

Full-featured APIs connect with SIEM, SOAR, and custom workflows. **Aegir** augments existing infrastructure without disruption or replacement.

TECHNICAL FOUNDATIONS

Telemetry and Data Pipeline

- Multi-year storage of telemetry data enables historical analysis and long-term anomaly detection.
- Captures system calls, memory registers, process activity, network connections, and kernel events.
- Data streams are correlated in real time and modeled as behavioral graphs for each endpoint.

Detection and Analysis

- Signatureless approach based on behavioral deviation rather than external updates.
- Embedded statistical models distinguish legitimate from malicious activity across heterogeneous systems.
- Indicators of compromise are generated dynamically and propagated instantly across the protected estate.

Response and Containment

- Machine Isolation: endpoints can be isolated from the network while maintaining secure analyst access.
- Process Control: malicious processes are terminated without collateral disruption.
- Persistence Removal: registry entries, hidden files, and malicious services are eliminated.
- Forensic Snapshots: system states are captured for judicial or post-incident review without altering evidence.

Performance and Deployment

- Sensors consume minimal resources (a few MBs of memory, negligible CPU).
- No reboot is required for installation or update.
- Designed to scale from dozens to tens of thousands of endpoints.

Compliance and Governance

- Full audit trails of detections, analyst actions, and responses.
- Alignment with GDPR, ISO 27001, SOC2, and equivalent standards.
- Provides insurers and regulators with documented evidence of resilience and active defense.

OPERATIONAL IMPACT

Aegir changes the operational reality of cybersecurity inside complex organizations.

- **Time to Detection** – Intrusions that typically remain hidden for months are revealed within seconds.
- **Containment** – Actions that previously required days of coordination are executed in minutes.
- **Clarity** – Analysts are presented with complete context, eliminating noise and reducing dependency on manual correlation.
- **Continuity** – Operations continue without interruption, even during deployment or remediation.

STRATEGIC VALUE

For institutions where confidentiality, compliance, and trust define their position in the market, **Aegir** provides a level of assurance previously unavailable outside the national security domain.

- **Resilience** – Capabilities designed for adversaries operating at the highest levels.
- **Compliance** – Documentation and visibility that strengthen posture with regulators, insurers, and legal frameworks.
- **Discretion** – Silent protection that reinforces the confidence of boards, clients, and partners.
- **Longevity** – An architecture capable of adapting to emerging threat models without dependence on external updates.

Aegir represents the consolidation of national security–grade defense into an endpoint solution available to the private sector. It is a standard in itself, defined by precision, resilience, and discretion.

More than a cybersecurity product, **Aegir** is a strategic counterintelligence asset for corporate security leaders. It ensures that the protection of data, people, and decisions are aligned, turning endpoint defense into a cornerstone of organizational resilience and executive protection.

ProActive Risk Management

PARM

CONTACT US TO BUILD YOUR RESILIENCE PROGRAM

ProActive Risk Management (PARM) is a leading firm in risk management, intelligence, and security services. With an integrated approach and a team drawn from the highest levels of the security and intelligence community, PARM is the trusted partner of organizations that require discretion, resilience, and uncompromising standards.

info@parminc.com - PARMINC.COM