OS3™

Operational Security, Safety, and Standards Software

Cybersecurity Software for Secured Autonomous Platforms and Fleets

HIGHLIGHTS

- Continuous Runtime Protection
- Streamlined Integration
- Compliance Management
- Fleet Cybersecurity

Autonomous platforms face evolving cybersecurity threats that can compromise individual missions or spread across entire fleets. When cybersecurity fails, missions fail—often without warning. Some threats target individual platforms, while others exploit the systems that connect them all. A single vulnerability can ripple outward, jeopardizing not just one system, but every system it touches.

OS3™ is cybersecurity software that provides continuous runtime protection for autonomous platforms and fleets—two pillars of Mobilicom's Secured Autonomy™ framework. Unlike external defenses, OS3 integrates directly into the autonomy stack, removing complexity while delivering real-time threat detection across host, network, and application layers.

Built on more than a decade of experience safeguarding defense fleets through battle-tested innovations, OS3 provides fleet cybersecurity with unified policy enforcement and automated threat containment. It transforms compliance from a burden into confidence, meeting accelerating regulatory demands while ensuring mission resiliency under the most demanding conditions.

WHAT IS SECURED AUTONOMY?

Mobilicom's Secured Autonomy framework protects uncrewed systems across three pillars: Secured Autonomous Platforms, Secured Autonomous Fleets, and Secured Communications & EW Protection. Together, these pillars deliver end-to-end resilience for drones and robotics.

OS3 provides the cybersecurity foundation for the first two pillars, keeping autonomy secure, operational, and trusted. With multi-layer protection across host, network, and application levels, OS3 reduces compliance risks and strengthens mission reliability for drones and robotics. Visit securedautonomy.com to learn

KEY BENEFITS

Proactive Threat Detection & Response
Real-time identification and neutralization of cyber threats through continuous monitoring and autonomous response systems that minimize downtime and enable swift recovery.

Strengthened System Integrity
Prevention of unauthorized access, malware insertion, and system tampering through secure boot, process monitoring, and platform integrity protection across diverse threat surfaces.

Mission Continuity
Stable operations under cyber threat through layered defenses across host, network, and application layers with precision performance for mission computers.

Fleet Cybersecurity
Extended protection across connected fleets through unified policy enforcement, automated isolation, and tamper-resistant logging that prevents lateral spread and maintains compliance.

Streamlined Integration
Accelerated deployment and reduced complexity through pre-integrated partnerships with mission computer and autonomy solution providers, or direct licensing options.

Compliance Confidence
Streamlined regulatory alignment through automated reporting and secure tamper-resistant logs that meet NIST 800-53, live hack tests, SBOM delivery, 24-hour patch plans, and Europe's Cyber Resilience Act requirements.

OS3 SOLUTION COMPONENTS

OS3 Edge
Runs on the mission computer, enforcing secure boot, protecting file integrity, monitoring processes, controlling applications, and logging activity in real time.

OS3 Controller
Operates at the ground control station, enrolling devices, managing configurations, raising alarms, and enabling secure log access for operators.

OS3 Cloud
Secures uncrewed fleets, delivering real-time oversight, unified policy enforcement, automated isolation, compliance monitoring, and tamper-resistant fleet logging.

KEY FEATURES

Host Security	Real-Time Reporting • Real-Time System security health reporting with secured API Platform Integrity • Prevents modification of OEM files Secured Logger • Embedded logging module with self-protection File System Encryption • Sensitive data secured against tampering and access Process Monitoring • Detects anomalies and initiates corrective actions Root Access Monitoring • Prevents unauthorized system changes System Hardening • Reduces OS vulnerabilities against attack
Network Security	Stateful Firewall • Controls traffic, allowing only authorized communications Intrusion Detection and Prevention • Detects threats early, enacts countermeasures Secure Communication Protocols • Protects in-transit data from tampering Protocol Enforcement • Eliminates attacks from manipulated protocols
Application Security	Application Behavior Enforcement • Blocks unauthorized manipulation of system operations Behavior Monitoring • Detects deviations and breaches in application processes Application Shield • Secures OEM applications from malicious attacks

KEY FEATURES (CONTINUED)

Fleet Security	Fleet-wide Configuration Enforcement • One source of truth across all nodes Unified Policy Orchestration & API Hardening • Protects orchestration and GCS paths with secure cloud APIs and access control Automated Isolation / Containment • Quarantines compromised nodes instantly to prevent lateral spread Real-Time Fleet Health Monitoring • Live risk visibility with alerts for drift, anomalies, and misconfigurations Swarm and Coordination Integrity • Runtime validation of mission logic and task execution Centralized, Tamper-Resistant Logging • Fleet-wide audit and forensic assurance—even when units operate offline Automated Compliance Reporting • Supports procurement and regulatory alignment

Whether you're looking to license OS3 directly or partner with us to deliver integrated cybersecurity solutions, contact us to discuss how OS3 can secure your autonomous systems.

Contact us:

sales@mobilicom.com
www.mobilicom.com
securedautonomy.com

For more information:

https://mobilicom.com/os-platform/

MOBILICOM