Simplesense®

simplesense.io/platform | 1.718.618.4939 | hello@simplesense.io

Outpace Cyber Threats

Simplesense OTGateway 2.0

Leveraging open source technology and industry best practices, the Simplesense OTGateway creates a secure foundation for your installation. Automated deployment, long term support, segmentation and encryption at the facility level with FIPS-compliance reduces attack surfaces and increases resilience.

Zero Trust

Hardened to support Department of Defense programs and meet Zero Trust and FIPS 140-3 requirements with OS security patches guaranteed through 2032.

Low Maintenance

Leverage fanless hardware and automated provisioning and updating with little to no on-site expertise needed. Dynamic routing further increases scalability and decreases maintenance.

High Availability

Upgrade the OS with Over the Air (OTA) updates with A/B deployments that failover with automated rollback to ensure zero downtime.

Siemens Simatic IPC227G

The OTGateway relies on the Siemens Simatic Industrial PC (IPC) hardware line. Manufactured in Ohio and fully TAA compliant, Siemens Simatic IPC 227G is compact and maintenance-free, providing the highest industry functionality for flexible deployment in harsh conditions at temperatures up to 55 °C.

Key features include:

- Small footprint and mounting flexibility
- Rugged design with sealed, fanless metal enclosure maintenance-free, continuous operation
- Designed for 24/7 continuous operation at up to 55°C ambient temperature and high vibration/shock requirements
- High-performance and energy-efficient dual-core and quad-core Intel® Celeron® processors
- A variety of interfaces and configuration options (4 x USB 3.1, 3 x Gbit Ethernet, RS232/RS485/RS422, M.2 Solid-State-Drive (SSD))
- Optimized for headless operation with LED for efficient self-diagnostics
- Long-term availability: Service & support period up to 11 years

What is the OTGateway?

The OTGateway leverages the latest open source operating system and automated deployment technology as well as industry best practices to reduce on-site time to a minimum, reduce maintenance time and costs, increase availability, and decrease overall attack surfaces following Zero Trust principles.

Core software components include:

- Ubuntu Pro 22.04 with security patches through 2032
- Mender Over-the-Air (OTA) software updates and Metal-as-a-Service (MaaS) provisioning
- Advanced networking with built-in firewall for filtering traffic and dynamic routing to minimize configuration and maintenance costs and maximize scalability
- Integrated with Simplesense DevicePilot asset management and SecuritySphere continuous monitoring tools

Ubuntu Pro

10 years of vulnerability management for critical, high and selected medium CVEs for all Ubuntu software packages

Average 24 hours to fix Critical CVE vulnerabilities versus industry average of 98 days

1,800+ additional Ubuntu Pro high and critical patches

10 years of maintenance for the whole stack

Hardened to meet the latest DISA-STIG and FIPS compliance requirements.

MENDER by Northern.tech

Over-the-Air Software Updates for IoT Devices

Update without the risk of bricking devices. Robust in the face of limited bandwidth, unstable connectivity or power loss. Secure and verified to standards, at every step.

End-to-end security: Mender's security-by-design principle ensures each step is verified and authorized. Keep your devices secured and compliant with corporate IoT security standards.

Avoid lock-in: Mender's focus on integration, not platform, as well as our Open Source edition means you are never locked-in to a single provider.