PLANTFORMANCE CASE STUDY · SECURITY AND INFRASTRUCTURE

Zero-trust OT security with zero critical pen test findings

Plantformance · Cross-industry

Plantformance designs every customer-facing deployment security-first, with zero-trust networking, CISA Linux hardening, container isolation and multi-layer intrusion detection. Multiple independent penetration tests found zero critical issues.

THE PROBLEM

Factories need their OT environments connected to central management and cloud services. That connection is also an opening. Without security designed in from the start, it exposes plants to lateral-movement attacks, OS-level exploits and compliance gaps. Adding security after deployment rarely closes all of them. Flat networks, unhardened operating systems and shared processes stay in place, and one compromised component can become a path to everything else on the site.

HOW WE DID IT

Plantformance engineered every customer-facing deployment around a security-first, zero-trust architecture covering both the network and OS layers. Operating systems are hardened following CISA Linux hardening guidance. Processes run in strictly isolated containers, so services do not share an attack surface. Multi-layer OS intrusion detection and prevention watches for threats continuously. Security is part of the build from day one, not a layer added once the system is live. The same design applies at every managed client site.

BEFORE

Standard deployments often put fast delivery ahead of security by design. That left flat networks, unhardened operating systems and shared processes open to cross-process compromise.

AFTER

Even if a single container process is targeted, strict isolation stops the compromise from spreading to the host OS or other factory services, with continuous multi-layer threat detection behind it.

RESULTS

- Passed multiple independent penetration tests with zero critical findings
- Zero-trust OT/IT security applied across all managed client sites
- Container isolation contains a compromised process before it reaches the host OS
- Continuous multi-layer intrusion detection and prevention

Plantformance products and services: FactoryBrain

PLANT FORMANCE

NEXT STEP

Planning a project like this?

Talk to an Ignition engineer about your sites, timeline and architecture. We will tell you honestly what it takes.

Contact Plantformance

Read this case online and see more Ignition projects: plantformance.com/case-studies/zero-trust-ot-security-ignition · all case studies

---

Plantformance is an Inductive Automation Alliance Partner that helps enterprises deploy, secure, and scale Ignition across sites through plug-and-play modules, turnkey zero-maintenance HMI hardware, and 24/7 managed infrastructure.

plantformance.com
info@plantformance.com
Ennetbaden, Switzerland