Tripwire Industrial Visibility for the Automotive Sector

Automaker Drives Toward Comprehensive OT Security

As the scope of an auto manufacturer's operation grows, the complexity of its security requirements often increases exponentially. Struggling to gain a unified view into its operational technology (OT) security posture, this large automaker was seeking a vendor to provide comprehensive OT asset visibility offering. This discovery led to a host of other benefits that ultimately helped the company improve availability, reliability, and safety across its entire OT environment.

Challenges

The company—like many others in its industry—sought a way to view, monitor and manage the security of its numerous production sites, each consisting of hundreds of assets, in order to proactively strengthen its OT security and more effectively manage the inherent risks.

1. **Complex and diverse attack surface:** Automakers typically have numerous factories, usually spread across a large geographic area, each comprising a wide range of networked devices. This poses a particular challenge in finding a scalable but consistent approach to OT security because the technical requirements for OT devices differ considerably across use cases and vendors.

2. **Lack of production-related alerting:** OT security incidents are often difficult to detect until after they have already begun to impact production, which has a cascading effect on operations. Precise and automated alerting are necessary to allow staff to respond quickly and keep the plant operational.

Solution

After a comprehensive evaluation process, the underlying technology included in Tripwire® Industrial Visibilty was chosen and deployed across an automobile manufacturing operation spanning more than 40 factories across two continents.

Platform components utilized include:

» The underlying technology included in Tripwire Industrial Visibility Threat Detection Console for full-spectrum OT asset visibility, continuous security monitoring, and real-time risk insights with zero impact to operational processes and underlying devices.

» The underlying technology included in Tripwire Industrial Visibility Management Hub to simplify management overall, consolidating data from across the platform and providing a unified view of assets, activities, and alerts across multiple sites. The platform also integrates seamlessly via the Management Hub for IT security infrastructure, wherever appropriate.

Results

The underlying technology included in Tripwire Industrial Visibility immediately profiled all assets in the company's network and provided a depth and volume of detail on each asset that was unmatched by any other vendor evaluated. This process was achieved without disruption to operational processes.

By giving the company a unified view of all devices in the ecosystem, even legacy devices in use since before modern cybersecurity was a primary design consideration are identified, monitored and secured. This comprehensive OT visibility and real-time threat detection empowered the company to be proactive about protection against a much wider range of threats.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at** tripwire.com

The State of Security: **News, trends and insights at** tripwire.com/blog
Connect with us on LinkedIn, **Twitter and** Facebook