

Secure Patch Management and Compliance

Tripwire Integrated with FoxGuard Solutions

When it comes to compliance and security, efficient patch management is a critical capability. In order to be effective, patch management requires a closed-loop process for approval and reconciliation, especially in highly sensitive operational environments. Whether you are evaluating patches for security or operational purposes, Tripwire and FoxGuard integrate seamlessly for an innovative approach to patching within both IT and OT environments.

FoxGuard's Patch Analysis

FoxGuard Solutions provides an exceptional patch management capability, enabling evaluation and prioritization of available patches. Through thorough analysis of existing patches for software lists, FoxGuard validates and recommends critical patches necessary for their specific environment. With discussion of emerging trends, inadvisable updates and more, FoxGuard is a leader in secure patch management.

Achieving Compliance with Tripwire

Tripwire[®] Enterprise and Tripwire State Analyzer give users a full picture of the software installed on their devices, in addition to identifying and maintaining an ideal baseline configuration for each asset. This visibility enables you to capture the operational state of their devices while demonstrating compliance against required standards (PCI, NIST, NERC, or self-defined). By combining Tripwire Enterprise's visibility with the allowlisting capability of Tripwire State Analyzer, users can easily audit their environment for non-compliant objects such as open ports, routes, installed software, and users.

The Value of Partnership

By integrating Tripwire State Analyzer and FoxGuard, organizations can improve patching for both security and compliance. Tripwire begins the integration process by exporting data on existing software and sharing this information with FoxGuard. FoxGuard then analyzes the list of patches existing and available for installed software, providing insight into which patches are recommended and should be prioritized. Tripwire State Analyzer then provides an easy workflow enabling organizations to update their Allowlists to reflect the patches they wish to install. This update allows the next scan to validate compliance with patching requirements, and also easily identify unpatched machines.

By utilizing this integration, organizations can achieve:

- » Simplified patching and allowlisting
- » Proof of compliance and configuration to approved baselines
- » Save time and effort for security and GRC teams

Selecting and deploying patches is only part of the overall process for patch management. In regulated environments, patching is an auditable control that requires validation. The integration of FoxGuard and Tripwire equips organizations with a full process—from patch selection and deployment through to validation and auditing.



FoxGuard has over 15 years of experience creating secure comprehensive patching solutions. We know the industry's assets because we have analyzed, documented, and verified patch details for these assets for years. Founded in 1981, we have the experience and in-depth knowledge to support patch management programs in critical infrastructure. In 2014 we partnered with the US Department of Energy (DOE) to develop patch management for the energy utility industry. FoxGuard works with several leading energy equipment OEMs and directly with electric utilities, supplying patch management and cybersecurity solutions globally. [Learn more at foxguardsolutions.com](https://foxguardsolutions.com)



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](https://tripwire.com)

The State of Security: News, trends and insights at tripwire.com/blog
Connect with us on [LinkedIn](#), [Twitter](#) and [Facebook](#)