Sentrigard® SECURITY PLATFORM

SENTRIGARD PATCH

OVERVIEW

Industrial Control Systems (ICS) in critical infrastructure continue to be considered high-risk targets for attack and exploitation. Just as with typical home PCs and business computing platforms, cybersecurity vulnerabilities in these ICS environments are frequently discovered and exploited by malicious actors. The application of security patches to systems in those environments is one way to mitigate the vulnerability, reduce risk, and increase reliability.

Patch management in complex ICS environments requires a comprehensive approach designed to support the specific needs of these types of systems. Patch deployment can be challenging when assets, segmented from the internet, are included. Many of the existing patch deployment automation tools focused on traditional IT style technology environments comprised almost entirely of IT assets. The same tools that may be the right choice in a large-scale enterprise environment may prove to be too complex to use in ICS environments. Often, extensive capabilities present in enterprise solutions can become a hindrance when patching purpose-built embedded and industrial systems and equipment. How do you know what asset is the most vulnerable, and what should you patch first? What happens when a reboot is required to complete patch installation – how do you notify the user? How do you handle the patching of "air-gapped" systems disconnected from all other devices? Will patch deployment schedules impact the critical production of the ICS system? Should I even deploy a low impact patch on a high operational impact ICS asset? Those responsible for the patching of systems and equipment in an ICS environment must overcome these patch deployment challenges. A robust set of tools, procedures, and processes is required; to safely and efficiently patch and update equipment in these environments.

BENEFITS

FIELD PROVEN TOOLS

EXTENSIVE APPLICATION LIBRARY

DATA INTEGRATIONL

DISCONNECTED DEVICE SUPPORT

EXTENSIBLE PLATFORM

COMPLIANCE REPORTING

RELATED PRODUCTS

PATCH AVAILABILITY REPORTING

PATCH BINARY ACQUISITION

PATCH VALIDATION SERVICES

ON-SITE PATCH DEPLOYMENT SERVICES

VULNERABILITY NOTIFICATION REPORTING

ASSET ID & BASELINE CONSULTATIVE SERVICES

FOXGUARD SOLUTIONS®

SOLUTION

To simplify and streamline the process of patch deployment in these ICS environments, FoxGuard offers its Sentrigard Patch platform. Sentrigard Patch is a hardened, purpose-built patch deployment security platform that allows customers to manage their on-premise patch deployment efforts from a centralized suite of industry-proven automation tools. Sentrigard Patch will enable users to patch and update both Windows and Linux systems, including 3rd party software applications, from a common toolset. Patch deployment to network equipment (switches, routers, firewalls) and embedded ICS equipment is all supported by a common platform and a variety of industry-leading tools and capabilities that we embed within the platform.

In situations where vendors require the use of proprietary vendor tools to patch a system or update firmware on an embedded device, Sentrigard Patch provides customer accessible environments where those tools can be installed and configured in order to patch those devices.

SENTRIGARD PATCH CAN BE LEVERAGED AS A PLATFORM TO SUPPORT ALL OF YOUR PATCH DEPLOYMENT NEEDS.

Sentrigard Patch integrates FoxGuard's other patch management solution offerings, including Patch Availability Reporting (PAR) and Patch Binary Acquisition (PBA), into the platform, to simplify the overall patch management process. Our ICS Update Patch Visualization Engine included on all Sentrigard Patch security platform offerings. It allows users to get the most out of the patch data contained in the monthly PAR deliverable in an intuitive, easy to use dashboard. Use it in your environment to bring the most important details about your software assets and available patches for them, to the surface. ICS Update allows users a better understanding of the number of patches available, simplifies the identification of which software assets you should focus on first and know which patches address the most critical security vulnerabilities.

In essence, ICS Update helps you decide where to focus your patch deployment efforts first. In addition to increasing visibility to your patch data, Sentrigard Patch further simplifies the overall process with automated patch import capabilities.

Sentrigard Patch automates the transfer of patch files from the secure encrypted media you receive as part of the monthly PBA deliverable, to their respective file repository locations on the platform, for use by the different patch deployment technologies on the platform.

Sentrigard Patch is built on the same secure platform as other Sentrigard offerings from FoxGuard, providing users with the necessary protections against ongoing threats within ICS environments.

Delivered as a physical hardware platform, all Sentrigard Patch functionality is supported within virtual platform environments, allowing for platform extensibility and adaptation to your organization's needs. Leveraging industry-leading virtualization platforms, Sentrigard Patch offered on a variety of hardware platforms from leading manufacturers.

In situations where environmental conditions are less favorable, and standard enterprise hardware will not suffice, we offer an environmentally hardened, ruggedized hardware platform designed to operate in harsh conditions.

We want to be the **right partner** and *help* with your supply chain **COMPLIANCE NEEDS;** we document country of origin, ship dates of hardware, and so much more.

KEY FEATURES

FoxGuard's Sentrigard Patch platform is designed to support your patch deployment needs across a variety of system environments, equipment and devices types.

KEY PROGRAM FEATURES

ATTRIBUTES	FEATURES	SUPPORT STATUS
Core Features	Centrally Managed Windows Environment Patching with Reporting	●
	Centrally Managed Linux Environment Patching with Reporting	●
	Centrally Managed Network Device Patching*	●
	Disconnected Windows Environment Patching	●
	Disconnected Device Patching	Partial
	Custom / Proprietary Patch Creation & Deployment	●
Asset Support	AUTOMATED DEPLOYMENT	
	Microsoft Windows Operating Systems	●
	Microsoft Software (Non OS)**	●
	3rd Party Application Software**	●
	Network Equipment (Switches, Routers, Firewalls)*	Partial
	ICS Vendor Approved Patches at Device Level**	Partial
	Red Hat Enterprise Linux - 6.x, 7.x, 8.x	●
	CentOS - 6.x, 7.x, 8.x	●
	MANUAL DEPLOYMENT	
	Microsoft Software (Non OS)	●
	Driver Updates	●
	BIOS / UEFI Firmware	●
	ICS Vendor Approved Patches at Device Level	Partial
	ICS Device Firmware & Software	Partial
	Field Devices	Partial
Additional Platform Features	ICS Update Patch Visualization Engine	●
	Automated Patch Data / Patch File Import	●
	Hierarchical Patch Deployment Tools for Enterprise Deployments	Partial
Platform Architecture	VMware vSphere ESXi Hypervisor Support – 6.x, 7.x	●
	Microsoft Windows Server 2016 with Hyper-V	●
	Microsoft Windows Server 2019 with Hyper-V	●
Platform Maintenance, Support & Warranty	Quarterly Platform Patch & Update Release (Requires M&S)	●
	Annual Platform Upgrade Release (Requires M&S)	●
	Multi-Year Maintenance & Support Contracts	Optional
	1 Year Hardware Warranty with 9x5 Telephone Support	●
	Multi-Year Hardware Warranty Upgrades with Enhanced Support	Optional
Professional Services	Custom Patches Creation Services	Optional
	On-Site / Field Patch Deployment Services	Optional

* Where supported by the network device manufacturer / vendor

** Where supported by the 3rd party application patch library and vendor approved

KEY PROGRAM FEATURES

Field Proven Tools: Leverage field-proven, industry-accepted patch deployment tools that have been used extensively in ICS environments for over a decade. We've tested, vetted and qualified patch deployment technologies from industry leaders to support both OEM vendors and direct end-users with their patch deployment needs at hundreds of ICS sites across the world. These tools are simple to use and easy to understand, yet robust enough for use in demanding ICS environments. *FoxGuard is your one source.*

Extensive Application Library: Sentrigard Patch includes automated, central patch deployment support for one of the largest, most diverse 3rd party application libraries in the industry. While we realize that not every application is supported, we work with technology providers to cover as many of the software titles in your environment as we can.

Data Integration: Leverage the benefits of a single source for your patch information and patch binary files. We've engineered and automated the process to import FoxGuard PAR data and PBA patch files into the Sentrigard Patch platform to streamline and simplify the overall patch management experience.

Disconnected Device Support: Not every device is network accessible – we understand and appreciate the need for disconnected systems. Don't worry – we have a solution for that, too. Sentrigard Patch utilizes the DisPatch Update Utility to automate the deployment of Microsoft and other 3rd party application patches to those disconnected assets in your environment.

Extensible Platform: While the Sentrigard Patch platform is designed to support a wide array of your patch deployment needs, we realize that proprietary tools do exist and are often required to patch things such as specialty software, network devices and other ICS equipment. Use the Sentrigard Patch system to host them and keep everything on one platform, reducing the need to manage multiple systems.

Compliance Reporting: Utilize the pre-engineered reporting capabilities provided within centralized patch deployment technologies on the Sentrigard Patch platform to gain valuable insight into the current patch status of your environment as well as to support NERC CIP-007 compliance audit requirements. Pre-engineered reports have been used successfully to help meet security and regulatory requirements in all NERC regions throughout the U.S. and Canada.

WHY FOXGUARD

EXPERIENCE

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.

INDUSTRY LEADER

The company was founded in 1981, in Christiansburg, Virginia. We have the experience and in-depth knowledge to provide patch management programs to critical infrastructure. In 2014 we partnered with the US Department of Energy (DOE) to develop a patch management program 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.

AUDIT SUCCESS

Our customers are world wide and FoxGuard is proud to say that hundreds of our customers have successfully passed regulatory and security audits while leveraging our products and solutions to support their compliance needs.