SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Phone: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com

SEL Product Malware Risk Mitigation

At SEL, we have made security a top priority for over 40 years. Protecting critical infrastructure from the threat of malicious software (malware) is a central part of that effort. The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards require responsible entities to ensure controls are in place to detect, prevent, or mitigate the introduction and propagation of malware on all cyber assets. Additionally, IEC 62443-4-2 CR 2.2 includes specific requirements for protection from malicious code that vary by component type (embedded devices, host devices, network devices, and software applications), with each component required to provide appropriate protection capabilities based on its role in the system.

Malware is usually designed to target a specific operating system, application, or protocol to exploit security vulnerabilities. While most malware is designed to compromise commodity operating systems, sophisticated attackers create specialized malware to compromise embedded devices. SEL incorporates an array of anti-malware controls into our products to mitigate the significant and growing risk that malware poses to all embedded devices and software.

Modern SEL Protective Relays

SEL protective relays accept only firmware files cryptographically signed by SEL. These relays reject altered or unsigned firmware and cannot load or run other programs. On startup, SEL relays compare a checksum of the contents of permanent memory with a reference checksum to verify firmware integrity and perform a similar integrity check during runtime. These products can activate an alarm contact to signal a firmware alteration attempt. SEL publishes firmware hashes on its website for integrity verification prior to installation. Operating SEL protective relays also generate a value for comparison with a reference published on the SEL website as an added confirmation that the installed firmware is the expected version and is complete and unaltered.

SEL Automation Controllers and Security Gateways (RTAC, 36XX)

SEL automation controllers and security gateway products use a hardened Linux operating system that features SEL exe-GUARD, a kernel-level application allowlist technology to prevent malware installation on or modification of the system. Like SEL protective relays, SEL automation controllers and security gateway products accept only firmware files cryptographically signed by SEL and reject altered or unsigned firmware. SEL automation controllers and security gateway products log and alert on events that may signal an attempt to alter firmware, install malware, or bypass mandatory access controls.

SEL Blueframe

The Blueframe platform uses a hardened Linux operating system also protected by SEL exe-GUARD, an allowlisting technology that prevents the installation of unauthorized software or other system modification. Blueframe supports the creation of fine-grained user and role definitions to construct and enforce precise access levels and permissions. The Blueframe platform provides detailed logging of operations performed by any system users as well as logging of automated systems operations to support the investigation of any attempt to alter firmware, install malware, or bypass mandatory access controls. Blueframe is engineered to meet the stringent requirements of operational technology (OT) environments, providing a secure and resilient platform for critical infrastructure operation and orchestration.

Last updated on 04/29/2025