

Secure Software Update Service

Just like any network, secure networks contain computers, servers, control systems, databases, etc. that need software updates on a recurring basis. Historically software updates are downloaded from the software vendor's website to a local server, copied onto a portable media device (i.e. USB drive) and hand carried into the secure network for installation. The portable media device is plugged into a device on the secure network and the software patch is downloaded and installed.

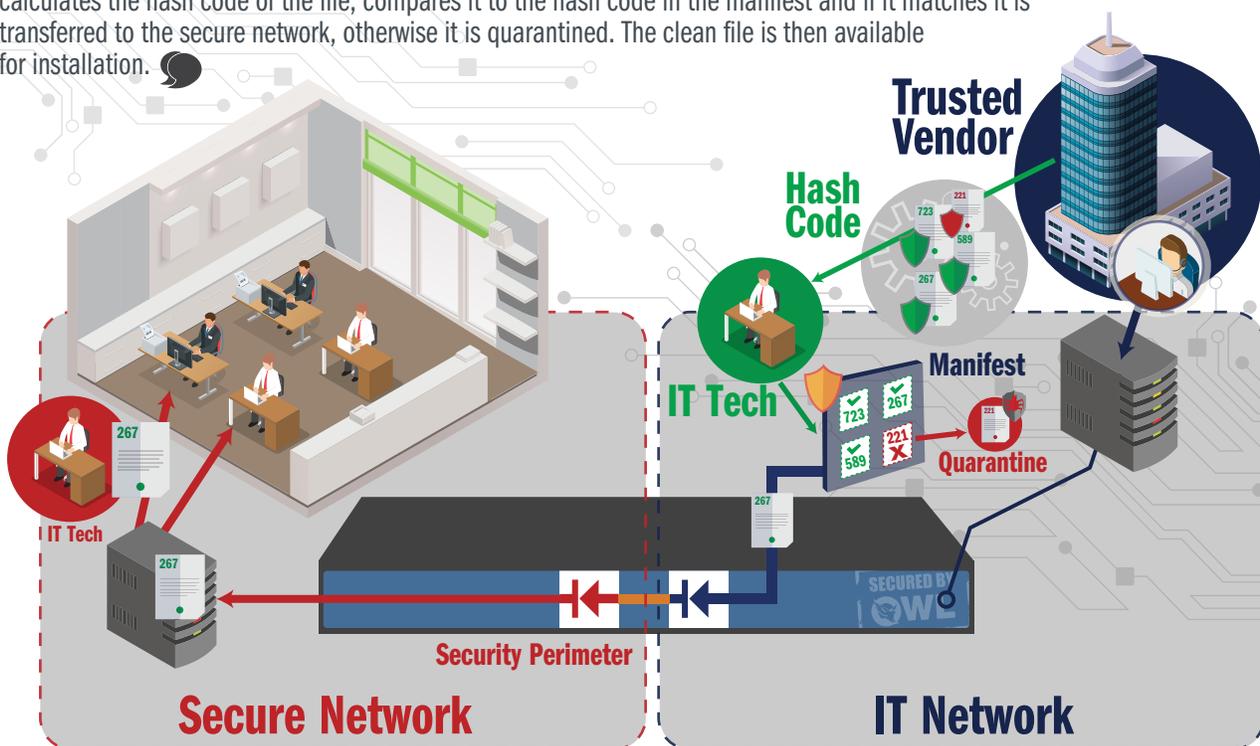
The security threat created by this method lies in two areas: the first is unauthorized modification of the source file provided by the vendor. In the process of downloading, saving, copying to portable media and uploading on the secure network, the file could be unknowingly manipulated. The second threat comes from unknown malware that can be lurking on the portable media device. SSUS provides a way to ensure the source file has not been manipulated and to safely transfer it into the secure network.

The Owl Solution

- SSUS is a software filtering product that secures automated transfer of files into secure networks. SSUS addresses the problem of how to transfer software patches & executable files (like anti-virus & malware updates). With SSUS, an executable or non-executable file is individually validated against a manifest (or list) consisting of pre-configured hash numbers. This hash number had been previously provided by the originator. Files that match hashes on the manifest list are validated and transferred. Those files with no manifest match are denied transfer, and are quarantined or deleted by administrators.
- The SSUS software augments existing hardware-enforced data diode security products to provide the following features: enhanced software security controls to ensure all files and software updates are subject to content inspection, file extension checks, antivirus examinations, hash code validations, and other checks before the files and updates are allowed across the perimeter boundary. SSUS permits implementation of a two-person authentication approval and release process. Owl's Secure Software Update Service allows for the establishment of a security policy which explicitly prohibits movement of data using Portable Media Devices (PMD) between security levels.

SSUS USE CASE:

The IT Tech responsible for updating the software applications within a secure network needed a reliable, safe and secure method for transferring software patches provided by vendors into the secure network. SSUS supports a number of verification techniques (file extension checks, filters, virus scans, ascii checks) to tightly control what enters the network. The core technique uses a hash code provided by the vendor that is independently entered into a manifest on SSUS. When a file is copied onto SSUS for transfer, SSUS calculates the hash code of the file, compares it to the hash code in the manifest and if it matches it is transferred to the secure network, otherwise it is quarantined. The clean file is then available for installation.



Security Features

- Secure transfer of any executable & non-executable files
- File integrity validation
- Transfers between two networks
- Convenient support for multiple hash code algorithms
- Administrator management of registered manifest signatures

Benefits

- Secure automated file transfer to secure network
- Secure process for timely updates of software patches & anti-virus programs
- State-of-the-art access to transfer audit trails
- Integration with Owl remote monitoring OPMS
- Operates over Owl data diode architectures

Hardware



The SSUS application runs on different Owl data diode platforms in order to address specific bandwidth requirements. The OPDS-100 and OPDS-1000 are the most popular platforms, offering a range of bandwidth options from 10 Mbps to 1000 Mbps with the flexibility to incrementally increase bandwidth using license keys as needs evolve.

The OPDS-100 is an entry level solution supporting from 10 Mbps to 100 Mbps and the OPDS-1000 is a high bandwidth solution supporting from 100 Mbps to 1000 Mbps. Both solutions are all in one, 1U rack mountable cybersecurity solutions designed to enforce a cyber perimeter. In addition to the SSUS application, the products support software interfaces (connectors) to a broad range of applications that generate business critical data (sensor information, data points, database historians, syslog messages, alarms, etc.). That data is securely transferred to the business network and used for remote monitoring, production planning, and other management tasks.

EAL certified, they have gone through shock and vibration testing with different models providing a number of physical security features to resist tampering. Licensable bandwidth tiers allow customers to purchase only the bandwidth they need with the knowledge that they can increase bandwidth at any time by moving up to the next tier.

DualDiode Technology

Owl's DualDiode Technology is built around patented circuitry which only allows data to physically flow in one direction thereby preventing all network based cyber attacks. The design also includes a deep protocol break which terminates all Ethernet traffic, transfers the payload via the ATM protocol and then converts it back to Ethernet. This has the unique benefit of hiding all the IP and MAC address information from the outside world and preventing any probing of the network. This technology comes in different form factors depending operational environment.

About Owl

For over 16 years Owl Computing Technologies has been implementing next generation cybersecurity solutions for critical networks. Owl's DualDiode Technology®, a proprietary data diode, boasts 24 technology patents and has over 2,000 successful deployments globally across intelligence, government, military, financial services, utility, energy, and other critical infrastructure networks. Owl's hardware-enforced technology ensures secure networks and enables the reliable and robust transfer of all data types and file sizes.

