REMEDIATE AND SECURE LEGACY APPLICATIONS

www.skyportsystems.com

Overview

Organizations typically have a number of legacy applications that are noncompliant and run out-of-support operating systems such as Windows 2000/2003/2008 and RHEL 4. They fail audit checks because patches are not available to fix known vulnerabilities. The applications must operate without interruption for the organization to function, but bringing them into compliance is difficult due to migration costs, limitations in software availability, and recertification complexities.

SkySecure remediates and secures these important assets without requiring that they be upgraded. These assets run as virtual machines in secure compartments, preventing exposure to vulnerabilities and meeting conformance with compliance audits.

Benefits of SkySecure

SkySecure is a turnkey platform for securely running high-value business applications. SkySecure is the only commercially available platform designed to host and protect legacy applications that fully integrates hardware, software, and services with a easy-to-use deployment and operational model. To achieve an equivalent level of protection with other tools, an organization would need to isolate legacy applications in a custom demilitarized zone (DMZ) in a separate network protected by dedicated firewalls.

- **Reduces Exposed Vulnerabilities of Legacy Applications**
  SkySecure shields legacy applications and their underlying operating system from vulnerabilities that are normally exposed during compliance audit network scans or cyberattacks. SkySecure intercepts and filters all IO through tailored firewall security policies, so only specific communications are allowed. This is especially important when protecting out-of-compliance operating systems, such as Windows 2000/2003, which have numerous critical vulnerabilities that can be exploited over the network and which can be used to compromise the entire system. Using SkySecure can be the difference between a pass or fail compliance audit check.
- **Protects Web Service Exposure**
  Legacy web servers are challenged to meet regulatory requirements such as PCI. They are also at risk due to frequent new vulnerability announcements, such as Heartbleed and FREAK, that cannot be patched. SkySecure proxies web connections, including the TLS/SSL sessions, to shield the applications from attack and ensure they are running the latest patches, crypto libraries, and secure configuration settings to guarantee compliance.

SYSTEM COMPONENTS

SKYSECURE SERVER

Trusted compute platform based on locked-down firmware, signed immutable images, Intel® Trusted Execution Technology and the SkySecure I/O Controller. Controller hardware enforces segmentation for every VM, enables wire speed network-flow policy and packet mirroring, and helps make evidentiary audit trails tamper-resistant.

SKYSECURE COMPARTMENT

A hardware facilitated security layer wrapped around each individual VM. It controls workload identity, protocol, I/O, file system and identity management access via a per-workload security policy.

SKYSECURE CENTER

Skyport Systems hosted cloud management and remote attestation service that verifies the integrity of the system and ensures configuration and patch best practices are followed. It deploys and orchestrates VMs, manages and monitors security policies, alerts on policy violations, and features built-in analytics to assist with audit and compliance requirements. Securely stores policy, audit logs, and credentials.

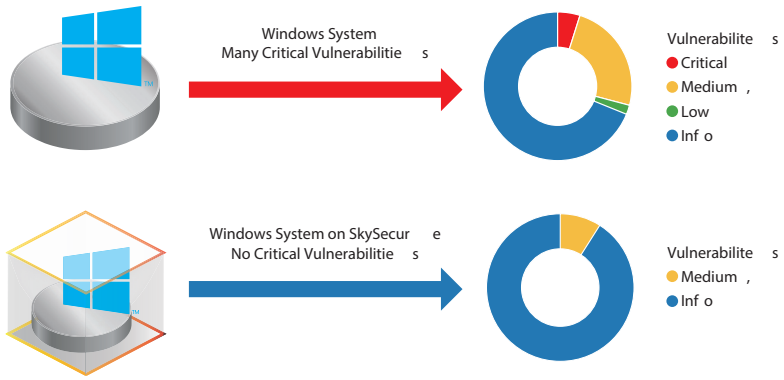
SKYPORT SYSTEMS

- **Protects Applications Against Attacks from Anywhere, even Neighboring Systems**
  SkySecure provides organizations assurance legacy applications are shielded. Each application is microsegmented with a hardware-based firewall to ensure it only communicates with approved whitelisted systems. The firewall enforces a policy that is specific to the VM and protects it from any sing point-of-attack, including lateral attacks from neighboring systems in the same network security zone and from VMs hosted on the same SkySecure server.

- **Ensures Infrastructure is Always Patched and Up-to-Date**
  Each SkySecure server is centrally managed from a privately hosted secure cloud environment. Skyport maintains responsibility for the entire hardware and software stack that hosts a VM, spanning the firmware, BIOS, drivers, operating system, virtualization layer, and the built-in security capabilities. Organizations are assured that their servers hosting legacy applications are up-to-date, without the usual patch-update treadmill tax.

- **Easily and Securely Deploy and Move Legacy Applications**
  Making changes to the location and capacity allocation of legacy applications is easy with SkySecure. Secure virtualization allows operators to quickly make moves, adds, and changes without introducing new compliance audit or security policy red flags.

- **Provides Audit Reporting**
  Traditionally, compliance auditors have been unable to determine if identified vulnerabilities are actually being exploited. SkySecure helps auditors determine the most relevant issues by providing a full activity record of I/O, system events, and administrative activity in a tamper resistant secure data warehouse, for the lifetime of the system. This allows the the organization to focus on proven security issues rather than theoretical conjecture.



- **Is a Bullet-Proof Solution for IT**
  The system requires no effort to assemble or maintain, yet retains a strong and organization-specific security posture by default. It eliminates the risk of operational complexity and human error while managing and patching the system. Built-in anti-surveillance and anti-exfiltration controls tie into audit tools and verify normal VM behavior by detecting attacks and providing oversight of administrative access into the legacy application. Out-of-box entitlements ensure the applications are hardened by default and immune to operator error. A forensic trail of all administration and I/O activity is stored for the lifetime of the system with a two-person administration rule to prevent tampering with records.

Secure Remote Management

SkySecure is managed remotely so there is no risk of local personnel changing security policies, altering event logging, or adjusting device configuration settings. The platform capabilities provide a unified secure approach to operations that spans device provisioning, VM orchestration, patch and updating, defining security policies, key management, and monitoring device and security events. All communications between the platform and SkySecure Center are authenticated and encrypted to provide a secure lights-out management environment as a built-in feature of the system.

SkySecure is also designed for turn-key deployment and requires no special IT skills on-premises during the installation or operation of the system. Simply rack the server, power it up, plug in the ethernet cables, and enable network access to SkySecure Center. The new system is then bootstrapped from the remote management center after it successfully attests. This reduces the cost of deploying and operating systems in remote locations.

Summary

SkySecure is an ideal solution for organizations that need to run legacy applications while conforming to compliance audit policies. Standardizing on SkySecure as the infrastructure platform is an easy way to continue to operate without demanding application migration or recertification. It reduces the risk of compliance failures, protects applications from cyberattack, and allows organizations to migrate at their convenience.

Cloud-Managed

On-Premise Secure Server

Visit us at www.skyportsystems.com or contact info@skyportsystems.com to learn more.

SKYPORT SYSTEMS