Legacy Platforms

One of the most significant challenges is managing the risks associated with legacy platforms. While often critical to business operations, these systems present unique vulnerabilities, especially with encrypted communications. The balance between the cost of upgrades and the risks associated with maintaining legacy systems is fraught with complexities.

Legacy platforms are a testament to the adage, "If it isn't broken, don't fix it." However, this mindset can lead to significant risk. The financial implications of upgrading legacy systems are often substantial, leading many organisations to defer upgrades, thereby increasing risk exposure. Legacy platforms may have well-known vulnerabilities that are no longer patched by vendors, making them prime targets for attackers. Vendors phase out support for older systems, and security fixes become scarce, exposing systems and increasing operational risk. Many legacy systems are tied to specific vendors, limiting upgradability and flexibility in responding to new risks. They often cannot comply with modern security standards, including those related to encrypted communications.

Venari Security offers a solution that provides visibility of the encrypted communication associated with legacy encryption protocols to help mitigate the risks and understand the nuances of encrypted communications specific to individual legacy platforms, allowing for a more granular security policy specific to the application or service. By creating explicit rules that define the encryption traffic profile, Venari Security enables organisations to maintain a controlled environment where only authorised communication is permitted. Defining which machines can communicate with the legacy platform reduces the attack surface and limits potential exposure. The policies can be adapted as platform cryptography is upgraded, ensuring continuous protection. The ability to monitor and alert on suspicious behaviour in near real-time is crucial. Venari Security's solution ensures that anomalies in encrypted traffic are quickly identified and addressed.

The challenges legacy platforms pose in encrypted traffic are significant but not insurmountable. Encrypted traffic analysis stands out as a critical component in the arsenal against the vulnerabilities inherent in these systems. Venari Security provides a comprehensive approach to understanding, monitoring, and controlling encrypted communications associated with legacy platforms. By implementing the solution, organisations can bridge the gap between the necessity of maintaining legacy systems and the imperative of ensuring robust cybersecurity. This strategic approach mitigates immediate risks and positions the enterprise for a more secure transition when system upgrades become viable.

Bridge your knowledge gap.
Visit: www.venarisecurity.com

Venari Security Ltd.

16 Great Queen Street, London,
WC2B 5AH, United Kingdom
+44 (0)20 7294 7749
info@venarisecurity.com

About Venari Security

Venari Security provides organisations with advanced visibility into their encrypted attack surface, ensuring regulatory compliance and privacy adherence through our cryptographic discovery tool.

Our focus is on crypto agility which helps you assess both external and internal cryptographic risks, preparing your business now and for the quantum future.