FORNETIX

Cybersecurity Vulnerabilities Continue Wreaking Havoc on Manufacturing Industry

> HOW VAULTCORE CAN HELP

» HIGHLIGHT

The myriad of technologies, networks, and suppliers utilized by the manufacturing industry nearly outnumbers the variety of products they deliver. From small office applications and wireless robotic transmissions to tracking transportation or a customer's receipt of goods, the entire manufacturing process is a rapidly changing environment that relies on efficient and secure supply chain management.

Unfortunately, advanced cyberattacks on manufacturing supply chain architectures are increasingly disruptive to business — exposing customer data, intellectual property, digital communications, and other vital data while costing companies and consumers hundreds of millions of dollars each year.

Fornetix® VaultCoreTM provides a critical layer of protection for the manufacturing industry. Whether data is at rest, in transit, or in the cloud, VaultCore helps ensure all data remains secure. VaultCore's centralized, automated, and highly scalable cryptographic operations platform and encryption key management solution works across the entire manufacturing ecosystem, including connected devices. Rooted in zero trust architecture, VaultCore's powerful policy deployment tools and robust device authentication have proven effective at securing data and mitigating harmful attacks on the manufacturing supply chain.

The key benefit of VaultCore is providing alignment and governance in a standards- based model with a focus on API-based integration and interoperability. VaultCore's combination of scale and zero trust architecture is ideal for multi-tiered manufacturing where data protection is expected to cross organizational boundaries.

» THE CHALLENGES

Manufacturing involves multiple tiers of suppliers providing components that come together to create the end product. Each tier is an exercise in unique processes to the manufacturer and their third-party suppliers' raw materials, production, inventory, and distribution. This complicated convergence of players, processes, and data creates a wicked infrastructure security problem.

Complex ecosystem relationships like these create weakness, so it is no surprise that the manufacturing industry has become a high-profile target for cyberattacks. The security strategy necessary to protect data in these ecosystems extends far beyond the manufacturer's network. In today's threat environment, a manufacturer's best defense is their ability to evolve rapidly, maintain adherence to stringent security guidelines, including zero trust architecture, effective protection of data at rest, in transit and in the cloud, and a well-orchestrated approach to encryption key management that extends security from the corner office to the shop floor through to the supply chain.

IOT, CONNECTED PRODUCTS, AND CLOUD SECURITY RISKS

The interconnectedness of the manufacturing process and IoT devices is accelerating. Installation of IoT systems is typically associated with increased efficiencies and cost savings. However, breaches resulting from ineffective cloud security, vulnerable IoT devices, and mismanaged IT security (human error) are on the rise and have been responsible for halting production, the destruction of property, and even creating dangerous workplace environments.

THIRD-PARTY RISKS

Manufacturing's evolution to a modern, connected, digital business environment has forced cybersecurity responsibility within the industry. Each manufacturer may feel confident in their internal security strategy and mandate adherence to strict security standards, but still over 50% of all network attacks originate from smaller, third-party vendor systems where security may not be as robust. Regardless, responsibility for data security ultimately lies with the manufacturer.

» THE SOLUTION

Gone are the days where perimeter security would suffice. Whether it is customer data, automated shop floor technology, or a vendor's list of raw materials, access to valuable data must be governed by security concepts that extend far beyond the facility's walls. Zero trust architecture must be implemented to protect data from product inception to final delivery. This strategy begins with encryption that knows no boundaries, sufficient access control, and robust encryption key management applied through the entire lifecycle of the product.

Gartner recently said it best: ***"Develop an Enterprise-wide Encryption Key Management Strategy or Lose the Data[1]."*** Encryption key management done correctly is rooted in zero trust architecture and simplifies data security policy through encryption and access enforcement across the entire manufacturing supply ecosystem.

This can be achieved by utilizing a key management solution like VaultCore™ that swiftly connects with legacy and new devices. While most Security Administrators are mindful of the latest advancements in encryption, historically, there has been a dangerous lack of attention to practical encryption key management requirements. Successfully managing the hundreds of thousands of encryption keys to the level necessary to adequately protect intellectual property, networking communication, IoT devices, and third-party data is critical. The bottom line is that managing encryption within and beyond the enterprise is a complicated and daunting task, and in some cases, best security practices are overlooked or ignored.

FORNETIX VAULTCORE

1 https://www.gartner.com/en/documents/3817045/develop-an-enterprisewide-encryption-key-management-stra

Manufacturing Use Case

VAULTCORE PROVIDES SECURE EXTERNAL ENCRYPTION KEY MANAGEMENT THAT SUPPORTS WIDE-SCALE PROTECTION FOR MANUFACTURING

VaultCore is a groundbreaking, state-of-the-art cybersecurity solution that simplifies encryption key management. It provides a single-pane-of-glass view and access for deploying automated processes and enforcing key management across an entire organization, including connected devices and the supply chain. This unified, centralized approach to key management allows storage and control of all encryption keys in all environments, whether data is on-premise, virtualized, in the cloud, or a hybrid.

As sensitive data is stored or transferred between vendors and customers, it remains encrypted and only appears legible to authorized users. However, for encryption to stay effective, it requires regular rotation and management of the encryption keys. Standard rotation is an impossible task to do manually on the scale necessary to protect any manufacturing enterprise. Yet, many continue to try, leading to devastating consequences from entirely preventable human error.

VaultCore provides complete lifecycle key management. Proper lifecycle key management means you have complete control to generate, register, store, distribute, install, use, rotate, backup, recover, revoke, suspend, or destroy keys. This unprecedented power ensures that only keys that comply with the most current policy are deployed only to the appropriate devices and are enforced down to the most granular level. Automation and policy enforcement control can easily be exercised across all environments, providing the ultimate cyber defense and data protection through VaultCore's Mandatory Access Control (MAC).

CENTRALIZED CONTROL PANEL AND STREAMLINED REPORTING

Capable of integrating seamlessly with newer KMIP (Key Management Interoperability Protocol) enabled or legacy non-KMIP devices through Fornetix's Orchestration Gateway™, VaultCore streamlines control, visibility, and reporting through a centralized control panel accessed via a simple web interface. Administrators have clear visibility of all encrypted devices with a signed, validated audit log on key management and key consumption. Transparent reporting includes who accessed the key, the event time, and the success or failure of the operation. The hassles of collecting access reports, locating client credentials, and organizing data from multiple locations for compliance purposes or internal reporting become a thing of the past.

LIFECYCLE CERTIFICATE MANAGEMENT

Certificate management plays a crucial role in security. The typical manufacturer may spend hundreds of thousands of dollars per certificate outage. With VaultCore, the request, renewal, approval, generation and deployment, and usage and monitoring of certificates is easily automated with a set-it-and-forget approach. A one-time setup process is all you need to automate what is currently an extensive, manual process, often complicated by human errors.

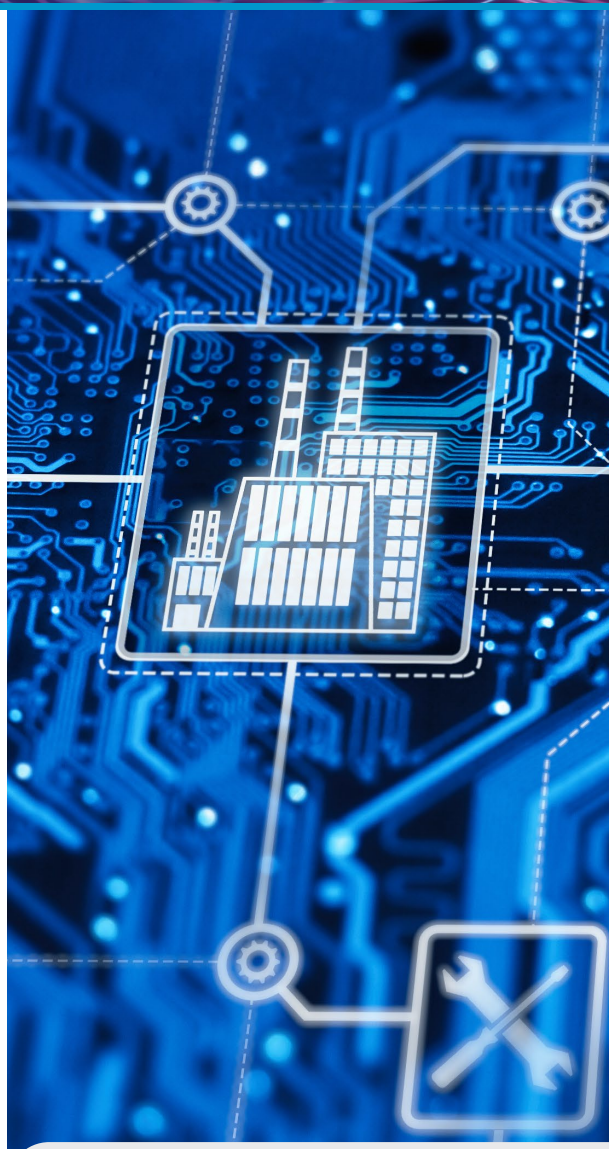
Delivered as physical hardware or a virtual appliance, VaultCore can also verify the cryptographic integrity of data to ensure critical code has not been tampered with between the facility and third-party vendors. Verification is a significant benefit in thwarting attack which can come from smaller, less secure partners. And with industry-leading capacity, VaultCore can manage over 100 million keys, more than adequate to serve the growing needs of the manufacturing industry.

VAULTCORE = A RETURN ON YOUR SECURITY INVESTMENT

VaultCore is competitively priced, and on average, savings are recognized in two (2) years. VaultCore, allows you to set a re-key schedule that matches your desired policy – an efficient approach – that turns a manual process into a simple click of a button, removing known risks associated with human error, rotating keys, and deploying policy.

» SUMMARY

Securing sensitive data and protecting against third-party weaknesses have become exponentially complex. The manufacturing industry continues to migrate communications to wireless networks, store and transfer sensitive data, embrace modernization of IoT devices, and utilize third-party vendors. As a result, security and risk management leaders struggle to support secure storage, access, and use of encrypted data while also meeting necessary speed, privacy, crypto-agility, mandatory data privacy compliance, and business needs. Fornetix's VaultCore provides a simple and powerful, cost-efficient solution that works with existing investments. It is also scalable to meet the growing demands of the manufacturing industry through an enterprise-level key management system capable of protecting all forms of data and negating security risks associated with less secure third-party vendors.



» ABOUT FORNETIX

Fornetix®, a pioneer in encryption key management, understands that securing data in today's complex environment can seem like an impossible task. VaultCore™ by Fornetix is a patented solution designed to simplify the encryption key management process across the entire enterprise. VaultCore provides a centralized system to automate the full key lifecycle and enable compliance policy enforcement. Scalable to over one hundred million keys for data storage environments including multi-cloud and hyper-converged infrastructures, VaultCore allows you to leverage existing technology investments and take complete ownership of your keys ensuring that critical data is safeguarded no matter where it resides.

FREE TRIAL: fornetix.com/freetrial
FREE DEMO: fornetix.com/demo

1-844-539-6724

5123 Pegasus Court, Suite X
Frederick, MD 21704