ITSNYC
INTEGRATED TECHNOLOGY SYSTEMS

Enhancing Cybersecurity for a Medical Device Company with a Zero Trust Network

Client Overview

A **mid-sized medical device** company, consisting of **120 users**, was facing significant cybersecurity threats due to outdated IT infrastructure and limited remote access security. With increasing pressure to protect sensitive patient and corporate data, the company needed a robust solution that would prevent unauthorized access and **minimize cybersecurity risks.**

The Challenge

The company was relying on an **aging VPN system** that allowed users to access company resources from remote locations. However, as more employees began working remotely, the VPN became a liability:

- **Security Concerns:** The company lacked comprehensive controls to verify each user accessing the network, leading to potential security gaps and vulnerabilities.
- **Compliance:** Compliance: As a public company and healthcare-related they company they need to meet strict **SOX** and **HIPAA** requirements regarding financial controls, data privacy and security
- **Scalability:** The existing IT infrastructure was not scalable to meet growing demands, especially as more users required remote access.

The company needed a solution that could:

- Securely manage remote access for its employees.
- Ensure that only **verified users** could access sensitive data, reducing the risk of **data breaches.**
- Help the company maintain **HIPAA compliance** while supporting future growth.

The Solution: Transition to a Zero Trust Network

ITS NYC proposed a Zero Trust Network architecture to replace the outdated VPN system and provide a more secure, scalable, and compliant solution. The Zero Trust model is based on the principle that no one inside or outside the network should be trusted without verification.

Key components of the solution included:

Microsoft Business Premium: A secure, cloud-based solution that integrated seamlessly with the company's existing Microsoft suite, allowing for improved data protection and easier management of remote access.

Entra (Azure Active Directory): Provided advanced identity protection by continuously verifying user identity and access privileges. This ensured that only authorized users could access the company's critical applications and data, even when working remotely.

Multi-Factor Authentication (MFA): Strengthened the security framework by requiring users to provide multiple forms of authentication before gaining access to sensitive resources.

Conditional Access Policies: Implemented custom access policies that dynamically adjusted security levels based on user location, device, and behavior, ensuring maximum protection for sensitive data.

The Results:

Increased Security: The **Zero Trust Network** model significantly reduced the risk of unauthorized access. By constantly verifying every request, the company ensured that only **verified users** could access sensitive information, protecting the business from potential **data breaches**.

HIPAA Compliance: With enhanced security features and the ability to monitor and restrict access, the company met **HIPAA regulations** more easily, ensuring that patient and corporate data were handled according to strict compliance standards.

Scalability: The company's IT infrastructure is now future-proofed and scalable to meet the needs of a growing workforce, with the ability to easily onboard new employees and manage access without compromising security.

Reduced VPN Vulnerabilities: By eliminating their reliance on traditional VPN infrastructure, the company mitigated several vulnerabilities that came with open VPN ports and unsecured remote access.

Conclusion:

By transitioning to a **Zero Trust Network** model, the medical device company not only protected its sensitive data from cyber threats but also ensured that it remained compliant with **SOX** and **HIPAA regulations**. This modernized IT infrastructure provides them with the **security, scalability,** and **compliance** necessary to support their growing remote workforce.

For companies in industries like **medical**, where patient data security and compliance are paramount, a Zero Trust approach can deliver the same benefits. ITS NYC's expertise in **cybersecurity** and **compliance** ensures that businesses can confidently adopt modern IT solutions while safeguarding sensitive information.

Key Takeaways:

- **Increased Security:** Constant verification of users and access requests dramatically reduced the risk of unauthorized access.
- **Compliance:** Ensured that the company met strict SOX and HIPAA requirements for financial controls, data security and privacy.
- **Scalability:** The Zero Trust model provided a future-proof IT infrastructure, allowing the company to easily scale up without compromising security.
- **Eliminated VPN Vulnerabilities:** Transitioned from an outdated VPN system to a more secure, modern infrastructure.

How ITS NYC Can Help Your Business:

ITS NYC specializes in providing **secure IT solutions** that meet the unique needs of your business. From transitioning to a cloud-based infrastructure to implementing a **Zero Trust Network,** we ensure your business is **secure, compliant**, and ready to scale.

Ready to modernize your IT infrastructure? Contact ITS NYC for a free consultation.

ITS: Your Office Without Walls

212-750-5420

itsnyc.com/contact-us

itsnyc.com

itsnyc.com/webinars

linkedin.com/company/integrated-technology-systems

ITSNYC
INTEGRATED TECHNOLOGY SYSTEMS