Secure IOT Data Transfer for Lockheed Martin

Zero Trust Data Security Safeguarding IOT across the Aerospace Industry

aws partner network

Introduction

Lockheed Martin is a renowned global technology leader specializing in aerospace, defense, and critical infrastructure solutions. With a rich history of innovation and expertise, Lockheed Martin plays a pivotal role in developing secure and resilient systems for critical commercial infrastructure and mission-critical applications.

Challenges

Critical infrastructure is the backbone of our society, encompassing systems responsible for energy delivery, transportation, emergency services, and manufacturing. Any compromise to these systems severely threatens national security, economic stability, and public health. Lockheed Martin recognized the pressing need to enhance the security and resilience of critical infrastructure, especially in the face of evolving cyber threats.

One of the significant challenges Lockheed Martin faced was the vulnerability of Internet of Things (IoT) devices used in critical infrastructure systems. Although essential for communication with critical systems like water pipes and manufacturing facilities, these devices often needed robust security measures. Insecure IoT devices could compromise critical infrastructure reliability, leading to potentially catastrophic consequences if left unaddressed.

Partner Solution

Lockheed Martin turned to XQ, a leader in Zero-Trust technology solutions, to address these critical challenges. XQ's Zero-Trust solution offered a robust and reliable approach to safeguarding critical infrastructure against cyberattacks. The partnership focused on integrating XQ's technology directly into IoT devices, transforming them into highly secure components of the critical infrastructure ecosystem.

XQ's Zero-Trust Gateway was pivotal in securing and monitoring data integrity in IoT devices. This innovative approach involved object level encapsulated encryption technology and Data Rights Management, ensuring that data packets remained secure throughout their journey. Data was encrypted at the edge, separated from encryption keys during transmission, and decrypted securely at their destination. XQ's system also logged every interaction, promptly alerting users in case of data compromise.

About the partner

LOCKHEED MARTIN

The Lockheed Martin Corporation is an American aerospace, arms, defense, information security, and technology corporation with worldwide interests.

Achievements and Business Impact

The partnership between Lockheed Martin and XQ yielded significant achievements and measurable business outcomes:

1. Enhanced Data Security: Integrating XQ's Zero-Trust technology into Lockheed Martin's IoT devices and sensors bolstered data security, safeguarding critical infrastructure against cyber threats.

2. Data Integrity: XQ's solution ensured data integrity, supporting informed decision-making based on reliable data collected from IoT devices.

3. Connectivity Resilience: Lockheed Martin's critical infrastructure systems remained operational regardless of the communication method, whether 5G, fiber lines, or satellite systems. XQ's technology guaranteed fail-over resilience.

4. Chain of Custody: The tracking and documentation of data throughout its life cycle provide a comprehensive view of data handling and promote transparency and accountability.

5. Logging and Monitoring: XQ's logging capabilities offered real-time insights into data interactions and ensured data remained tamper-free.

6. Financial Growth: With reliable connectivity, critical infrastructure facilities no longer face the threat of security breaches and data exfiltration, enabling increased yields and fostering growth.

The typical approach to IOT security is network segmentation to create an enclave. This requires a high amount of maintenance and fails to protect the data as it leaves the enclave and allows for lateral movement and malware once the enclave is breached.

A report published by the Ponemon Institute and industrial cybersecurity firm Dragos shows that the average cost of a security incident impacting industrial control systems (ICS) or other operational technology (OT) systems is roughly $3 million, and some companies reported costs of over $100 million.

Of the companies that confirmed suffering an incident, 1% said the total cost of the ICS/OT incident exceeded $100 million, and 2% reported costs between $10 million and $100 million. Overall, 13% of respondents said the incident had cost them more than $1 million.The average cost of protecting a single IOT device with XQ is less than $1 a year.

Conclusion

the collaboration between Lockheed Martin and XQ demonstrates a pioneering approach to securing critical infrastructure against the ever-evolving threat landscape. XQ's Zero-Trust architecture has revolutionized the field of reliable and secure connectivity for critical infrastructure systems. By integrating XQ's technology, organizations can significantly enhance the reliability and security of their necessary facilities, ensuring the uninterrupted delivery of essential services to citizens. The future of critical infrastructure protection lies in embracing XQ's Zero-Trust technology.

About XQ Message

XQ is a cloud-based solution for zero trust data access (ZTDA) that encapsulates your data and delivers object level security.
XQ's Zero Trust Data technology provides customers with exclusive encryption key control, data sovereignty, and a complete audit trail for data, enabling secure data migration and protection.

aws Qualified Software

aws PARTNER Public Sector