FROST & SULLIVAN

Securing Enterprise-Level IoT

Challenges and Solutions Driving Growth of IoT in Business

A Frost & Sullivan White Paper

by Jason Reed, Senior Industry Analyst, Cybersecurity

CONTENTS

INTRODUCTION TO INDUSTRIAL INTERNET OF THINGS

As a part of the ever-expanding Internet of Things (IoT), the Industrial Internet of Things (IIoT) focuses not on consumer products such as wearables and connected home appliances, but on connected devices used by enterprise in streamlining business processes, maximizing efficiencies, and reducing costs. The IoT is increasingly deployed across all industry verticals, including retail, finance, transportation, telecommunications, and healthcare, in addition to industries more traditionally associated with the IIoT.

In the challenging world of IoT, there is often some confusion in distinguishing Machine-to-Machine (M2M) services and the IIoT. M2M is defined as the transfer of information from a device that is mounted on an asset through wired or wireless communication networks, to a software platform that translates the information into useful information for the end user. While this on the surface seems to describe both M2M and IIoT, the two solutions differ in how they achieve remote device access. Traditional M2M solutions often rely on point-to-point communications using hardware modules and either cellular or wired networks. In contrast, IIoT solutions use IP-based networks to upload device data to a cloud or middleware platform.

IIoT solutions use IP-based networks to upload device data to a cloud or middleware platform.

IIoT machines and devices are diverse and varied. They include production machines in traditional industrial settings, but also include among other things the IT that increasingly permeates automobiles, and sensors built into critical infrastructure for proactive maintenance and monitoring purposes. In addition, each device in an IIoT infrastructure may use a different operating system, including a Linux-based configuration, Windows 10, or a custom operating system designed specifically for that device. The number of systems that underpin a single IIoT infrastructure can make securing that network an enormously complex and time-consuming task.

Nevertheless, IIoT adoption is rapidly accelerating because it enables higher productivity and business efficiency. In fact, Frost & Sullivan research predicts that the economic value created by IoT implementation globally across the public and private sectors will reach up to USD 19 trillion by 2022. Business leaders cannot ignore the on-going transition to IIoT if they wish to remain competitive in their respective markets. Some, however, are reluctant to unreservedly embrace IIoT due to security concerns, which are not without merit[1]. Despite these concerns, Frost & Sullivan's research shows that the IIoT is here to stay[2]. So what, then, are some of the ways that the IIoT is benefiting businesses across various verticals?

IIOT: PRACTICAL APPLICATIONS

From manufacturing, to aerospace and automotive, energy grids, and automation in buildings, today's market landscape is rife with examples of the IIoT usage. Below are some of many examples of the application of IIoT in various industries globally.

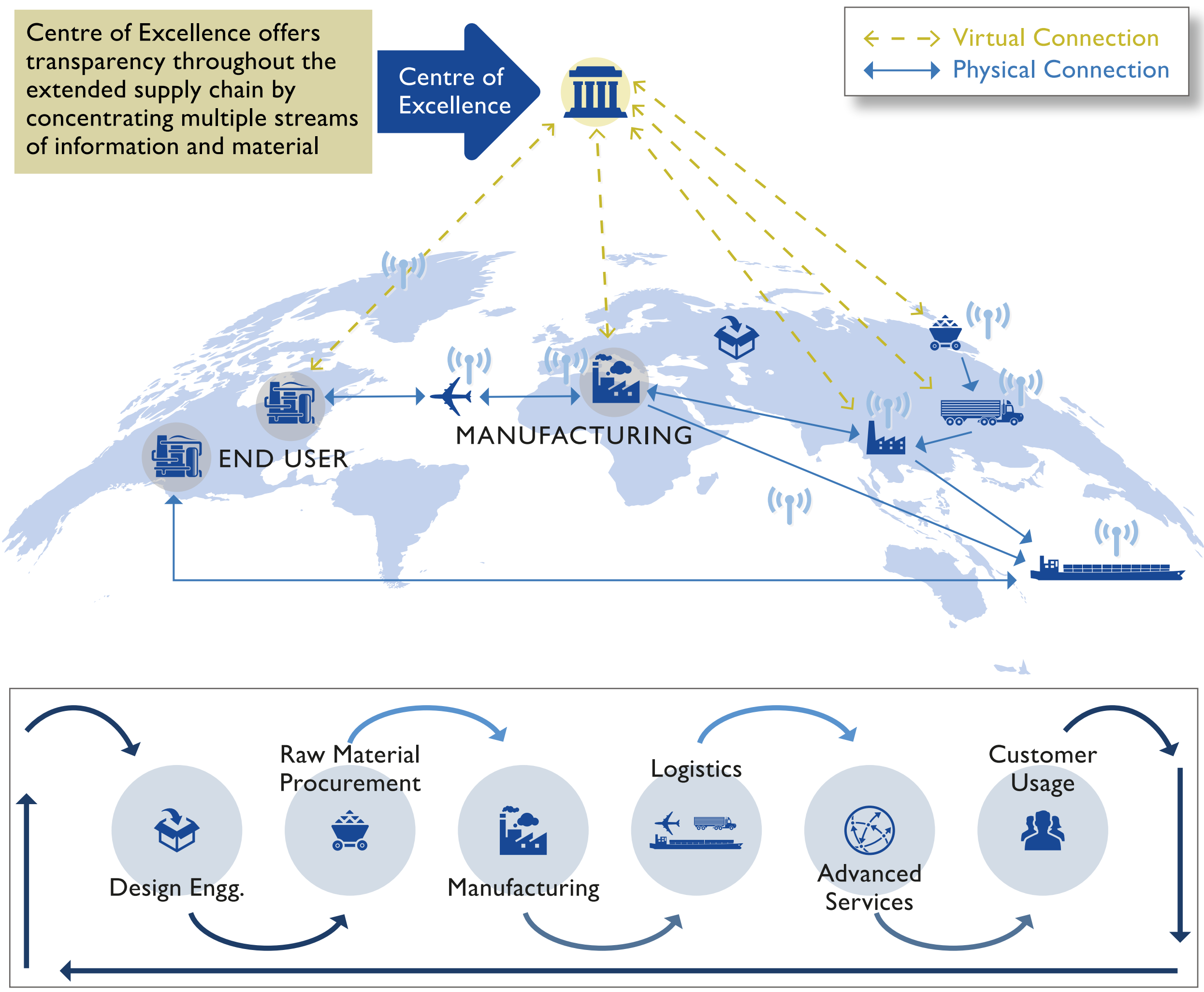
1 Krebs, B. (2016, October 16). IoT Devices as Proxies for Cybercrime. Retrieved from https://krebsonsecurity.com/2016/10/iot-devices-as-proxies-for-cybercrime/

2 Frost & Sullivan (2016, February 12). Internet of Things. Retrieved from https://www.youtube.com/watch?v=71YV0xF-1Ic

Connected Logistics: Redefining Supply Chain Management

The IIoT is redefining how supply chains are organized and monitored. With connected cameras and sensors embedded in devices throughout the supply chain, the IIoT grants organisations unprecedented visibility across all logistical processes.

Exhibit 1: Connected Logistics Workflow



Source: Frost & Sullivan

In this example, Centre of Excellence refers to a centralized command centre where all processes can be monitored individually or as a holistic system, with thousands of connected devices providing real-time feedback at each step of the supply chain. This feedback is created by monitoring the data that is exchanged between each device's "virtual connection", or the connection between endpoints. The enhanced visibility that the centralized command provides across all logistical processes increases efficiency and output while simplifying the task of identifying areas of concern or delays in the supply management chain. What is often overlooked in this process is the need to ensure that each device's virtual connection is uninterrupted and secure, as a disruption at any endpoint could result in a ripple effect that impacts the entire supply chain.

The impact could range from minor productivity losses to, in the event of a serious compromise of virtual connections, a complete shutdown of the supply chain until the compromised virtual connection can be identified and remediated.

Critical Infrastructure: Predictive Maintenance Enabled by IIoT

Embedding connected sensors at the design stage into infrastructure has become common practice in a variety of sectors[3], and nowhere is this trend more important than the maintenance of critical infrastructure that enables the global flow of capital, goods, and services. Utility companies, for example, have been deploying predictive analytics as a means of monitoring their technologies for some time now[4]. With the use of IIoT enabled devices likely to increase in coming years, so too is the sophistication of the connected devices. As well as alerting operators of potential maintenance issues, the emergence of Artificial Intelligence in these devices could result in routine maintenance tasks being performed by the device itself, without human assistance. The advent of AI-enabled IIoT devices will likely have a profound impact on operating procedures for critical infrastructure organisations.

Retailer's Edge: Streamlining Consumer Experience with IIoT Enabled Devices

Amazon's desire to deploy Unmanned Aerial Vehicles (or, more commonly, drones) as part of its delivery service has been the topic of a great deal of debate, but recent developments, including a private trial launched in the UK[5], suggests that this technology is close to being ready for rollout. With proper regulatory support in place, Amazon will be positioned to deliver some goods to consumers within 30 minutes of their ordering.

For heavier products, driverless vehicle start-up Embark[6] has begun deliveries in their self-driving semi-trucks from Texas to California[7]. This marks a new phase in ground-based logistics, as these autonomous vehicles are expected to become more common as time passes.

The Danger of "Everything, Connected"

While logistics, critical infrastructure, retail, and nearly all industry verticals stand to gain from the IIoT, the emergence of "connected everything" poses some significant challenges. Primary among those challenges is ensuring the security of communication between devices and their organisations, as a breach or compromise in security could lead to disastrous consequences for safety, revenues, or both.

THE BUSINESS NEED TO SECURE THE IIOT

Securing the IIoT is not a simple task, as attackers and malicious actors constantly strive to circumvent the security that is baked in to the devices that make up the IoT. And it is increasingly apparent that device

---

3 IIoT Viewpoints. (2017, January 30). Ambyint CEO on Analytics for Critical Infrastructure. Retrieved from https://industrial-iot.com/2017/01/ambyint-ceo-on-analytics-for-critical-infrastructure/

4 Custeau, K. (2017, January 2). Utilities Squeeze Assets with Predictive Analytics. Retrieved from https://blog.schneider-electric.com/utilities/2017/01/02/utility-asset-management/

5 Amazon.com. (2016, December 7). First Prime Air Delivery – Fully Autonomous – No Human Pilot. Retrieved from https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011

6 http://embarktrucks.com/

7 Davies, A. (2017, November 13). Self-Driving Trucks Are Now Delivering Refrigerators. Retrieved from https://www.wired.com/story/embark-self-driving-truck-deliveries/

security is simply not adequate[8] to prevent major breaches. In fact, there have been numerous incidents that demonstrate the inadequacy of existing security measures in a range of industries.

Smart Meters, 2009–2012

Smart meters are designed to maximize efficiency in energy usage and to allow utility companies to charge different rates for usage at different times of day. In addition, smart meters allow utility firms to remotely monitor energy usage. However, as Puerto Rico[9] discovered in 2009, hackers with relatively low levels of sophistication were able to hack smart meters, effectively allowing energy theft worth over $400 million. The FBI, who discovered the hack, was uncharacteristically candid in their assessment, stating, "The FBI assesses with medium confidence that as Smart Grid use continues to spread throughout the country, this type of fraud will also spread because of the ease of intrusion and the economic benefit to both the hacker and the electric customer".

Consumer Automobiles, 2015

Even vehicles that require a driver (as opposed to autonomous vehicles) are susceptible to attacks, as many of their systems and features increasingly rely on IoT connections. In 2015, BMW and Jeep vehicles were successfully hacked, with hackers able to imitate BMW servers and remotely lock and unlock the vehicles. In the case of Jeep, two security researchers demonstrated to a reporter how they could control all the vehicles' systems remotely[10], resulting in the recall of 1.5 million cars.

Retailers, 2013

Target was the subject of a massive breach in 2013, where hackers used malware to penetrate an HVAC company contracted by the retailer, resulting in the theft of the personal data of over 70 million customers. An investigation by security experts at Verizon revealed that once cyber adversaries were inside of Target's network, there was nothing to stop them from gaining direct and complete access to every cash register in every Target store across North America[11].

Power Grid, 2016

During the on-going conflict in the Ukraine, hackers gained remote access to the Ukrainian power grid[12] and cut power to more than 200,000 customers. The breach allowed hackers to install custom firmware, delete master boot records and shut down telephone communications.

Man-in-the-Middle Attacks

One of the main concerns in securing the IIoT is the attack strategy deployed by hackers termed man-in-the-middle. In this case, the attacker intercepts communication between two systems, posing as the original

8 Accenture. (2015). Security for the Internet of Things: A Call to Action. Retrieved from https://www.accenture.com/ca-en/insight-security-internet-of-things

9 Krebs, B. (2012, April 12). FBI: Smart Meter Hacks Likely to Spread. Retrieved from https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

10 Greenburg, A. (2015, July 21). Hackers Remotely Kill a Jeep on the Highway—With Me in It. Retrieved from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

11 Krebs, B. (2015, September 21). Inside Target Corp., Days After 2013 Breach. Retrieved from https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

12 Zetter, K. (2016, March 3). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

"sender." The attacker can then "trick" the recipient into thinking they are still getting a legitimate message. Within the IIoT, such an attack could, for example, fake temperature data in order to force a piece of machinery to overheat[13], causing serious financial damage to the organisation.

This type of attack could be particularly dangerous in the case of autonomous vehicles, where an attacker poses as the server guiding the drone or ground vehicle, potentially causing enormous financial and physical damage. What is clear is that organisations must match their deployment of the IIoT with equal attention to securing their networks.

SECURING ALL DEVICES ACROSS PLATFORMS AND AUTHENTICATION METHODS

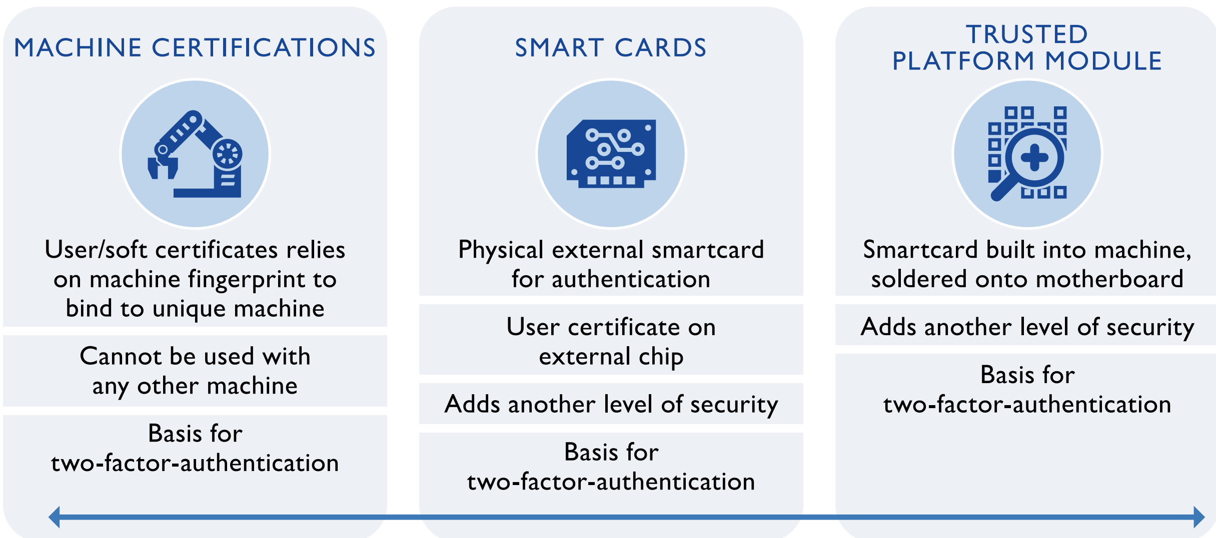
In order to prevent compromised devices or a disruption in the IIoT, it is essential that enhanced security is "baked in" to the infrastructure at the planning stages of implementation. Retroactively implementing enhanced IIoT security is costly, inefficient, and cumbersome.

The most effective way to prevent a man-in-the-middle attack, for example, is by implementing an encrypted Network as the primary mode of communication between virtual connections in an IIoT infrastructure. The encrypted communication tunnel between two or more devices, will secure all information that passes through it. When communications are encrypted, a potential man-in-the-middle would be unable to read the data that they are monitoring.

To achieve this, the solution will need a Digital Certificate and all the devices that it communicates with will need a certificate as well. As data flows between devices, required keys are swapped in a "handshake" and all data remains encrypted until it reaches its final destination.

Certificates are used in each step of the authentication process in a VPN security system for IIoT. Some authentication methods used in IIoT security are found in exhibit 2.

Exhibit 2: VPN Security Certifications



Source: Frost & Sullivan

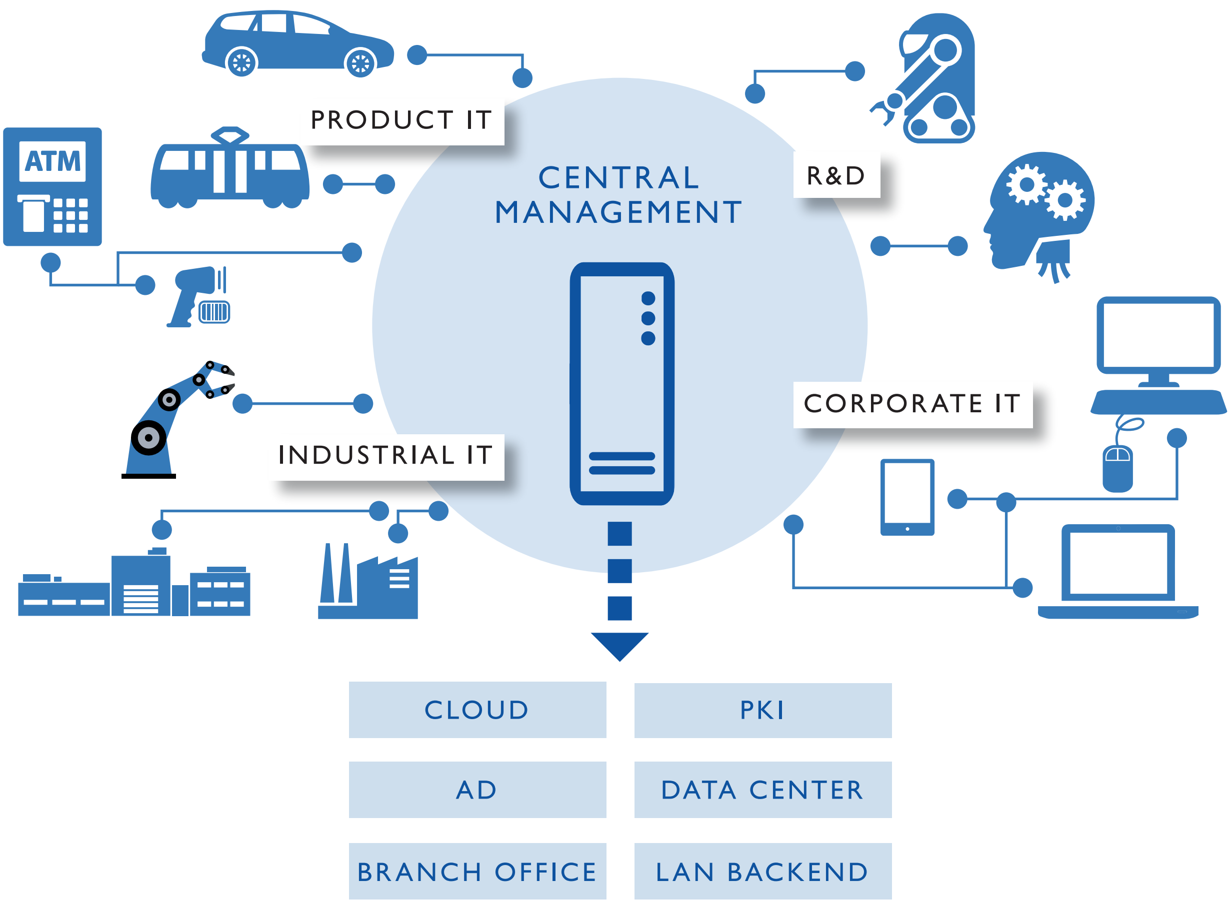
13 Simko, C (2016, February 26). Man-in-the-Middle Attacks in the IoT. Retrieved from https://www.globalsign.com/en/blog/man-in-the-middle-attacks-iot/

Authentication at each step along the encrypted communication channel is essential to ensuring that the IIoT is secure and resistant to the types of IoT compromises outlined above that can significantly damage business processes. Most organizations do not, however, have the in-house expertise to ensure that their IIoT is properly secured. As a result, Frost & Sullivan recommends a specialist VPN MSSP to mitigate security risks in the IIoT.

NCP ENGINEERING SOLUTIONS FOR IIOT

NCP, a secure communications software vendor, has incorporated best-practice communication and security into their offering for IIoT. NCP's solution consists of "IIoT gateways" and "IIoT clients", both software, for different operating systems, including Linux, Windows 10, and specific embedded operating systems in devices in the IIoT. Functioning both as a classical and IIoT VPN connection, the solution, through its Central Management system, has evolved to bridge the gap between production IT located in devices and machines and operational IT. Traditionally, these two IT systems often do not operate under the same management platform, rendering navigation between the two cumbersome and difficult.

Exhibit 3: NCP VPN Solution for IIoT



Source: NCP Engineering

With certificates exchanged at each stage in their IIoT solution, the system revolves around IIoT Clients, which are lightweight and installed on endpoints, Central Gateways, and a Central Management component The process begins with Clients, which are installed directly on systems or machinery, while the IIoT Gateway manages encryption and ensures the certifications from each device meet the standards of a trusted Certification Authority. Additionally, the encrypted communications are in accordance with Suite B Cryptography to ensure the highest level of encryption sophistication available.

One key differentiator for NCP Secure Communications is its Management component, which provides visibility across all components. This is a central management system available to administer the Clients and the Gateway in the IIoT architecture. It allows full central configuration of the IIoT components, including machine certificates. This type of holistic solution, which provides centralised visibility across the IIoT, allows administrators to proactively manage their IIoT Clients and their IIoT Gateways within the same network architecture.

CONCLUSION

While an encryption solution for IIoT networks is an essential first step, organisations such as NCP Engineering enhance the user experience by operating not only as a secure communications vendor, but as a form of systems integrator that can link existing IIoT infrastructure into a centralized command centre. In effect, a system of this sort that includes a central management component, builds a bridge between the Corporate IT, the Product IT and the Industrial IT. This enhances the end-user experience by simplifying the integration process and creating a high degree of visibility across the whole IIoT system. This type of technology should offer reassurance to those suspicious of the security of IIoT, and ease the transition from a traditional organisational process to an IIoT native workflow.

FROST & SULLIVAN

NEXT STEPS

Schedule a meeting with our global team to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.

Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.

Visit our **Digital Transformation** web page.

Attend one of our **Growth Innovation & Leadership (GIL)** events to unearth hidden growth opportunities.

SILICON VALLEY
3211 Scott Blvd
Santa Clara, CA 95054
Tel 650.475.4500
Fax 650.475.1571

SAN ANTONIO
7550 West Interstate 10
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

LONDON
566 Chiswick High Road
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

877.GoFrost
myfrost@frost.com
www.frost.com

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organisation prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?