IDC Manufacturing Insights

T E C H N O L O G Y S P O T L I G H T

Maximizing the Value of the Secure, Networked Plant

May 2017

Adapted from *IDC FutureScape: Worldwide Manufacturing 2017 Predictions* by Kimberly Knickle, et al., IDC #US41837317

Sponsored by Tempered Networks

This paper examines the changing requirements of manufacturers as they increasingly depend on the convergence of informational technology (IT) and operational technology (OT) in the plant and in their overall operations. In addition, we highlight our worldwide manufacturing predictions that emphasize the importance of more integrated IT and operations and a business approach to security. We also review the role of Tempered Networks' Identity-Defined Networking (IDN) platform, which can help manufacturers seamlessly secure and isolate network segments and transform vulnerable IP-enabled devices into hardened, invisible assets. As a result, Tempered Networks' technology increases productivity and supports manufacturers' path to digital transformation.

Introduction

Technology continues to reshape the manufacturing industry, especially as IT and OT increasingly come together to improve productivity, innovation, and digital transformation (DX). Manufacturers want to work smarter using digital technologies in their products and processes and throughout the value chain. Some of the major factors impacting manufacturing are as follows:

- **The DX delta.** The best-performing manufacturers can successfully adopt new technologies and leverage their technical resources for maximum value in all aspects of their business, including in the plant. Industry leaders keep transforming how they operate, and manufacturers that want to remain competitive will make innovation as high a priority as, if not a higher priority than, productivity. These manufacturers not only are able to innovate in their products and processes but also are more innovative and agile in the way they work with partners, suppliers, and customers.
- **Revolutionizing industrial processes.** Digital technologies are increasingly embedded in the physical world: Internet of Things (IoT), robotics, and 3D printing are on their way to becoming mainstream technologies that can transform productivity, quality, and efficiency in industrial applications and processes. IDC forecasts that by 2025, 80 billion IoT (sensor-enabled) devices will be online, creating 180ZB of data. In 2019, worldwide spending will reach $135 billion for robotics and more than $31 billion for cognitive systems. These digital technologies must integrate more easily and more often with older investments already present in the plant, including OT, to create a single system that supports increasing demands placed on manufacturers' operations. Scale will no longer be the deciding factor of who leads the market.
- **Data as digital capital.** Manufacturers are seeing growth in data and access to data. However, IDC estimates that less than 10% of data is effectively used, partly because manufacturers often have limited access to data when they need it. Data must be treated as a digital asset, or digital capital, to improve experience, provide insight, influence decisions, and enable innovation and business agility. Leading manufacturers are already creating new, secure access points to data

for themselves and their value chain through networks or industry clouds that hold asset performance data for benchmarking performance, predicting maintenance, and driving the initiation of existing services or the creation of new services. Data as digital capital is also why manufacturers need to address questions about secure access to product or equipment data and ensuring data privacy and security now.

Digital Business Transformation in Manufacturing

As much as we like to measure the health of the manufacturing industry based on productivity, the benchmarks of the future are innovation and digital transformation. DX — using technologies to create new ways of operating and growing businesses — is already under way. Even now, we see manufacturers that can successfully apply new technologies to their products, processes, and business models are leaders in the industry.

In this paper, we focus on two of our predictions that we think are very relevant to manufacturers as they maximize the value of their plants with secure, networked connections throughout their operations:

- **Integrated operations.** By the end of 2020, 50% of manufacturers will derive business value from the integration of supply chain, plant operations, and product and service life-cycle management.
- **Business security essentials.** By 2018, a proliferation of connected information, instrumentation, and decision cloud ecosystem networks will drive manufacturers to redesign their security architectures.

Integrated Operations

Manufacturers large and small recognize that today's business demands require new processes and new organizational coordination. However, manufacturers' IT portfolios are full of business applications that serve one line of business or one set of business processes. They manage silos of information pertaining to and focusing on their dedicated processes. These silos are limiting the ability of organizations to maximize investments in digital transformation and new technologies such as big data and analytics, cloud, mobile, and new collaboration tools. In response, manufacturers are changing how they use enterprise applications. Today, companies are actively figuring out how to provide information effectively across their organization and even externally with suppliers and customers.

To this end, using information in a coherent way will be central. Standardize, integrate, and connect are the keywords here. Companies will leverage their existing enterprise applications to create a "digital core" that delivers all business applications (PLM, SCM, manufacturing, CRM, service, etc.). The outcomes will be more streamlined product and product-related releases, responsive and integrated supply chain and manufacturing processes, timely digitally enabled services, and stronger relationships with customers.

We think this change is happening fairly quickly as manufacturers today are already investing in new, adaptable IT applications and integration to create a digital thread from product development to factory planning, manufacturing, supply chain execution, and service delivery. In a way, it's about "next" practices, not "best" practices. IT and OT convergence will complement these efforts as well.

Business Security Essentials

New business conditions, increasing complexity in manufacturing supply chains, and more integrated operations necessitate a better approach to security that unites business risk with technology security requirements and execution. Cybersecurity threats continue to grow in number and become more sophisticated. Manufacturers expect the integration of IT and OT systems to provide them and their suppliers with visibility down to individual devices and machines. New services, connected products, IoT-enabled assets in the plant and the supply chain, increasing partner collaboration through the cloud, and more integration with customers all create security vulnerabilities. The business risk makes it essential for manufacturers to move ahead quickly.

This situation is posing many more security challenges for manufacturers and not just related to network vulnerability and plant floor malware. Manufacturers will invest more in next-generation security technologies and will redefine next-generation security architectures to protect their business IP and operations. Manufacturers should start by taking advantage of the built-in capabilities in their applications and review their overall security approach to make sure it considers new business requirements. They should also look at the possibilities new technology advances offer.

Considering Tempered Networks

Tempered Networks' platform is designed to help enterprises move away from address-defined networking to identity-defined networking, where communications can be established only between trusted cryptographic identities (CIDs). The company's IDN platform starts with zero trust and uses a point-and-click orchestration engine, the Conductor, to create secure overlay networks based on device whitelisting. It enables enterprise IT to achieve identity assurance and granular network microsegmentation across networks.

By leveraging the Host Identity Protocol (HIP), Tempered Networks makes device IP conflicts a nonissue. Every endpoint that joins an IDN fabric is based on unique host identities, not an IP address. Further, HIP is compatible with IPv4 and IPv6 applications, utilizing customized IPsec tunneling for confidentiality, authentication, and integrity of network applications.

Tempered HIP services are available on a variety of platforms and form factors, including physical hardware, virtual appliances, or the cloud. They are also available to run on clients (laptops, phones) and servers, and they can be embedded in custom hardware or in applications. HIP services are topology and protocol agnostic and can provide connectivity over any mix of wired, Ethernet, serial, or cellular communications.

When deploying HIPswitches, a manufacturing firm effectively builds a private, segmented, and encrypted overlay network between devices. The overlay network is completely agnostic to and isolated from the "underlay" network, meaning it can leverage existing enterprise investments in network infrastructure. The IDN platform is designed to reduce network complexity while improving a manufacturing operation's security posture through device cloaking, which hides the IP footprint of a device or anything within a secure overlay.

Challenges

Manufacturers also should consider the fact that new IT investments and IT projects in the plant and across their operations come with challenges, many of which can be addressed with advance planning. Some of the specific issues we see most frequently are as follows:

- **Change management.** Companies need well-defined people and process changes, a change management program, and executive support. Change management is especially challenging when IT and OT teams have not worked closely together with common goals in the past.
- **Limited staff with advanced IT skills.** Insufficient staff with the right skills can significantly impede operations or delay responses to IT issues. The challenge of the skills gap becomes particularly sensitive in the plant, where any delays in the production line can translate into thousands of dollars of losses in a matter of minutes. OT systems often present significant difficulties because of IP conflicts, security vulnerabilities, and incompatible legacy systems, which also hinders converged plantwide Ethernet initiatives. Being able to connect and streamline these systems can help significantly improve manufacturing processes by allowing companies to better leverage the data and information resident in their systems.

- **Incremental versus transformative.** Manufacturers have a tendency to favor incremental improvements over transformational improvements or the development of road maps that are necessary for long-term success. In this case, there is a need to recognize that the security of the plant cannot be addressed by merely implementing firewall rules or other perimeter-based security devices. Plant security must be automated, intelligent, dynamic, and pervasive.

While Tempered is taking an innovative approach to delivering an integrated platform that addresses problems that afflict networking and security, it faces a few notable challenges in the marketplace.

First, Tempered's approach, based on HIP and cryptographic identity, is a departure from traditional networking and security offerings based on TCP/IP. Despite its inherent strengths, HIP represents a new approach to managing and securing networks, and IT professionals must familiarize themselves with the technology before they become comfortable using it. Typically, IT practitioners initially perceive the risks associated with adopting a new technology before they appreciate the benefits that can accrue from using it. IT staff can be particularly skeptical when technologies advertise themselves as being easier to use and maintain.

Additionally, Tempered faces entrenched competition from established networking and security vendors. These vendors have large installed bases of customers and are difficult to displace. Moreover, several venture-funded security start-ups have joined the fray in the past few years, many of which claim to provide solutions that offer software-defined security. Amid such a crowded and competitive market, Tempered will have to ensure that it stands out from the crowd with a clearly articulated value proposition and sustainable differentiation.

Finally, as a start-up vendor itself, Tempered Networks must overcome customers' concerns about its long-term viability in the marketplace. In response, Tempered will cite the proven nature of its HIP-based technology, a growing roster of customers in the manufacturing vertical, and an engineering team that has grown sixfold since 2014.

Conclusion

It's critical that manufacturers take steps toward digital transformation and securely integrate their operations now. We offer the following guidance to manufacturers as they move forward:

- **Evaluate** your relative maturity in the adoption of new technologies and, more importantly, your ability to translate those technologies into business value and digital transformation. IT and line-of-business staff will need to work together in the selection and implementation of new technology. Make sure that IT and OT teams are working together.
- **Review** your foundation to make sure it's ready for increasing levels of digitally enabled products and processes. Today, your foundation includes components such as core applications, datacenters, network connectivity, cloud, and mobile devices throughout the business, including in the plant.
- **Create** a single source of the truth for your business. Data within your enterprise and from connected products, supply chains, and assets will be the starting point for new initiatives. This fundamentally depends on secure, flexible access to data, whether in applications, databases, devices, or external data sources.
- **Cultivate** your access to IT talent, whether within your own company or through partners large and small. They should be able to help you adapt to new technologies quickly and effectively and maximize the outcomes from your investments.
- **Select** a partner that understands your industry and your business requirements and is willing to help you maximize the value you receive from your investment over time.

IDC believes that the market imperative of digital transformation and the continued ascent of cloud computing and IoT are driving the need for a profound confluence of networking and security. While software-defined networking (SDN) has arisen as an architectural response to the networking requirements of cloud computing in the datacenter and SD-WAN has emerged to address new connectivity requirements at branch offices and remote sites, there is an opportunity for a new variation that unifies networking and security to address complexity and connectivity challenges that span the entire network.

Tempered Networks perceives this market need and has proposed its IDN platform as a solution to the problem. With IDN, Tempered has acutely anticipated the secure networking requirements spawned by the pursuit of digital transformation and the robust growth of cloud computing. By enabling enterprise customers to secure network segments and to transform vulnerable IP-enabled devices into hardened, invisible assets, Tempered Networks' IDN platform positions the company to address a market opportunity that will extend from the near-term needs of enterprise networks today to the long-term requirements that will help manufacturers innovate and continue their digital transformation journey in the years ahead.
