BlackBerry
Intelligent Security. Everywhere.

White Paper

Endpoint Security for Smart Manufacturing: Protection from the Factory Floor To the Supply Chain

TechTarget | Custom Media

Manufacturers have embraced digital transformation in many ways to become more data driven, make more intelligent decisions, improve flexibility and cut time to market. This digital transformation means capturing more and more data on many new and different types of endpoints, both in their factories and throughout their logistics channels. But with all that data comes added security risks. This white paper looks at those threats and their implications, and offers concrete suggestions on ways manufacturers can minimize cyber-risk.

The manufacturing sector has gone through a number of important and strategic changes in recent years, from sophisticated new production equipment and intelligent parts handling to global, integrated and predictive logistics. This has allowed manufacturers to adopt improved processes ranging from just-in-time manufacturing, lean inventory, smart, connected products, statistical quality control and global—yet truncated—supply chains.

For manufacturers, this digital transformation has yielded many tangible benefits, heavily based on the ability to capture, process, share, analyze and act on vast amounts of new data. Much of that data is coming from a proliferating volume and variety of endpoints throughout manufacturing workflows. And, with this digital transformation throughout the manufacturing sector, has come a challenging flip side to its many benefits: an expanding set of cybersecurity threat vectors.

A stark reality is that the manufacturing sector has historically been later than other industries to adopt IT hardware and software that could make their operations more efficient and intelligent—and more secure. Research indicates that manufacturers spend an average of between 2% and 4% of their overall IT budget on cybersecurity, substantially lower than the 5% to 8% of budget spent across all industries.[1]

Ironically, one of the cybersecurity challenges facing manufacturers is that, unlike highly regulated industries such as healthcare and financial services, the manufacturing sector lacks a signature compliance mandate. It is therefore imperative that manufacturers take steps to address risks stemming from vulnerable global supply chains and new initiatives such as industrial internet of things (IoT).

A stark reality is that the manufacturing sector has historically been later than other industries to adopt IT hardware and software that could make their operations more efficient and intelligent—and more secure.

1 "Tech Chiefs Plan to Boost Cybersecurity Spending," wsj.com, December 30, 2019.

Fortunately, as manufacturers' digital transformation efforts have helped them understand and appreciate the strategic and operational value of all the data being collected and shared by their endpoints, that reticence in investing in cybersecurity is starting to change. For instance, research from Enterprise Strategy Group notes that 68% of manufacturing organizations intend to increase their cybersecurity spending in 2020 compared to the previous year, making it one of the industries with the highest increased commitment to cybersecurity.[2]

Undoubtedly, a key driver to manufacturers paying more attention and committing more resources to cybersecurity is the increased digitalization of their operations on the factory floor and in their global connected supply chains. With that increased use of technology—and the increased magnitude and diversity of endpoints—comes a stunning increase in the sheer volume of unstructured, semi-structured and structured data. So, with more points of entry for attackers, an exponential expansion of the attack surface, and digital data increasingly driving business outcomes of manufacturers, it is essential for manufacturers to take endpoint security seriously.

Endpoint Cyberthreats in Smart Manufacturing

When thinking about cybersecurity challenges in the manufacturing vertical, it's important to keep in mind that manufacturing is not a single, monolithic market. Instead, it is valuable to think of manufacturing as an intertwined set of functions that take place in three unique, yet related, areas: on the factory floor, in business operations centers, and through integrated—and often global—supply chains.

Obviously, there are different types of endpoints in each segment—and this is a vital part of the discussion since the overwhelming majority of cyberattacks are endpoint-targeted. Data from IDC indicates that 70% of cybersecurity attacks are initiated at an endpoint, and nearly one-third of enterprise IT decisionmakers consider endpoint security to be a significant component in their overall cybersecurity strategy.[3]

The business operations center endpoints include desktops, notebooks and, to a lesser degree, tablets and smart phones. This is undoubtedly the type of endpoint landscape most organizations are intimately familiar with, and which attackers often attack with a wide

When thinking about cybersecurity challenges in the manufacturing vertical, it's important to keep in mind that manufacturing is not a single, monolithic market.

2 "Cybersecurity spending trends, 2020," csoonline.com, February 12, 2020.

3 "Improving Endpoint Security Needs To Be A Top Goal In 2020," forbes.com, October 27, 2019.

range of methods, from mobile malware and advanced persistent threats to ransomware and theft of account privileges. Manufacturers traditionally have protected their users' computers by air-gapping them between the factory floor and office environments—something that clearly is no longer an option.

On the factory floor, traditional computer formats also are relevant as ways to control and command assembly line equipment, but robotics equipment and other sensor-based endpoints also are relevant. There also are a number of highly specialized and unique endpoints that may look nothing like traditional computers—such as smart glasses—but capture and store proprietary data, such as intellectual property drawings that can be hacked and compromised.

In the supply chain, things like vehicle-mounted computers, wearable computers, and RFID-based, location-aware, application-specific sensors are capturing huge amounts of unstructured data in various formats as part of edge computing and IoT initiatives. For instance, a company manufacturing potato chips is using smart glasses in their workflows—an admittedly innovative use case, but one where new, unanticipated endpoint security risks now can occur.

Needless to say, all of these different types of endpoints represent fertile ground for attackers and must be part of a manufacturing organization's comprehensive cybersecurity framework. For instance, 48%[4] of United Kingdom-based manufacturers report they have been victim of a cyber attack, making cybersecurity a critical initiative for manufacturers. There also are more malicious actors targeting private-sector organizations like manufacturers as geopolitical tensions drive more cyberattacks. Think of it this way: as manufacturing functions get smarter and generate more data, they attract more attackers, who also are getting a lot smarter. An important example is the global automotive manufacturer Honda, whose operations were recently hit by a ransomware attack, causing a production shutdown.[5]

Addressing Cyberthreats in the Fast-Changing Manufacturing Sector

In order to address the growing number and diversity of cybersecurity threats, manufacturers need to acknowledge the expanding threat vectors and take concrete steps now to prepare for and prevent the attacks. This requires a heightened commitment to more tightly secure their endpoints against a wider variety of threats, and to be proactive in looking for new types of solutions with a wider array of features to detect, defend against and mitigate the impact of cyberattacks.

Obviously, some of the ways manufacturers need to fortify their defenses are not necessarily based on technology, per se. These include end-user training, especially for manufacturing and supply chain employees without a lot of computer expertise, as well as studying and addressing good cyber hygiene by users.

4 "Nearly half of UK manufacturers victims of cybercrime," Internet of Business, 2020.

5 "Honda could be victim of ransomware cyber attack," The Telegraph, June 8, 2020.

But from a technology-adoption standpoint, organizations need to embrace solutions with essential functionality to provide much tighter endpoint security. These include:

- Unified endpoint management to break down management silos and reduce complexity.
- Unified endpoint security to simplify security policies, updates and enhancements across multiple endpoints and different formats at the same time.
- Protecting the endpoint in a way that also protects users and the data with which they are entrusted.
- Increased use of security analytics to spot trouble spots before they flare up into actual data breaches.
- Increased use of automation to take the burden off badly stretched internal security resources.
- Support for essential endpoint security frameworks and principles, especially Zero Trust.
- Support for AI/machine learning to act as a force multiplier in endpoint threat detection, prevention and remediation.
- Single-pane-of-glass management.
- Continuous authentication.
- Support for containerization for security micro-segmentation.
- Integrated software developer kit for build-your-own extensions.

How BlackBerry Solutions Fortify Endpoint Security

BlackBerry® endpoint security solutions offer a comprehensive and market-proven security framework, as well as highly regarded individual point products for a number of unique endpoint requirements. BlackBerry® suite-based solutions all fall under the umbrella of its BlackBerry Spark® security management framework, which is powered by artificial intelligence and is available in both cloud and on-premises versions.

BlackBerry Spark® Suite includes:

- **BlackBerry Spark® Unified Endpoint Security Suite**, comprising endpoint protection, endpoint detection and response, mobile threat defense and continuous authentication.
- **BlackBerry Spark® Unified Endpoint Management Suite**, which includes a software development kit, digital rights management and identity management.
- **BlackBerry Spark® Unified Endpoint Management Express Suite**, which includes device management, secure productivity applications and popular Microsoft® applications.
- **BlackBerry Spark® Suite**, which comprises Unified Endpoint Suite and the full Unified Endpoint Management Suite.

The individual BlackBerry endpoint security products that are part of those suites include:

- **BlackBerry® Protect**, which helps users defend against zero-day threats, mobile malware and fileless attacks, among others.
- **BlackBerry® Optics**, which provides users with the endpoint visibility necessary for exacting functions, including root cause analysis, threat hunting and incident response.
- **BlackBerry® Digital Workplace**, which helps users access a wide range of applications, data, and tools from their home offices, remote offices or other facilities. BlackBerry® Digital Workplace was designed with security as a prominent requirement from the very start, allowing users to securely use any device to access applications and services behind a corporate firewall.
- **BlackBerry® Persona**, which provides users with analytics-driven security via secure containers and information captured, analyzed and served from a network operations center to determine real-time risk scores, without impacting user experience.

Additionally, manufacturers can secure their remote workers' data, applications and identities with BlackBerry® Work from Home. This solution helps organizations solve the work-from-home security challenges that many manufacturers are now facing at unprecedented levels with so much of their workforce doing their jobs remotely, by enabling remote users to securely access applications, databases, websites, content and files.

Manufacturers also should take advantage of BlackBerry® AtHoc®, a suite-based approach to security event crisis management and critical communications that is part of the BlackBerry® IoT solutions group. AtHoc® helps manufacturers make and implement real-time security decisions through end-to-end event management, including visibility into

personnel safety, emergency mass communications, cross-enterprise collaboration and situational awareness.

Conclusion

As manufacturing organizations increasingly add technology throughout their business and operational workflows, they are enjoying the benefits of a more intelligent, automated and prescriptive set of systems and applications. The vast range of new types of data—and massive amounts of that data—is helping manufacturers shorten their supply chains, become more responsive to fast-changing customer requirements, and improve productivity and profitability.

But smart manufacturing also is more vulnerable, due to the proliferation of more and different kinds of endpoints in the business offices, on the factory floor and throughout global supply chains. This has raised the stakes immeasurably on manufacturers to fortify their cybersecurity defenses, especially at the endpoint.

Manufacturers looking to withstand the growing onslaught of cybersecurity threats should investigate the solutions and expertise of BlackBerry®. With a long, established history of endpoint leadership, BlackBerry® is uniquely qualified to understand how, where, and when both traditional and new endpoints are being used in manufacturing applications, and where the new threats are. BlackBerry® is a formidable ally for manufacturers looking to secure their data and all their digital assets.

To learn more about all the ways that BlackBerry helps to secure their customers, visit: https://www.BlackBerry.com

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 150M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow @BlackBerry.

This content was commissioned by BlackBerry and produced by TechTarget Inc.

BlackBerry
Intelligent Security. Everywhere.