WHITE PAPER

Security for Modern Manufacturing

Embrace the Factory of the Future with Confidence

Executive Summary

Manufacturers engage in a constant search for improvement — in facilities and operations, logistics, product quality, information systems and business practices. New technological frontiers like the Internet of Things (IoT), 3D printing, robotics and big data present opportunities to enhance production, quality, efficiency and cost savings. They can also present new risks to your organization and your supply chain if security considerations are overlooked.

Security doesn't have to act like a hand brake on the forward progress of your technological innovation. Instead, it should work to foster more optimization and improvement in manufacturing. As more manufacturers move further into the cloud and IoT, there is an opportunity to secure and strengthen the integrations required to make these technological advancements count. As sensors, switches and all kinds of devices from the shop floor to the supply chain begin to churn out data, you need a strategy to keep up and a single pane of glass to view your important data and systems.

Securing Your Integrations and Intellectual Property

If you're going to take advantage of interconnected factory equipment, devices and data, you're going to need a security strategy. Consider this sobering statistic from the PwC *2016 Global State of Information Security Survey:* theft of "hard" intellectual property (IP) such as product designs doubled in 2015, while loss of "soft" IP like business

What you will learn

- How to protect and enhance manufacturing with security
- The importance of risk assessment
- The value of targeted threat hunting
- The power of unified visibility
- Why communication and training are vital

Who Should Read This White Paper

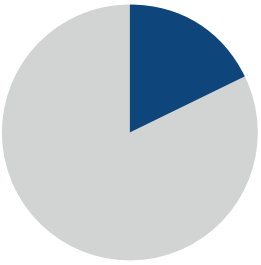
» CISO/CSOs
» CIOs
» CFOs
» Directors of Security/IT
» Security Architects

processes climbed 27 percent over the year before.[1] While credit card data and credentials may be the primary target in the retail and financial space, the manufacturing sector needs strong protection for its intellectual property, designs, patents and formulas.

Many organizations are already examining ways to leverage innovative cloud-based cybersecurity solutions to manage potential risks to IoT. Risk-based cybersecurity frameworks such as the NIST Cybersecurity Framework, or ISO 27001, can also provide helpful guidance for establishing security practices.

In the interconnected world of modern manufacturing, you're only as secure as your integrations. Make sure you have visibility into the sensitive data that traverses your supply chain network. Work to close any security and accountability gaps between you and your suppliers. Apply protection across your trusted and untrusted networks and set limitations on who can access sensitive data.

Your level of strategic and operational preparedness can set you apart, make you more resilient to cyber threats and ensure that you retain customer trust. The following steps can help you stay secure without constraining the ability to innovate and grow.



Only 18% of IT security professionals believe their company's cybersecurity program is in a "mature" stage.[2]

Step 1: Identify Your Most Valuable Assets and Assess Your Risk

It may sound basic, but you must be able to identify your most valuable data assets in order to prevent them from being stolen. For manufacturers, it is usually intellectual property related to formulas, designs, patents, mining rights and resource locations. This information is sought by cybercriminals — either for corporate or state-sponsored espionage or theft, or worse, for disruption to critical infrastructure.

Start by assessing what data you are storing, where it resides and who can access it. For sensitive information, label it, and grant access only to the most limited set of people who need it, placing stringent policies and controls around its use. Administrator credentials are a hacker's keys to the kingdom — the more people who have them, the more avenues for attack. Other more sophisticated approaches and technology can also help protect your trade secrets, including encryption, digital rights management and persistent document tagging and policy-driven data protection.

To understand risk across your manufacturing operations, you must also examine the movement of data and messages between networks — especially when data is moving between extremely different levels of trust. For example, when sensitive information jumps between the IT network and the manufacturing network, or from the manufacturing network to the safety network, you may need to apply stronger security and policy controls.

Step 2: Think Like a Hacker

The best way to outsmart your adversaries is to think from their perspective. Identifying your most valuable data assets and examining how they are stored and accessed is a smart first step. Now, you need to go a step further.

Testing is a crucial and ongoing component of an effective security program. Engage qualified security experts that will emulate hackers using real techniques and evasion methods to validate your security effectiveness across networks, endpoints, IoT and mobile technology. Regular penetration testing should also include phishing techniques to identify weaknesses in the human side of your security program.

Penetration testing of IoT devices using real world scenarios can help analyze weaknesses in these new devices, help with debugging and reveal methods of hardware exploitation. Targeted threat hunting is another way to validate your current security posture. Targeted threat hunting produces valuable, actionable insight into the presence of threats and deficiencies in the security stack.

For many manufacturers, security has become a continuous, multilayerd quest to improve prevention while minimizing the duration and impact of the stealthy attacks that bypass even strong defenses. Targeted threat hunting is a proactive service that not only finds indications of compromise, but also provides context and analysis of a breach to help prevent similar intrusions.

Targeted threat hunting relies on security professionals who possess a highly specialized background and skills to effectively seek out and identify targeted and advanced adversaries. There are four essential capabilities required, including:

- Deep experience with advanced adversaries and varied tactics
- Sweeping visibility into threatened environments
- Access to ongoing, active research driven by field engagements
- The ability to correlate data from many vantage points and cohesively analyze it.

Information security professionals now know that completely eliminating the possibility of a breach is an unrealistic goal. Even layered security technology can no longer provide a complete defense. An effective security program accounts for eventual compromise and takes steps to rapidly identify, contain and eradicate threats inside the network.

When it comes to targeted threats against your critical manufacturing network, it may not be enough to follow standard intrusion detection and incident response (IR) protocol. Motivated adversaries anticipate standard IR doctrine and they train to avoid and bypass these measures.

This is where security researchers with direct experience combating these threat actors are invaluable. Look for a security provider that has been performing intensive inspections of a variety of computing environments for many years. In addition to familiarity with the security operations of multiple industries and different-sized organizations, you want a targeted threat hunting team that has firsthand experience with a range of adversaries using a full spectrum of tactics to achieve their goals.

Step 3: Combat Threats with Unified Visibility

If organizations had the foreknowledge of what to look for, many threats would be prevented. Now, more than ever, manufacturers need unified visibility across their environment. As more manufacturers move to the cloud, the critical integration layer is often overlooked, as well as the large amounts of data coming from IoT devices.

Sensors, switches and various devices from the factory floor and along the supply chain are churning out massive amounts of data. Manufacturers are faced with a complex environment with multiple cloud apps and multiple data sources. While each of these systems serves a purpose, manufacturers still need the integration layer in order to realize the full value of their cloud environments —and unified visibility to be able to secure them properly.

The ability to combine threat data from multiple sources and analyze it intelligently affords powerful protection against advanced threats. Unified security visibility goes beyond viewing your manufacturing environment through a single pane of glass. It should also enable you to learn from other computing environments around the world.

Find a security provider with the ability to collect, correlate and analyze data from network security sensors, log data, endpoints and IoT devices. This should include a flexible platform to interrogate systems' file and registry settings, process launch patterns, process memory and encoding schemes. With access to the latest threat intelligence and analysis, it becomes possible for you to know what is happening now, how it's happening, who's behind it and what they may want from your organization.

A threat intelligence service primed with global visibility across thousands of client networks that uses proprietary toolsets for analysis will deliver early warning and actionable insights to help you reduce risk.

Step 4: Keep Security Top Of Mind with Your Employees and Partners

Humans remain the weakest link in any security program. One of the most powerful defenses against cyber attacks is an informed and vigilant workforce. A successful security program relies on employees, partners and suppliers having strong awareness of security policy and an understanding of their role in supporting security and privacy.

Instead of relegating security to the boardroom and IT, make communication about risk and prevention strategies a priority with your employees and partners. Hackers know that humans are a particular point of weakness in any organization's defenses. Because most workers are helpful and trusting, the hackers employ attack techniques to exploit these qualities.

Your security program should include periodic employee training on security for everyone from the boardroom to the factory floor. It should also clearly communicate security requirements to supply chain partners. These components are just as vital as security technology in preventing attacks.

Conclusion

The confluence of data-driven technologies and devices will continue to improve manufacturing. The Internet of Things will open up new frontiers for efficiency and quality in manufacturing production. Security can help foster this innovation and ensure that having more interconnected devices doesn't have to mean more risk.

Many best practices still apply to modern manufacturing networks, as varied as they may be. Risk assessment and identifying your most valuable assets remains paramount to security. So does regular penetration testing and more advanced testing methods like targeted threat hunting. Finding an experienced targeted threat hunting provider with expertise across multiple environments and industries can make a difference when it comes to identifying the weak spots in your complex network.

As you grow and innovate with technology and IoT, take the opportunity to improve your security posture. It's never too late to assess what data is at risk and how cyber criminals might access it. What you can't prevent, you can detect with the help of unified security visibility and expert global security intelligence. This intelligence can also be used to predict the next attack target, creating a cycle of continuous prevention.

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com

[1] Price Waterhouse Coopers LLC, The Global State of Information Security® Survey 2016, PwC, http://www.pwc.com, (2016)
[2] Ponemon Institute, Ponemon 2015 Global Study on IT Security Spending & Investments, http://www.ponemon.org, (June 9, 2015)