Automation.com

Advancing Automation

Cybersecurity in Industrial Environments

Volume VII

CISCO™

INTRODUCTION

In the increasingly connected environments of today's industrial facilities and factories, the threat of cyber-attack looms as a growing threat amidst all the technological advancement. All the advancements in productivity, data-driven efficiency, and remote monitoring can be the undoing of any facility that leaves their virtual back door unlocked.

To help arm companies against the threats, Automation.com has worked with the IoT experts at Cisco to provide you the latest edition of our Cybersecurity eBook, filled with detailed reads on the latest strategies and technologies to keep your industrial networks secured, and your company one step ahead of the hackers. Whether you specialize in IT, OT or executive management, you don't want to miss this incredible resource designed to help your company safely navigate this technological wave.

This ebook includes:

Cisco's in-depth guide to establishing and maintaining effective security in today's connected factories

In a factory with thousands of moving parts and floods of data and information, it's justifiable if you're not sure where to begin securing your facility. This detailed article explains several areas where organizations should focus, both in virtual and physical security, in order to ensure effective and redundant safeguards for their key processes and equipment.

A detailed run-down of Cisco's IoT Threat Defense services and experience

A major key for overwhelmed organizations to remember is that companies such as Cisco have been specializing in helping enhance virtual security for companies for many years and continue to be on the front lines of information and technology to keep the hackers out and the productivity up. This read will go further into detail about what Cisco can do to help you get your security up and running.

An inside look at Cisco's view of the secured, connected factory of the future

While IT and OT continue to converge, the need for reorganization and departmental control can hinder the cybersecurity effort. This article discusses the dangers that can present for any manufacturer, and details Cisco's effort to give these companies a blueprint to a secure, connected future for their factories.

Cisco's list of Top 10 with high-level questions to ask of any prospective vendor looking to secure industrial control systems (IACS).

The key for any organization looking to secure their systems is knowing who to trust. In this article, Cisco details 10 questions that organizations need to ask in order to make informed decisions about the services and features they need to adequately secure their IACS. From manufacturing location, to solution interoperability, this Cisco guide will help you ensure that you leave no stone unturned in finding the best security provider for your systems.

CONTENTS

The Cisco Connected Factory: Holistic Security for the Factory of Tomorrow

Global manufacturers protect mission-critical industrial operations with Cisco Connected Factory security solutions

By Cisco

The Rising Threat to Manufacturers

Cybersecurity has never been more important to the world's leading manufacturers—and for good reason. Despite impressive advances in cybersecurity in recent years, manufacturing and industrial operations still remain "islands of vulnerability" waiting to be exploited by bad actors. Legacy industrial control systems—many of which were never built with security in mind—remain especially prone to cyber threats. And as these systems are converged and integrated with enterprise IT technologies, new vectors of attack open up. A recent cybersecurity report from MAPI/Deloitte explains why security is becoming such a big concern for manufacturers:

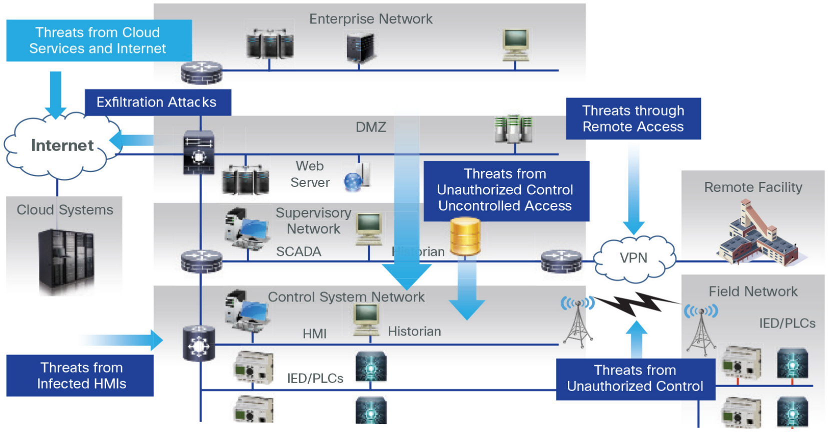
- 39% of respondents experienced a breach within the past year
- 36% cited IP protection as a top concern
- 35-45% use sensors, smart products, and mobile apps; 55% encrypt the data used by those systems
- 50% perform ICS vulnerability testing less than once per month
- 77% have performed end-to-end product assessments
- 27% do not include ICS in incident response plans
- 37% do not include connected products in incident response plans[1]

Manufacturers face two major obstacles when implementing effective security in industrial environments:

- Traditional security platforms lack visibility to identity industrial assets like controllers, IO, drives etc. which makes it challenging to define security policy for these devices based on just network attributes like IP and MAC.
- Fear of impacting production due OT personnel having to depend on a centralized IT team to modify security policies to accommodate control system adds, moves, and changes needed for day to day operations

No single product, technology or methodology can fully secure industrial operations. Protecting critical manufacturing assets requires a holistic defense-in-depth security approach that uses multiple layers of defense (physical, procedural and electronic) to address different types of threats.

Figure 1. The Evolving Threat Landscape for Manufacturers



To overcome these challenges, Cisco has developed integration between OT tools used for process network monitoring and IT security platforms. This integration not only provides security systems with visibility to industrial assets, but also puts control back in the hands of OT personnel by giving them the ability to express operational intent and automatically have the system select the appropriate IT defined security policies without requiring network or security skills.

[1] "Cyber Risk in Advanced Manufacturing", MAPI, November 2016.

Today, manufacturers need even more sophisticated technologies to police the new Industrial IoT landscape, which connects millions of machines across global networks. But many plant and operations managers are wary of implementing measures that could impact production schedules, and are thus reluctant to make changes to existing segregated networks. In addition, managers have their hands full overseeing plant-floor access for partners and vendors—often across multiple sites—increasing the likelihood that a malicious actor could slip through. In fact, human error is one of the biggest causes of security breaches. Some important cybersecurity findings for the manufacturing industry:

- 28% of manufacturing organizations reported a loss of revenue due to attack(s) in the past year—the average lost revenue was 14%.
- 46% of manufacturing organizations use six or more vendors, with 20% using more than ten. 63% use six or more products, with 30% using more than ten products.
- Nearly 60% of manufacturing orgs report having fewer than 30 employees dedicated to security, while 25% consider a lack of trained personnel as a major obstacle in adopting advanced security processes and technology.[2]

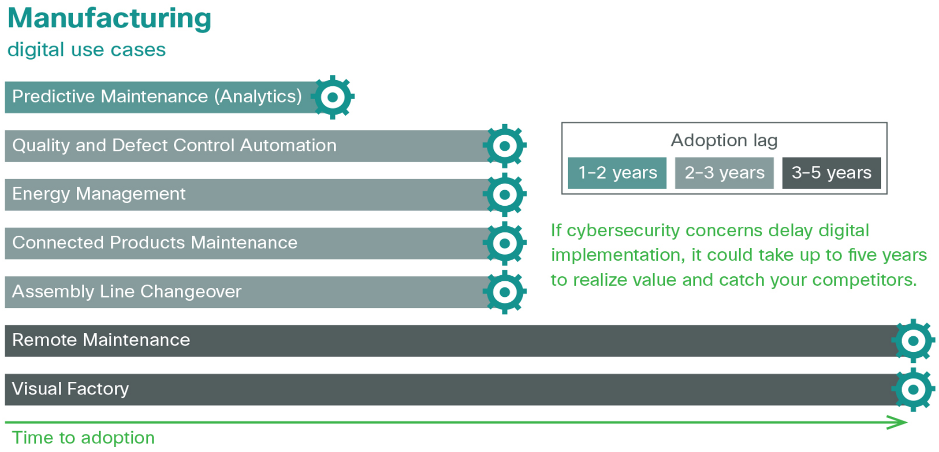
For example, a global pharmaceutical manufacturing company lost half a billion dollars in 2017 due to an accidental infection and there were at least $1B in losses due to 2017 infections at industrials according to SEC 10Q statements and european financial releases. In the worst case, the health and/or safety of workers may be at risk.

Manufacturers that fail to address security threats face another, perhaps costlier risk: missing out on revenue and market-share growth. Figure 1 shows the potential impact of cybersecurity risks and adoption lags related to seven use cases that will drive most of this industry's "digital value at stake" over the next decade. All of these use cases require manufacturers to instrument their operating environments with new digital capabilities. But manufacturers must first have confidence in their integrated IT and Operations cybersecurity strategy. If not, they will miss out on this value and the enhanced profitability it promises. Given the escalating cyber threats facing manufacturers today, and the real competitive disadvantage faced by companies that are late in deploying security solutions, it's no surprise that Cisco's latest survey of more than 350 companies showed that 89% reported they have an executive with direct responsibility and accountability for security.[3]

Costly Breaches

The damages inflicted by security breaches are well known to businesses and industrial operators. Harm can range from physical and environment damage to intangible impacts like brand reputation and customer trust. Economic losses can be particularly severe in industrial settings, where an attack can cause millions of dollars in downtime, disrupt production schedules and damage expensive machines.

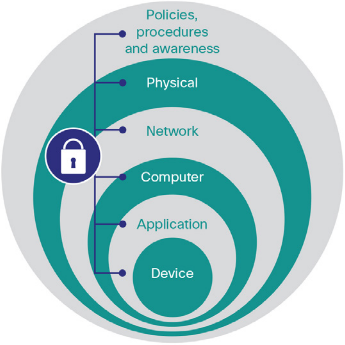
Figure 2. When Cybersecurity Concerns Delay Digital Initiatives, Growth Potential and Market Position Suffer



[2] Cisco 2017 Midyear Cybersecurity Report, 2017
[3] [2017], Manufacturers, Here's What You Need to Know from the 2017 Midyear Cybersecurity Report, [Blog post]

A Holistic Strategy

Figure 3. Defense in Depth



To thrive in the new threatscape, manufacturers need to implement new strategies and architectures. “Defending the edge” with firewalls and access management is as necessary as a strong network segmentation strategy, both of which are generally lacking in IACS networks today. But this is only part of the solution in today’s vulnerable industrial environments, where threats can originate both outside and inside the factory, and may be unintentionally caused by human error. Today manufacturers need “defense-indepth” strategies that incorporate layers of independent security controls (physical, procedural, and electronic).

In an era of converged IT and Operations networks, cloud computing, mobility and IoT platforms, a holistic approach to data security is required. Manufacturers must now deploy next-generation security technologies to protect against threats unheard of just a few years ago, as mobile devices and Wi-Fi networks proliferate, and Operations networks become more reachable and exploitable.

In doing so, manufacturing security leaders can maintain their competitive advantage and safeguard their brands and reputations. Enabling secure connectivity within Operations networks and between IT and Operations networks is imperative. A secure network fabric can broaden data accessibility while also ensuring that companies can safely gain efficiencies by improving collaboration, overall equipment effectiveness (OEE), and product quality. What’s more, a secure and integrated IT and Operations network helps manufacturers systematically address environment, health, and safety concerns on the factory floor, further reducing risk.

Cisco Connected Factory Security

For years, Cisco has been helping manufacturers secure some of their most critical operations. Thousands of industrial operators—among them premiere manufacturing brands like GM, Daimler Trucks North America, Stanley Black & Decker, Air Liquide, and many more—have implemented Cisco security solutions in their manufacturing operations to guard against security threats and ensure operational continuity, system integrity, and safety.

Security for the Modern Manufacturer

Threats

The threat landscape has evolved in today’s world of connected factories and machines, and robust security is more important than ever for manufacturers. As the factory floor and business processes align more closely, security issues are extending beyond the enterprise and can impact machines and operations.

Next Gen Security

To thrive in this world of ever-more sophisticated threats and multiplying attack vectors, modern manufacturers must embrace a holistic security paradigm built around multiple layers of defense and linking infrastructure, machine processes, and people.

The Secure Factory Cloud

The use of cloud in the manufacturing sector will grow as it becomes a common tool for companies to collect and analyze data at lower costs. Cisco factory cloud technologies give factory managers and remote experts secure access to production data from anywhere and protect data traffic between IoT-connected machines.

The Secure Factory Data Center

Breaches of factory data centers can be devastating, leading to data loss and downtime. Cisco IPS solutions provide actionable security for data centers and block threats before they can disrupt data center services. Deploying secure, resilient services is fast, and Cisco firewalls lead the market in performance and manageability.

The Secure Factory Floor

Connections are deepening not only between the plant floor and the business, but also with the broader ecosystem surrounding the manufacturer. The new factory floor demands a more flexible and sophisticated level of security and threat protection. Cisco's portfolio of secure routers, firewalls, intrusion prevention systems, wireless IPS, and Cisco TrustSec provides multi-layered protections for your factory floor and everything it's connected to.

Secure Factory Machines

Today companies are connecting thousands of factory machines across clouds and IoT networks, enabling a new level of production efficiency and business innovation, but also presenting complex security challenges for Operations and IT managers. Cisco and its partners offer next generation technologies that defend against attackers inside and outside the factory floor.

Cisco security solutions transform diverse manufacturing processes, allowing companies to safely secure integrate infrastructure, machine processes, and people. Designed to deliver maximum ROI and measurable business outcomes, these solutions and services include:

- **Asset Discovery and Monitoring.** Cisco enables manufacturers to identify and monitor assets and users in their networks and create a solid foundation for secure remote access.

- **Identity and Access Management.** These solutions facilitate vendor and contractor access, streamline device onboarding, and dynamic policy enforcement.

- **Industrial DMZs.** Cisco's Industrial Demilitarized Zones provide advanced perimeter network buffers that enforce data security policies between trusted and untrusted networks. The industrial DMZ is sub-network placed between the Industrial and Enterprise IT zones to protect the industrial zone from external attacks. It contains business facing assets that act as brokers between the on-premise data stores and the outside world.

- **Industrial Cybersecurity Services.** Cisco helps manufacturers protect industrial assets and prevent disruptions by analyzing cyber risks, assessing security gaps, and designing and implementing cyber and physical security controls that mitigate these risks.

- **OT Insights Managed Services.** This modular cybersecurity and compliance solution for the operational environment scales as a company's needs evolve and offers affordable as-a-service delivery options.

- **IACS Network Architecture and Design Services.** Cisco works with manufacturers to provide solutions that not only deliver next-gen security, but ensure improved operational performance and ROI.

Let's look how manufacturers are deploying Cisco solutions to create holistic security platforms to compete better.

Comprehensive Access Control

Netflow technology found in Cisco network platforms provides a trace of every conversation in the network. It enables the collection of records everywhere in the network, including north-south as well as east-west communication, to allow for network usage measurements and anomaly detection. Netflow technology when combined with an industry-leading machine learning and behavioral modeling platform like Cisco Stealthwatch helps manufacturers monitor, detect, analyze, and respond to advanced threats. Data exfiltration or other anomalous traffic behavior may be caused by a variety of reasons; sometimes it may be from internal users who have succumb to phishing attacks, but many times they are linked to attacks and threats trying to subtly maneuver around the industrial network. Cisco Stealthwatch not only detects these anomalies, but also helps analyze them to identify the root cause of an incident – quickly. And with its historic network audit trails, you have days, months and years of data at your fingertips, enabling you to conduct thorough forensic investigations to determine how and where the threat entered your network.

As the number and types of devices connecting to an IACS network continues to increase, existing techniques for managing security and reducing risk are challenged to keep pace. The Cisco Identity Services Engine (ISE) empowers manufacturers with a new generation of technologies to ensure highly secure wired and wireless access within the plant, while providing centralized policy management, streamlined device onboarding, and dynamic enforcement.

Cisco's Identity Services Engine supports multiple external identity repositories and simplifies administration by providing a single integrated management interface for both IT and Operations networks.

Manufacturers now have a centralized context-aware system to efficiently control access within an industrial zone. The ISE solution automatically sets the right level of access privileges and policies based on the user's role and group, and constantly monitors the network to ensure that users are only accessing the network on authorized, policy-compliant devices. Users gain access only to those segments of the industrial network that policy allows—and are barred from others—and the process is completely transparent to users.

Diebold Secures Global Machine Network with Cisco Identity Services Engine

As the world's leading manufacturer of ATMs, Diebold Inc. knows something about security. "Security is a very integral part of our organization," says David Kennedy, Diebold's Chief Security Officer. "Our number one security priority is to ensure our business generates revenue." Diebold currently deploys a range of security solutions from Cisco—including Cisco Identity Services Engine (ISE)—to help protect its network of 87,000 devices in 77 countries.

As new technologies and devices enter the Diebold workplace, Kennedy says it's ever more challenging to achieve complete network visibility and control. "Today there are more exposures and insider threats," he notes, a situation that is complicated by the influx of tablets, smartphones and other mobile devices into the industrial workplace. In these settings it's hard to get "granular control" over identities operating in the network, he says.

Diebold looked at competitors, but "nothing did what Cisco ISE could do," Kennedy recalls. "Cisco ISE's comprehensiveness was a big win for us." The solution, which is integrated with Cisco AnyConnect Secure Mobility Client, allowed Diebold to profile all devices in the network and streamline guest and contractor access. "It's made our whole process significantly easier," the CSO says—and safer too. "[Contractors] are only assigned the information, ports, and protocols that they need," he says, adding that the process is fully automated and transparent to the user.

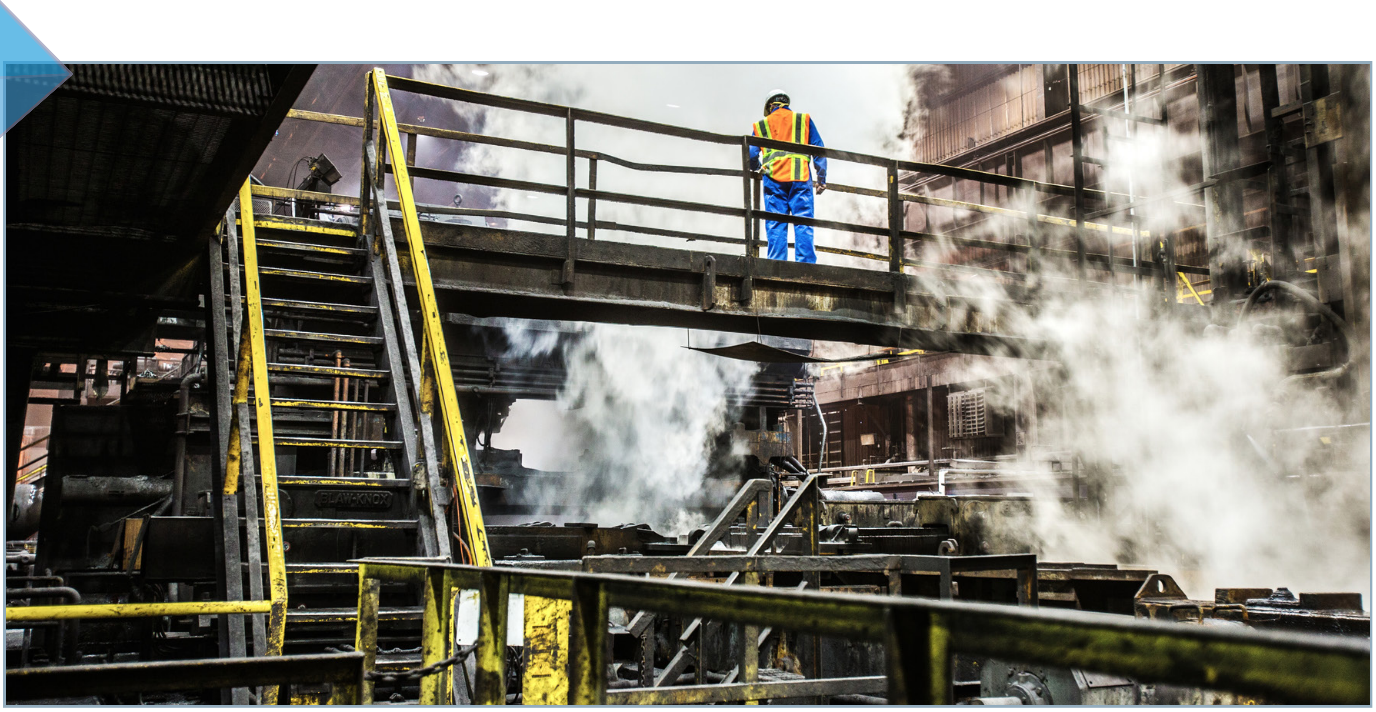
Best of all, Diebold is now effectively addressing the risk of mobile devices in industrial settings. "Mobile is a huge concern for us, but we have less of it because of Cisco ISE," Kennedy says. "Cisco ISE is completely revolutionizing our network."

Deep Protection with Industrial DMZs

More manufacturers are combining comprehensive identity services with advanced perimeter network buffers known as Industrial DMZs that enforce data security policies between a trusted network (Industrial Zone) and an untrusted network (Enterprise Zone). These IDMZs form a separate network situated between the two zones.

IDMZs typically consist of numerous infrastructure devices, including firewalls, VPN servers, IACS application hosts and reverse proxy servers, in addition to network infrastructure devices such as switches, routers and virtualized services.

If you are serious about security in your IACS network, consider the range of IDMZ solutions for Converged Plantwide Ethernet (CPwE) environments offered through a strategic alliance between Cisco and Rockwell Automation.



Global Aluminum Company Leverages DMZs to Optimize and Protect Industrial Network

Industrial DMZs play a major role in securing and optimizing one of the world's largest aluminum production facilities. Built by the Emirates Aluminium Company Ltd. (EMAL, part of Emirates Global Aluminium) at a cost of $US6 billion, the massive smelter located in Abu Dhabi produces 1.4 million tons of aluminum annually. The plant is organized into several independent industrial zones—and IT networks—corresponding to different stages in the aluminum production process.

The challenge: how to converge these disparate networks and share valuable information to optimize production without compromising security and resilience.

EMAL deployed a Cisco-based IDMZ to link information from each zone with enterprise IT without compromising security. Each area has a DMZ, with twin firewalls, providing a "neutral zone" where suspicious traffic can be identified and isolated before it can penetrate networks, servers, and systems.

The company has effectively merged its enterprise and manufacturing networks using a DMZ as a bridge, enabling data sharing between both networks and overcoming proprietary interfaces. "DMZs are normally used to protect corporate networks from internet threats," says Sylvain Boily, Automation Manager with BBA, a project consultant.

The aluminum manufacturer is looking at other solutions, including an IP-based surveillance system that could integrate video monitoring with other techniques, such as analytics and access control, to provide a future-proof plant-wide security solution.

"We have created a network for now and the future," says Boily. "It has everything we need to move information to where we want it. Redundancy, security, traffic control; everything is there."

Cisco OT Insights: Comprehensive Security at a Manageable Cost

As threats escalate and the Internet of Things is making factories more efficient, the increased connectivity is making their Industrial Control Systems (IACS) more vulnerable to cyber threats. Manufacturers need a more robust secure solution to protect their networks against cyber-attacks. They are looking at alternatives to conventional solutions that require large upfront investments in capital equipment and staff. They want solutions that are natively flexible and able to change quickly to keep pace with new business demands.

For those reasons, more manufacturers are adopting Cisco OT Insights, a managed security service to defend IACS and supervisory control and data acquisition (SCADA) networks, improve efficiency, and reduce site downtime. It is a comprehensive end-to-end system that gives manufacturers a centralized view of what's happening at multiple far-flung sites.

It can detect anomalies and alert human personnel, trigger the incident management process, and protect the most critical factory systems.

It utilizes a modular, building-block approach to security controls, providing the flexibility to address new attack vectors as the business grows and security demands evolve. In addition, manufacturers have the flexibility to implement OT Insights on-premise.

The solution interfaces with every major automation company for asset discovery and inventory, secure access and more. Some of the automation vendors are joint delivery partners. Using this robust partner ecosystem, OT Insights uniquely provides the richness of Cisco security, networking expertise with industrial control system security and operational intelligence.

OT Insights provides a single, optimized approach for remote vendors to securely access systems on the plant floor. The approach includes a powerful audit with compliance capabilities, auditing who accesses the system, and delivers operational efficiencies.

Energy Leader Protects Critical Infrastructure, Cuts Costs with OT Insights

Cyber attacks, operational risks, and compliance are top concerns for this global energy leader, which produces more than 3 billion barrels of oil and natural gas a day across 70 countries. The growth and complexity of the company's industrial automation and control system (IACS) dictated an innovative security solution that could protect critical infrastructure—both legacy and greenfield—and help ensure compliance while also controlling costs.

"Whether [it's] refineries, or wells or lubricant plants, we need to protect our critical infrastructure," says the company's CIO. "So we asked Cisco to join with us in a comprehensive solution." The solution—Cisco OT Insights—uses field-deployed software and networking gear to remotely monitor more than 50 upstream and downstream sites, providing a secure "tunnel" from the field infrastructure to a centralized management console. Engineers and IT experts at a global service desk quickly respond to any security threats.

Working with partners specializing in IACS and industrial health-and-safety, Cisco delivered an end-to-end solution as a comprehensive service, significantly reducing the company's upfront capital expenditures.

An ROI study performed by the company found OT Insights reduced costs by $700,000 per site deployed over five years. By more quickly managing risks and mitigating threats, the company has increased business agility, lowered operations and security costs, and significantly reduced downtime.

With OT Insights, manufacturers can leverage people, process and technology to:

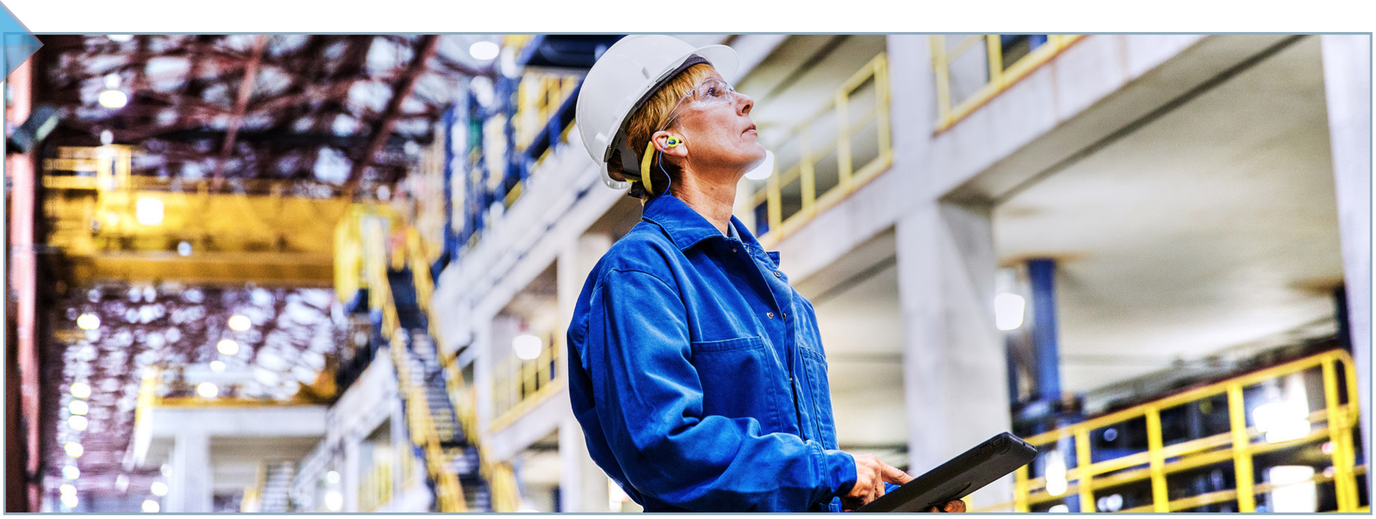
- Automate asset discovery and the inventory process to Level 1 of the Purdue Manufacturing Model
- Tighten security by updating systems, limiting remote access and monitoring compliance
- Automate process of downloading and distributing qualified system patches and antivirus updates
- Gain operational insights using behavioral analytics and machine learning techniques to alert on human and system errors or malicious security incidents
- Increase OEE and productivity through reduced downtime
- Increase visibility and control costs with less complexity, and greater consistency
- More easily manage cybersecurity and compliance on a site-by-site basis
- Resolve the problem of not having skilled resources to manage and control cybersecurity

Physical Security: Your First Line of Defense

Manufacturers face some of their most severe threats from cybercriminals who gain entry into plant floors and do their damage from the inside. Whether it's preventing inventory theft or data loss, companies can benefit from a comprehensive physical security solution integrated with a secure wired and wireless industrial network.

Concerns over physical security prompted Del Papa Distributing, a Texas-based regional beer distributor, to incorporate Cisco IP-based surveillance and security systems into the designs for its 27-acre headquarters near the Gulf Coast. "We wanted the new distribution center to have a single, secure network we could use for physical security, communications, collaboration and even monitoring the temperature of our inventory," says Steve Holtsclaw, manager of Information Systems for Del Papa.

Working with Cisco partner Zones, the distributor built a secure IP network incorporating Cisco solutions for video surveillance, physical access control, digital signs, temperature sensors and more.



IP cameras monitor the property perimeter, a 100,000-square-foot warehouse, office corridors, and all delivery gates. System alerts notify employees when a door to a restricted area is open and provide links to live video. Doors can be opened and closed by pressing a button on an IP phone.

The physical security and surveillance system is just one part of Del Papa's overall converged network architecture, which also features Cisco unified communications and collaboration solutions that have improved safety and business efficiency. "The Internet of Things is here today," says Stephen Lurie, VP, Internet of Things for Zones. "For Del Papa Distributing, 'connecting the unconnected' helped to increase physical security and improve business processes."

Protecting the Edge

A critical segment of a manufacturing network is the Internet edge, where the corporate network reaches the public Internet. The Internet edge acts as the gateway for manufacturers and other businesses to the rest of the cyberspace, and serves other parts of a typical enterprise network. As network users reach out to websites and use email for business-to-business communication, the resources of the corporate network must remain both accessible and secure.

Cisco provides a modular building-block approach to the Internet edge, enabling flexibility and customization in network design to meet the needs of customers and business models of differing sizes and requirements. Manufacturers are turning to Cisco to provide "security at the edge" and mitigate the many threats that present themselves in this critical area of the network. This includes solutions and validated designs for:

- **Firewall and intrusion prevention.** Protects the network infrastructure and data from Internet based threats such as worms, viruses, and targeted attacks.
- **Remote access (RA) VPN.** Provides secure, consistent access to network resources from remote locations.
- **Web security.** Provides acceptable-use control and monitoring while managing the increasing risk associated with clients browsing the Internet.

Securely Connecting Machines

When plant managers and business executives were asked in a survey what "things" they were connecting now and in the years ahead, 62 percent put production equipment at the top of their list. And there are a lot of connections to be made: By some estimates there are 60 million machines in factories throughout the world and 90 percent are not connected.[4]

That number of connections is expected to grow rapidly as more manufacturers leverage IoT technologies to connect machines and factory robots beyond the plant floor, all the way to the machine builders that created them.

Cisco is leading the move to securely connect machines in factories worldwide. The Cisco Connected Machine Solution is a digital solution portfolio that enables rapid and repeatable machine connectivity, providing business improvements such as better OOE, predictive maintenance, and process optimization. The solution gives machine builders and end-user manufacturers machine-embedded or near-machine switching, security, and computing technologies. The solution enables edge and cloud analytics that support predictive machine monitoring and maintenance.

[4] "Smart manufacturing: when factories go digital", Cisco, 2017

Summary

Manufacturers are entering a brave new world of connected factories. No longer isolated by obscure, stand-alone networks, and walled off from other factories and suppliers—or even headquarters—industrial operators are achieving new levels of productivity, quality, and visibility. But these larger and more complex networks also open up avenues for cybercrime and security breaches that are harder to defend against. And as the IoT continues to grow, a wider ecosystem of connected machines is adding a new dimension to the security challenge.

Manufacturers are rising to the challenge—and gaining a competitive edge in the process—by implementing the next generation of security protections built for the age of the IoT. These solutions marshal multiple layers of defense to protect intellectual property and physical assets from unintentional breaches and cyber theft, while speeding threat resolution, reducing downtime, and driving efficiency gains across facilities. Connected Factory Security solutions from Cisco and its partners are setting the standard in this new landscape, helping manufacturers such as Diebold, GM, Air Liquide and thousands more ensure effective, robust plant-floor security while protecting their brands and paving the way for future growth.

Get Started with an Industrial Cybersecurity Threat Assessment

How vulnerable are your industrial operations to attack? Cisco can help you find out with a comprehensive Industrial Cybersecurity Risk & Vulnerability Assessment. We'll evaluate your IACS infrastructure, networks, and processes to understand your cyber risks and vulnerabilities. Then we'll help justify future cybersecurity investments by quantifying the financial risk to business leaders, and rationalizing specific cybersecurity solutions which mitigate the top cybersecurity risks identified. By developing a business case and action plan, Cisco will help defend your operations against current and evolving threats.

How comfortable are you with your existing IACS security architecture and designs? Cisco can help build a site-specific or company-wide Industrial Cybersecurity Reference Architecture for your Operations networks. We'll evaluate the capabilities of your industrial network infrastructure to protect business critical assets, and provide a comprehensive vendor-agnostic and industry best practices based evaluation of the existing network architecture and design. The outcome and resulting Industrial Cybersecurity Reference Architecture provides a plan for how to tighten the security of the network, including where to implement specific security controls and how to classify systems into specific security zones. It is aligned to the ISA-95 Model and ISA-99/IEC-62443 Security Framework and accounts for all necessary security controls including the products and solutions previously mentioned in this white paper.

To learn more: Go to cisco.com/go/factorysecurity or contact inquire-factorysecurity@cisco.com.

Cisco IoT Threat Defense

By Cisco

Defend your business against IoT threats at scale

We at Cisco believe that the Internet of Things (IoT) will alter society. But for the IoT to truly fulfill its promise, it must be secured. Yet IoT devices are notoriously vulnerable. These vulnerabilities present opportunities for attackers to gain access to your network where they may install malware, steal intellectual property, or worse.

We have been designing, deploying, and securing networks for more than 25 years. We invent the technologies, build the equipment, and develop the standards that have helped make the Internet possible. And we continue to invent.

Cisco® IoT Threat Defense segments IoT devices with exceptional security. It is an adaptable, extensible means of protecting vital services such as oil and gas facilities, electric utilities, manufacturing, and more.

The human factor in securing the IoT is the most important. Our people have decades of experience helping our customers assess and manage risk, develop incident response and readiness strategies, secure their networks, and protect their businesses. Who better to help you?

Benefits

- Extensible, scalable network segmentation protects IoT devices at scale
- Visibility and analysis help you detect anomalies and block threats
- Highly secure remote access protects communications between locations and with third parties
- Security services help you get the most out of your technology investment

Protect your business at IoT scale

IoT devices are vulnerable to cybersecurity threats. They cannot protect themselves. We estimate that there will be 50 billion connected things by 2020. Defending so many vulnerable devices is beyond the capability of legacy techniques such as VLANs and point products.

Cisco IoT Threat Defense:

- Is a cybersecurity architecture based on a suite of integrated technologies and services It is designed to detect and block threats on devices, across your network, and in the cloud.
- Protects IoT devices using extensible, scalable, and automated segmentation aligned to your business. Segmentation is based on policy and enforced across your network.
- Secures communications among your locations, no matter how remote, and puts control of third-party access in your hands.
- Improves your ability to manage cybersecurity risk by helping you assess, design, and implement highly secure IoT solutions with our expert-led professional and technical services.

Point products cannot provide the depth, breadth, or scale of protection you need to defend your organization against IoT threats.

Reduce cybersecurity risk in your IoT environment

Are you taking advantage of the benefits of IoT in a way that aligns to your business requirements and risk tolerance? Get the assurance you need with Cisco IoT Threat Defense. For additional information, visit www.cisco.com/go/iotthreatdefense.

Cisco
Connected Factory — Security

By Cisco

Manufacturing: A target-rich environment

Many manufacturers view data security as a top barrier to realizing the value of IoT. And this threat is increasing as manufacturers adopt new technology standards and converge the traditional boundaries between IT and Operational Technology (OT) systems and organizational silos.

Statistics show manufacturing faces a particularly dangerous security situation:

- Nearly 40% of manufacturing organizations reported targeted attacks and advanced persistent threats as high security risks to their organizations (Cisco 2017 SCBS Study).
- 28% of manufacturing organizations reported a loss of revenue due to one or more attacks in the past year (Cisco 2017 SCBS Study).
- Industrial networks top the list of systems most vulnerable to cybersecurity issues.
- 46% of manufacturing organizations use six or more vendors, with 20% using more than ten. 63% use six or more products, with 30% using more than ten products. (Cisco 2017 SCBS Study).

Automation and control systems in OT networks are inherently vulnerable due to their use of proprietary hardware and software, with little to no security built into aging legacy factory networks. This vulnerability is actually increasing as manufacturers implement IoT capabilities across their factories and connect their plant assets to higher-level applications.

We designed Cisco Connected Factory – Security and IoT Threat Defense to address the specific security risks of IoT deployments from a holistic perspective. Cisco IoT Threat Defense for manufacturing is an architectural approach to security. Protect your Industrial Ethernet infrastructure with a prescribed, regimented approach to security while still adhering to a standard defense-in-depth approach commonly followed in manufacturing facilities.

Benefits

- Safeguard production integrity.
- Gain competitive advantage by protecting sensitive information, intellectual property, and physical assets from attack.
- Speed resolution of security threats and reduce downtime, driving efficiency gains across facilities.
- Improve Overall Equipment Effectiveness (OEE) with secure, and reliable access to plant assets, including secure remote access.
- Help ensure effective, robust plant-floor security with validated designs and proven methodologies from Cisco® Services and industry-leading partners, such as Rockwell Automation.

Employ a suite of integrated, interoperability-tested security products, starting with the Cisco Identity Services Engine (ISE) and Cisco TrustSec®, which facilitate extensible, scalable segmentation using group- and device-based access policy throughout the network. These are layered with Cisco Stealthwatch®, and Next-Generation Firewalls, as well as, Cisco AnyConnect® VPN, and Advanced Malware Protection (AMP).

Cisco Security Services puts real people into the solution to help organizations make decisions about protecting their intellectual property and, just as important, their production integrity.

The result is a solution that transforms diverse manufacturing processes into a unified, tightly integrated, and secure communication system, linking infrastructure, machines, processes, and people. With the solution, you can:

- Securely access machine data on the plant floor, aggregate it, and apply analytics to determine optimal operation and supply chain workflows, improving efficiencies and reducing costs.
- Share intellectual property securely with global employees, partners, and vendor ecosystems, helping scale expert resources.
- Mitigate risk with a posture assessment capability that helps ensure policy compliance, operating system updates, and software patch deployments.
- Securely and remotely troubleshoot machines.

Industrial DMZ

- Connected Factory - Security supports a standard industrial DMZ approach with an architecture that supports security and business needs.
- Provides standard network services for control and information disciplines, devices, and equipment found in modern Industrial Automation and Control System (IACS) applications.
- Includes firewalls, remote-access VPN services, IACS application hosts, and network infrastructure devices, such as switches, routers, and virtualized services in proven, validated architectures.

Security and business agility in the age of IoT

The piecemeal Product or Technology-driven security strategy is no longer effective. A holistic approach to IT and operational-technology data security is required to effectively prevent, detect, and mitigate security threats to company intellectual property, capital assets, reputation, and privacy.

Take the next step

Cisco has the infrastructure expertise, services, and strategic partnerships needed to secure business IT and operations, spur faster decision making and enable new business models without compromising reliability, security, or network response time.

To find out more about Cisco Connected Factory – Security, or to schedule a demo, visit https://www.cisco.com/go/factorysecurity and contact your Cisco representative.

> **"...one of the biggest vulnerabilities of the IoT is a lack of visibility. Defenders are simply not aware of what IoT devices are connected to their network. (Manufacturers) need to move quickly to address this...because threat actors are already exploiting security weaknesses in IoT devices..."**
>
> 2017 Cisco Midyear Cybersecurity Report

Industrial Control System Cybersecurity

Buyer's Top 10 Guide

By Cisco

The purpose of this guide is to provide you with high-level questions to ask of any prospective vendor looking to secure your industrial control systems (IACS). It will provide you a path to determine critical information about the vendor's ability to offer a successful IACS security solution.

By asking the following 10 questions, you will better understand if the vendor offering meets your IACS security requirements.

When looking to secure and maintain your control system it is essential to understand:

Why Answers to these Questions Matter
Make an informed decision around the services and features required to properly secure your IACS

What to Look for in the Answers
Comprehensive responses with details and examples of successful implementations

Potential Pitfalls
Every vendor has strengths and weaknesses and these answers help you pinpoint the potential weaknesses

1. How do you detect and protect against an IACS security threat?

Why it Matters
Monitoring, defending, and remediating against risks and threats throughout your network prevents downtime and loss of control – even against physical anomalies like squirrels, jellyfish, or birds.

What to Look For
A vendor that can baseline your environment by detecting and alerting you to anomalies that can cause system failure such as malicious security threats or human error, provide continuous monitoring for your IACS environment down to the control of physical processes, and offer robust forensic analysis after an attack to drive rapid remediation.

Potential Pitfalls
A vendor offering single, point-in-time security focused on a single type of threat, fragmented one-off security projects that create vulnerabilities in your system, and lacking an Intrusion Prevention System (IPS) for threat detection.

2. How do you participate in IACS standards creation, research and industry training?

Why it Matters
Adhering to IACS standards with up-to-date products, policies, and procedures ensures you won't implement an inefficient security solution that doesn't drive compliance.

What to Look For
A vendor that is involved in the security community and leads the development of new standards, is aware of new policies, procedures, system designs, training and threat reports, and is a member of the International Society for Automation (ISA).

Potential Pitfalls
A vendor that does not participate in the ISA or adhere to most current standards, leaves your team the burden of understanding and implementing standards, and offers a solution that won't drive compliance or adjust to frequently-changing standards.

3. How do you secure each boundary level of an IACS network?

Why it Matters
Applying a strategy to secure every level of your IACS network prevents disjointed solutions and insufficient levels of security.

What to Look For
A vendor with a portfolio of integrated physical security and cybersecurity solutions, the ability to apply passive and active security levels within a single environment, and solutions that address the specific security needs of each boundary level.

Potential Pitfalls
A vendor that provides unnecessary security levels for your system, lacks integration with your current architecture, and offers pointsecurity solutions that can't communicate with other systems.

4. How is your industrial hardware manufactured and supported?

Why it Matters
Employing compatible, supportable, and flexible hardware from a vendor with design and support expertise is vital to avoid unnecessary network traffic and implementation issues from a poorly designed system.

What to Look For
A vendor with industrial design experience, support from design engineers that have extensive knowledge of the software, hardware components, and any impacts they may have on your system, and tested, lasting hardware.

Potential Pitfalls
A vendor with generic, original-device manufacturer (ODM) hardware, unintelligent hardware designs with excessive functions that cause latency, installed hardware with unusable features, and hardware without longevity or support options.

5. How does your security help drive broader business outcomes?

Why it Matters
Maintaining the same standards of availability while securing your IACS is critical to achieve the increased connectivity required for an IoT network and drive the digital transformation of your architecture.

What to Look For
A vendor that offers industry-leading security and knowledge and has a broad services portfolio and partner ecosystem that can: drive compliance, increase business visibility, create innovative business processes and policies, lower costs, reduce risk management on systems and the environment, decrease threat remediation time, and enable consistent management across physical and virtual environments.

Potential Pitfalls
A vendor that lacks the knowledge and tools to effectively manage risk across your environment, provides a superficial, non-holistic view of your security requirements, and increases operating costs and management resources.

6. How does your solution integrate with other IT and Operations products and services you offer?

Why it Matters
Integrating IT and Operations security products and services decreases the likelihood of introducing vulnerabilities and gaps into your system.

What to Look For
A vendor committed to delivering fully-integrated products and services, working closely with an integrated partner ecosystem to offer a robust security portfolio, and providing a single source for management and decision making without introducing risk.

Potential Pitfalls
A vendor with multiple point solutions that create disjointed security policies and management layers, a lack of integration processes that leave you with additional costs, and poor system visibility for decision making related to risk management and compliance.

7. What types of visibility does your solution offer into an IACS?

Why it Matters
Gaining full visibility into every zone and segment of your IACS enables you to defend against risks and threats that go undetected through different layers.

What to Look For
A vendor that provides baseline asset discovery/inventory to determine the machines, network devices, and products that exist in different zones, offers passive discovery and inventory capabilities that quantify risk and residual risk, and who enables remediation against signatureless threats when they hit your system.

Potential Pitfalls
A vendor offering a “flat” network without zones and segments to differentiate your system, no firewalls or protection between different zones and segments, and manual asset discovery limited to the control system and manufacturing operations system layers.

8. Can you describe the full range of security provided by your solutions at the IT and Operations interconnect?

Why it Matters
Establishing network requirements and management processes through IT and Operations convergence preserves
the existing availability standards and improves your security.

What to Look For
A vendor that aligns IT and Operations strategies and processes for visibility, enables secure communication between IT and Operations systems, and helps you implement IEC-62443/ISA99 standards to secure your IACS.

Potential Pitfalls
A vendor unaware of key differences between IT and Operations requirements, who provides limited communication between IT and Operations organizations leading to vulnerabilities in your system, and increases latency from unnecessary features such as spam protection for a system without e-mail.

9. What authentication and authorization protocols do you implement for network access?

Why it Matters
Utilizing a comprehensive set of authorization policies and protocols lowers your risk by keeping out unknown or unwanted entities, without impacting operations.

What to Look For
A vendor that provides context-aware identity management based on identity, location, and access history, allows you to streamline service operations by establishing specific standards throughout the network, and empowers you to make proactive governance decisions by tying identities to network elements.

Potential Pitfalls
A vendor offering limited network connectivity for access control, lack of an identity database and allowed protocols for your IACS, and inflexible rule definitions for granting access to segments of the network, applications, or services simply on authentication results.

10. How do you know that your security solution will successfully integrate with my network architecture?

Why it Matters
Implementing a solution that integrates seamlessly with your existing systems helps you avoid introducing unknowns and unintended consequences, or creating new vulnerabilities.

What to Look For
A vendor offering a tested and validated solution put through rigorous analysis and exposure to threats, comprehensive documentation around the implementation of security measures in your environment, multiple types of support and services for applying the security solution, and deep understanding of the IACS environment and what is required to secure it.

Potential Pitfalls
A vendor that doesn’t know their solution will be successful in your environment before implementation, can’t offer multiple levels of support and services to run the solution, and doesn’t work with a robust partner ecosystem to secure an IACS.