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

Cisco Manufacturing White Paper

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

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. “Aging industrial machinery infrastructure presents huge security challenges that will continue to grow in the coming months and years,” a recent Dell Security Annual Threat Report stated.¹

Today, manufacturers need even more sophisticated technologies to police the new IoT landscape, which connects millions of machines across global networks. But many plant and OT 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. "Attackers tend to go after systems that can be successfully compromised, and Industrial Automation and Control Systems (IACS) networks have shown themselves to be a target-rich environment," according to McAfee.²

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. 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 OT 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

²https://blogs.mcafee.com/mcafee-labs/is-this-scada-hacking-friday/

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

Manufacturing
digital use cases

<table>
<thead>
<tr>
<th>Predictive Maintenance (Analytics)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality and Defect Control Automation</td>
<td></td>
</tr>
<tr>
<td>Energy Management</td>
<td></td>
</tr>
<tr>
<td>Connected Products Maintenance</td>
<td></td>
</tr>
<tr>
<td>Assembly Line Changeover</td>
<td></td>
</tr>
<tr>
<td>Remote Maintenance</td>
<td></td>
</tr>
<tr>
<td>Visual Factory</td>
<td></td>
</tr>
</tbody>
</table>

Adoption lag

1–2 years
2–3 years
3–5 years

If cybersecurity concerns delay digital implementation, it could take up to five years to realize value and catch your competitors.

Source: Cisco, 2015.
A Holistic Strategy

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 OT segmentation strategy, both of which are generally lacking in ICS 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-in-depth” strategies that incorporate layers of independent security controls (physical, procedural, and electronic). In an era of converged IT and OT 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 OT 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 OT networks and between IT and OT 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 OT network helps manufacturers systematically address environment, health, and safety concerns on the factory floor, further reducing risk.

“Gaining visibility into this world of previously undetected cyber threats helped reassure our team that we were doing the right thing by adding intrusion prevention technology across our industrial network.”

Charles Harper, Director, National Supply & Pipeline Operations, Air Liquide
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 OT 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 all the 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, streamlined 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.
- **Network Address Translation (NAT) Technologies.** These IP addressing solutions streamline plant-wide machine networks and provides additional security to guard against internet intrusions.
- **Industrial Cybersecurity Services.** Cisco helps manufacturers protect industrial assets and prevent disruptions by analysing cyber risks, assessing security gaps, and designing and implementing cyber and physical security controls that mitigate these risks.
- **Secure Ops 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.
- **ICS 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.

“Cisco Identity Services Engine is completely revolutionizing our network.”

David Kennedy, VP, Chief Security Officer, Diebold Inc.
Comprehensive Access Control

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 OT 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 easily 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

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.

This is why 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. “This application of DMZs within a manufacturing environment is groundbreaking.”

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 Secure Ops: 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 (ICS) 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 Secure Ops, a managed security service to defend ICS 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 and alert anomalies, 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 Secure Ops 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, Secure Ops uniquely provides the richness of Cisco security, networking expertise with industrial control system security and operational intelligence.

Secure Ops 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 Secure Ops

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 control system (ICS) 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 Secure Ops—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 ICS 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 Secure Ops 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.
“Now we don’t spend anywhere near the amount of time we used to, dealing with security events and malware problems. In fact, since switching to Cisco Cloud Web Security, I cannot recall a client being infected, and we seldom have to go into the admin portal.”

-Peter Kersting, IT Security Manager, Arup

With Secure Ops, 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 new 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.”
Manufacturers face unique challenges in Internet-connected factory environments. One of them is that industrial machines and machine skids often use the same range of IP addresses, which makes it hard to replicate the equipment on the plant floor without introducing duplicate IP address errors into an IACS architecture. Manufacturers can incur significant development and machine commissioning costs to overcome this shortcoming.

Cisco and Rockwell Automation jointly solve this problem—and also provide added security—with a network address translation (NAT) solution specifically designed for converged Ethernet factory environments. Based on industry standards, Cisco and Rockwell’s architecture gives manufacturers the flexibility to reuse their finite supply of IP addresses, offering key advantages for manufacturers. Since identical machines and skids can have the same IP addresses, the solution makes the hardware easier to troubleshoot and maintain. Commissioning time can also be significantly reduced by quickly and easily mapping duplicate IP addresses.

NAT solutions can also enhance security when they are configured to advertise only one address for the entire network to the outside world—thus effectively hiding the manufacturer’s entire internal network behind that address. Sophisticated manufacturers increasingly leverage NAT to provide both address conservation and security, especially in remote-access environments.

Protecting the Edge

A critical segment of a manufacturing network is the Internet edge, where the corporate network meets 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.
- **Email security.** Provides spam and malware filtering services that help protect against lost data and reduced network-user productivity.
- **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 recent 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. 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 overall equipment effectiveness (OEE), 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.

### Summary

Manufacturers are entering a brave new world of connected factories. No longer 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 ICS 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 ICS security architecture and designs? Cisco can help build a site-specific or company-wide Industrial Cybersecurity Reference Architecture for your OT 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.