cisco Meraki

E-BOOK

Manufacturers: Securing Everyone and Everything

Contents

Dramatically increase your team's capacity, capabilities, agility, and experience without overextending your means.

1. SECURITY IS JOB ONE

Weaving a security blanket

Technology's reach throughout manufacturing organizations has never been more apparent, and its holistic role makes security more essential than ever.

Whereas security protocols once primarily targeted data centers and doors, remote workforces, Internet of Things (IoT) devices, automation, cloud, a multitude of diverse endpoints, and aggressive malware mongers mean manufacturers' IT leaders are weaving security solutions and processes throughout their entire organizations.

But more secure does not necessarily mean more complex work.

It's no overstatement to say manufacturing is vital to a nation's success.

As the World Bank Group's International Finance Corporation wrote, "In most countries, manufacturing generates more economic activity per dollar of production than any other business sector. Manufacturers directly create jobs across a range of skill levels, enabling people, especially women, to move from informal work to formal employment with benefits such as more security, better pay, [health] insurance, and access to financial services. Manufacturing creates opportunities across industry value chains by increasing demand for raw materials, energy, construction, technology, and services from a broad array of supplying industries in the economy."[1]

Thus, for the betterment of each manufacturer and its suppliers, partners, employees, and stakeholders, security is paramount.

1 World Bank Group's International Finance Corporation, "IFC's Work in Manufacturing"

Just as protecting employees, partners, data, and suppliers is a constant, so too is change. At no time was this more apparent than during the COVID-19 pandemic, when manufacturers adept at harnessing change protected their workforce and organizations by quickly shifting staff to remote work environments, safeguarding frontline employees on shop floors and adjusting supply lines.

By leveraging cloud-based platforms and automated approaches, manufacturers can manage—and benefit from—disruption. Accomplishing this translates into transparency and simplification of today's often complex environments.

> "Visibility is likely to become the most critical capability for manufacturers in the coming months … digital technologies could be important enablers.[2]
>
> **DELOITTE**

2 Deloitte & Co., "2021 manufacturing industry outlook"

2. THE TREND TOWARD TRANSPARENCY

Eliminating blind spots

Manufacturers want insight into the blind spots that have ratcheted up costs and time to market.

For example,

almost 43%

of inventory shrinkage is due to employee theft at warehouses,[3]

and the inventory overcharges vendor fraud accounted for was

about 4%.[4]

Misplacement of items, whereby supplies are stored incorrectly and must be reordered, creates another unnecessary expense, both monetarily and time-wise.

3 Statistic Brain Research Institute, "Employee Theft Statistics"
4 SheerID, "25 Jaw Dropping Stats about Employee Fraud"

"Our experience … shows that even in well-run companies, anywhere from 20%–30% of inventory is dead or obsolete," wrote Manufacturing.net.[5] "When all additional costs are taken into account, **the total cost of holding inventory can represent a shocking 25%-30% more** than the inventory's unit cost value. Having your cash tied up in inventory-related expenses … **can translate to as much as 15% or more.**"

5 Manufacturing.net, "What is the Real Cost of Dead Inventory?"

Securing all that’s cyber

Protecting virtual assets is fundamentally important, too. Across industries, cybersecurity spending increased 39% in 2020 vs. 2019.[6]

All markets came under attack, but **manufacturing underwent the steepest increase.** In the first quarter of 2020, **attacks surged 156%** compared with the prior quarter.[7]

6 Hiscox, “Hiscox Cyber Readiness Report 2020”
7 Beazley Group, “The enduring threat of ransomware”
8 Cisco Talos, “Quarterly Report: Incident Response trends in Summer 2020”

3. PEOPLE ARE THE POWER

Putting people first

It's **people** who are central to any manufacturing organization.

It's paramount for manufacturers to ensure the safety of employees, visitors, and partners at all times, whether on a factory floor, in a warehouse, or in the office. During the pandemic, manufacturing plants were especially focused on assuring employee health by complying with government regulations related to personal protective equipment (PPE), preventing contagion, contact tracing, and tracking.

Emergency evacuation of facilities or emergency response to workplace injuries are always crucial functions. Manual oversight can mean longer response times and poor visibility into the location of employees, making it difficult to ensure proper evacuation when an injury occurs, or even locate an injured worker within a large facility

Manufacturing has an average turnover rate of 26.7%.[9] It can cost between half to twice an employee's salary to replace that individual, according to estimates.[10]

Workspace safety

Technology can address these concerns.

Manufacturers can equip personnel with Bluetooth®-enabled devices and badges that give management immediate insight into workers' locations for smart mustering and safety. Smart sensors and cameras leverage artificial intelligence, machine learning, and analytics to rapidly identify anyone who is not complying with safety-equipment rules (such as PPE, gloves, or goggles), maintaining safe distances, or otherwise acting in a potentially perilous manner.

This creates securer work environments that meet or exceed safety standards. Automated alarms supplant time-consuming manual processes while smart solutions' ability to learn provides insight into best practices, people who need improved educational resources, and employees who need more coaching. These safer workplaces are more attractive to employees, reducing turnover and accidents and improving morale, profitability, and employee experience.

9 Leftronic, "19+ Employee Turnover Statistics to Be Aware of in 2020"
10 Ibid, "19+ Employee Turnover Statistics to Be Aware of in 2020"

Remote work is here to stay

Having successfully accessed work-from-home strategies, 41.7% of manufacturers plan to redesign work models to support hybrid workflow for at-home and on-site employees.[11]

Indeed, the majority of executives surveyed rated their full-time employees who worked remotely as "effective".[12] About half of finance teams expect to continue working remotely, and more than 35% of sales teams will be fully remote, the Manufacturers Alliance for Productivity and Innovation determined.[13]

11 International Data Corp., "COVID-19 Impact on Manufacturing"
12 Manufacturers Alliance for Productivity and Innovation (MAPI), "Remote Work Practices and Post-Pandemic Outlook"
13 Ibid, "Remote Work Practices and Post-Pandemic Outlook"

4. FROM THE CLOUD TO THE FLOOR

Cloud soars

More and more manufacturers are adopting cloud solutions to support corporate functions. With the growing acceptance of remote teams, it's even more imperative for cloud usage.

This approach empowers authorized users, regardless of location, to access corporate assets such as client lists, sales data, and supplier information from anywhere at any time. In addition, cloud-based infrastructure is well-suited to disaster recovery, remote backup, and automated maintenance, as well as analytics, IoT, artificial intelligence, virtual reality, and other bandwidth-hungry applications that can get hung up on traditional hub-and-spoke networks.

Cloud computing is becoming the de facto standard across industries ranging from financial services to healthcare, and is the foundation for current and next-generation architectures using this approach as a building block.

On the shop floor

With cloud, IT further underscores its role in contributing value and differentiation through its ongoing enablement of digital transformation initiatives, including smart factory technologies like sensors, automation, robotics, and analytics.

As of August 2020, 38% of manufacturers paused smart factory investments so they could assess COVID-19 impact, with most expecting to resume within 12 months. But 62% are "committed to forging ahead," dedicating 36% of factory investments to smart manufacturing, which represents a 20% increase from those surveyed in the 2019 report.[14]

"It is difficult for manufacturers to maintain the pace of rapid digital transformation on their own and for ecosystems to allow for greater capacity and flexibility in adapting to the new world at scale. The win-win is that the success of these many-to-many relationships can be shared by all participants," the Deloitte-MAPI report said.

62%

of manufacturers are committed to forging ahead

20%

year-over-year increase in factory investment in smart manufacturing

14 Ibid, "Accelerating Smart Manufacturing: The Value of an Ecosystem Approach"

Enter the ecosystem

Likewise, technology ecosystems help ensure manufacturers' ongoing health. There's a trend among manufacturing and other industries to reduce vendor partners to curtail costs and complexity, but entering into relationships with vendors that have vibrant ecosystems delivers the benefits of so-called "best of breed" strategies without the drawbacks.

These ecosystems should feature a growing array of manufacturing and horizontal applications, consulting, and integration options that build on open APIs in a cloud-based environment.

Setting the stage for SASE

By adopting cloud and moving away from traditional hub-and-spoke infrastructures, SASE—Secure Access Service Edge—is becoming an increasingly attractive proposition for manufacturers.

Broadly speaking, SASE is an architecture which converges networking and network security functions and shifts them toward an as-a-service (aaS) cloud-edge model that allows consistent security and experience, regardless of where apps or workloads reside. Because this journey taps technologies such as SD-WAN, SD-Access, Firewall-as-a-Service, and more, it's a journey that will build and depend on organizations' existing infrastructure and strategic IT objectives.

The overall goal of SASE is to consolidate architectures to provide effective, homogenous levels of security and experience to users from anywhere—such as the office, factory floor, or home—on any device, including laptops, smartphones, and other hand-held devices.

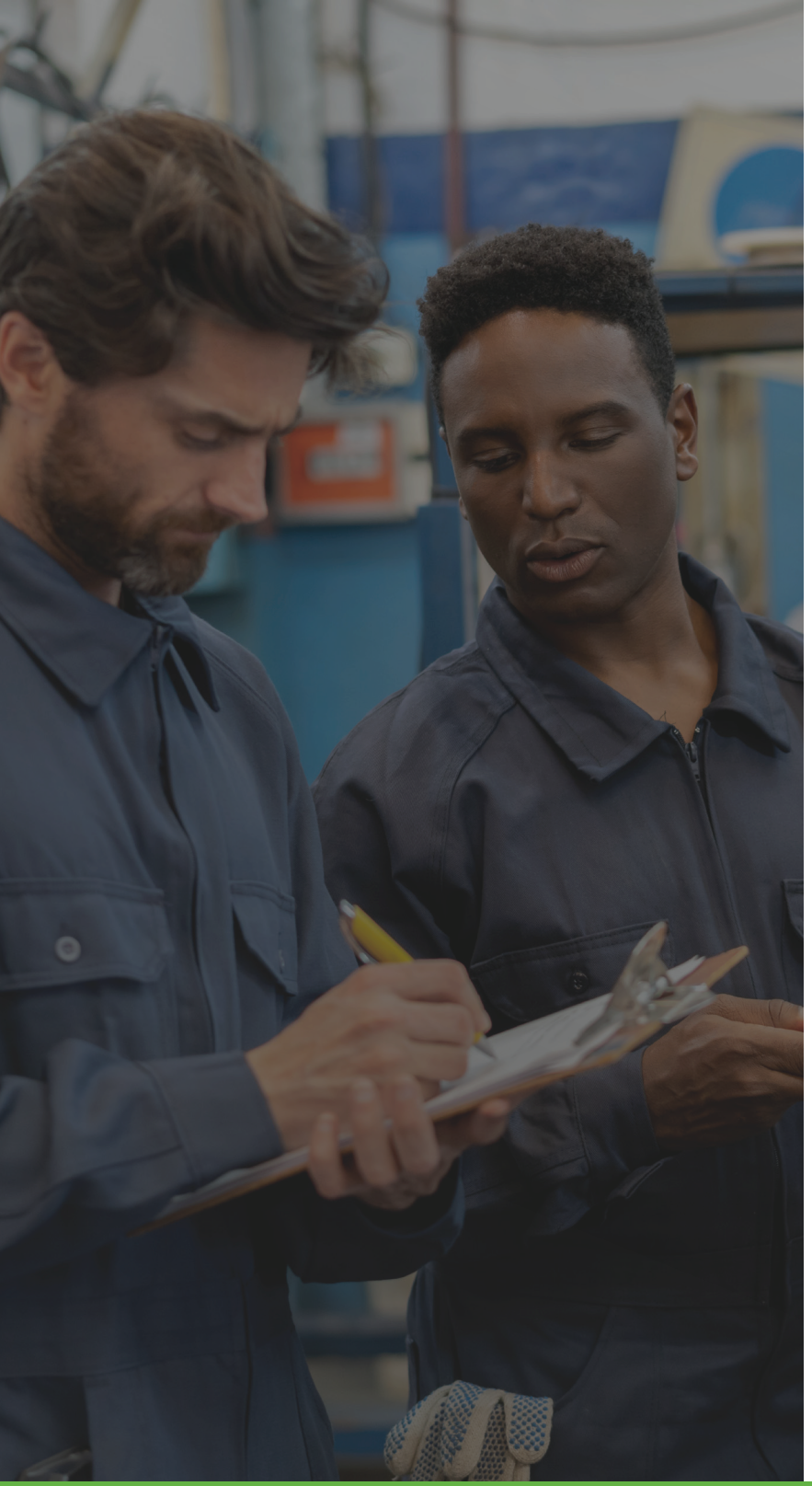
Next-generation architectures

Just as networking and network security, business demands, and ecosystems are colliding to create a perfect environment for IT leaders to deploy deceptively simple and robustly secure solutions, so too are communications architectures like Wi-Fi 6.

Wi-Fi 6 provides tighter security than earlier iterations of Wi-Fi standards, and while most pundits do not expect manufacturers to become predominantly wireless enterprises, the ability to securely use Wi-Fi 6 in some scenarios brings new agility.

Manufacturers that have untethered machines from wired connections could have an easier time rearranging equipment and adapting operations to produce critically needed supplies such as ventilators or medication.[15]

15 Deloitte Insights, "Enterprises building their future with 5G and Wi-Fi 6"



No communications breakdown

"Wi-Fi 6 has inherent capabilities that enable wireless to be more deterministic, which is important for mission-critical IoT assets being used in manufacturing automation," said Matt MacPherson, CTO Wireless at Cisco. "When we look at mission-critical IoT programs and accelerating digitization initiatives, we also need to keep security top-of-mind."[16]

16 Electronic Specifier, "Wi-Fi 6 to demonstrate delivery of transformation for Industry 4.0"

5. A FOUNDATION FOR TODAY AND TOMORROW

Act now, benefit always

By adopting cloud, manufacturers' IT teams can more easily accomplish the goal of keeping security top-of-mind without disrupting employees' ability to do their work.

Solutions that use a single pane of glass for centralized network management can automate updates and patches to ensure consistency and eliminate the need for time-consuming manual patching.

In a recent report from Cisco, only 56% of SMBs patched security vulnerabilities daily or weekly.[17]

17 Cisco, "Cisco Cybersecurity Report Series: Big Security in a Small Business World

Management made easy

The key to IT's increasingly critical role in manufacturing's transformation is in the elimination of the mundane. If technology professionals continue spending upwards of 90% of their time on housekeeping tasks, like maintenance and patching, they cannot feasibly focus on more interesting and business-oriented missions, like data-driven analytics, Industry 4.0, robotics, and customer experience—not unless the team is quadrupled, which is hardly likely.

A cloud-based solution that uses a single pane of glass to deliver network insight into automated tasks—one that allows the rapid deployment of assets across a diverse workforce—allows an IT team to hone in on the tasks that drive revenue and productivity.

Secure everything

Securing today's manufacturing workforce is a challenging endeavor, but it does not need to be.

Just because manufacturing employees, partners, and suppliers are more dispersed and diverse, and are more likely to work from home, coffee shops, and around the world, does not mean your IT team has to double its staff or workload. Rather, by relying on a cloud-based, open API solution that taps into an ecosystem of tested and trusted partners, you dramatically increase your team's capacity, capabilities, agility, and experience without overextending your means.

Discover - Protect - Transform with Cisco Meraki Manufacturing solutions.

Connection
we solve IT

Contact an Account Manager for more information.
1.800.800.0014 ■ www.connection.com/Meraki

C1588260-1221