HYPORI™
VIRTUAL MOBILITY

How Virtual Mobility Can Protect the Manufacturing Industry Against Costly Ransomware Attacks

WHITEPAPER

Summary

While businesses across the US face growing cybersecurity issues, and COVID-19 exacerbates these with increased mobile device use, more remote work, and cloud migrations, the manufacturing sector presents a particularly robust cybercriminal opportunity. Cyberattacks come in many varieties, but today, cybercriminals increasingly deploy ransomware. Ransomware is often the easiest way to make money from compromising an extensive network. Ransomware also gives bad actors access to intellectual property and sensitive enterprise data.

The manufacturing industry is an especially vulnerable ransomware target and has recently seen a significant uptick in such incidents. According to Kivu Consulting, in 2019, despite making up only 18% of all paid ransom cases, the manufacturing industry represented 62% of the total ransom, spending nearly $7 million on ransom payments. In Q4 2020, Tawainese laptop maker Compal, the second-largest original design manufacturer (ODM) of laptops globally, with companies like Apple, HP, and Dell rebranding their devices or designs, suffered a DoppelPaymer ransomware attack demanding $16.7 million ransom.

The Situation

Like other industries, manufacturing is digitizing. According to Statista, in 2023, manufacturers are predicted to spend **$479 billion digitally** transforming their operations, increasing $327 billion from 2017. At the heart of manufacturing's digital revolution are mobile devices delivering real-time data streams and monitoring systems that impact supply chain operations at every level. A recent PwC CEO survey reports that 81% of manufacturing CEOs say mobile technologies are strategically important, and they're prioritizing mobility, cybersecurity, and data mining.

Today, manufacturers seek to improve shop floor productivity while supporting the launch of new digitally-driven businesses. As manufacturing organizations reinvent themselves and empower employees to achieve cost, growth, and profit goals, they look to mobile technology.

As the industry embraces mobility, cybercriminals focus on manufacturing, explicitly perpetrating ransomware attacks. One, manufacturing makes an essential and significant contribution to our economy. A malfunctioning supply chain has disastrous socio-economic consequences, and production line downtime is costly. A McKinsey Global Institute study reports that a halted production line loses an estimated $20,000 per hour, putting significant pressure on businesses to pay exorbitant ransoms. Money isn't the only concern. A recent IBM X-Force report revealed malicious cyber actors targeting the COVID-19 cold chain—an integral part of delivering and storing a vaccine at safe temperatures.

Manufacturing is also a target because it is not known to have robust cybersecurity systems, and it often relies on complex Industrial Control Systems (ICS) to function. Because ICS environments are complex and interconnected, they represent ripe remote access hacking opportunities. Increased mobile device use and a larger remote workforce resulting from COVID-19 expand the manufacturing sector's attack surface and give bad actors even greater access than ever before.

Manufacturing is key to maintaining a functioning economy and securing national security. Cybercrime is a $1.5 trillion economy. Manufacturing needs comprehensive, adaptable, and cost-effective approaches to cybersecurity that protect their complex ICS and secure their organizations' networks.

The Problem

Years ago, manufacturing control systems existed in silos that required manual processes to complete supply chain tasks. Today, thanks to IoT and other advancements, mobile technology allows manufacturing organizations to scale, function, and ensure more consistent quality control and product safety.

As a critical infrastructure ecosystem producing vital materials, finished goods, and medicine, manufacturing organizations are ripe cyber targets. Due to the interconnected nature of facilities and operations, a manufacturing entity attack can impact timely supply chain production, product fulfillment, health and safety, and even national security.

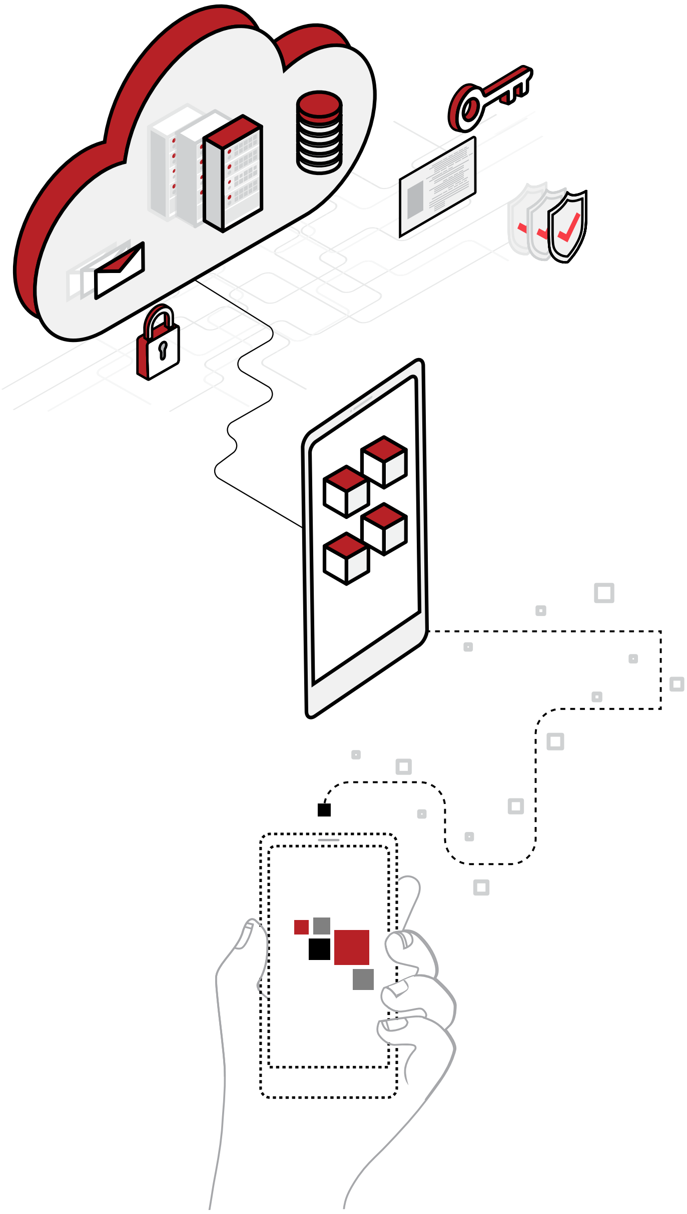
While digitization efforts and increased mobile device use in manufacturing transform businesses, every device's identity becomes the new security perimeter, regardless of its location. Manufacturers must incorporate security into their technology implementation strategies to preserve customer trust and remove roadblocks that might hamper operations. Every sensor, device, employee or company phone, tablet, or laptop becomes a threat surface, and many organizations are taking zero trust models. According to a recent Gartner study, by 2023, the average CIO will be responsible for more than three times the endpoints they managed in 2018.

Industrial control system (ICS) ransomware represents a new and specific industrial operations risk. Dragos reports that manufacturing entities publicly said ransomware attacks have more than tripled in 2020 compared to 2019. While ICS ransomware strains are IT-focused, they can indirectly impact operations and process control networks and resources, including logistics, fleet management, sales operations, and fulfillment.

Most recent manufacturing ransomware attacks are post-intrusion, meaning they come from attackers who have already gained a network foothold via malware. These ransomware incidents are not single incidents but a manifestation of multiple security problems that allow attackers lateral access to the network. A compromised IT network can then lead to a breached OT network (the organization's support infrastructure, lights, heating, etc.). Mitigating individual incidents and resuming production won't solve these problems. The only solution is to address the initial security weaknesses that enabled the attack.

For the manufacturing sector to maintain operations, compete globally, and address cybersecurity risks, it must innovate with next-gen technology that empowers employees and ensures enterprise-wide data and network protection.

The Solution



Hypori Virtual Mobility™ delivers a solution.

Hypori® is military-grade secure, centrally managed enterprise mobility that protects employee mobile devices and secures sensitive enterprise data. Hypori's solution securely contains all organization data on a fully-featured virtual mobile device in the company-owned data center with 100% separation of personal and enterprise data. Manufacturing organizations can empower employees to use mobile devices while protecting proprietary company data and ensuring full supply chain functionality.

A centrally managed hub reduces administrative costs. Organizations don't need to access end-user devices, minimizing IT departments' burdens, protecting employee privacy, and eliminating company exposure should devices be compromised. Cybersecurity management shifts from vulnerable personal devices to a secure data center with no data at rest on mobile devices allowing remote workforce secure enterprise data access in an intuitive, confidential environment.

Hypori Virtual Mobility enables today's manufacturing organizations to improve productivity, innovate with next-gen technology, and gain a competitive advantage.

To learn more about Hypori Virtual Mobility, contact us for a demonstration today.

Contact us

info@hypori.com

*The National Security Agency Commercial Solutions for Classified (CSfC) provides DoD entities the ability to conduct secure classified communications using Commercial-off-the-Shelf (COTS) products. Under this program the Mobile Access Capability Package v2.0 provides a framework for how to secure these communications from mobile end user devices into government enterprise resources. Under the MACP v 2.0, communications must be established using an inner and outer tunnel to provide the secure communications path. Intelligent Waves, LLC's Hypori Client v4.1 for iOS and Android is eligible to be used as a TLS Software Application Product component in a CSfC solution. This means that in combination with a CSfC eligible TLS Protected Server, Hypori is eligible to provide the inner tunnel for secure communications.

11 March 2019

hypori.com