VECTRA®

How manufacturing organizations can reduce business risk from cyberattackers

Manufacturers have long used industrial control systems to increase the speed and efficiency of production. But these production control systems were largely kept separate from the administrative and enterprise systems.

No longer.

In the age of Industry 4.0, manufacturers are racing to get an edge by integrating complex digital systems, industrial internet-of-things (IIoT) devices and cloud computing resources to power analytics, automation and optimization. Consequently, operational technology (OT) networks are converging with information technology (IT) networks.

They are using a broad variety of smart, connected IIoT devices on a vast scale: A single manufacturing plant may have tens of thousands of IIoT devices and sensors – sending a steady stream of data to the edge or cloud.

In addition, manufacturers use many enterprise IoT devices – surveillance cameras, digital signage, building automation and environmental controls, for example. Like IIoT sensors and instruments, many of these smart devices are new and lack a proven history of security.

The inherent cyber-risks

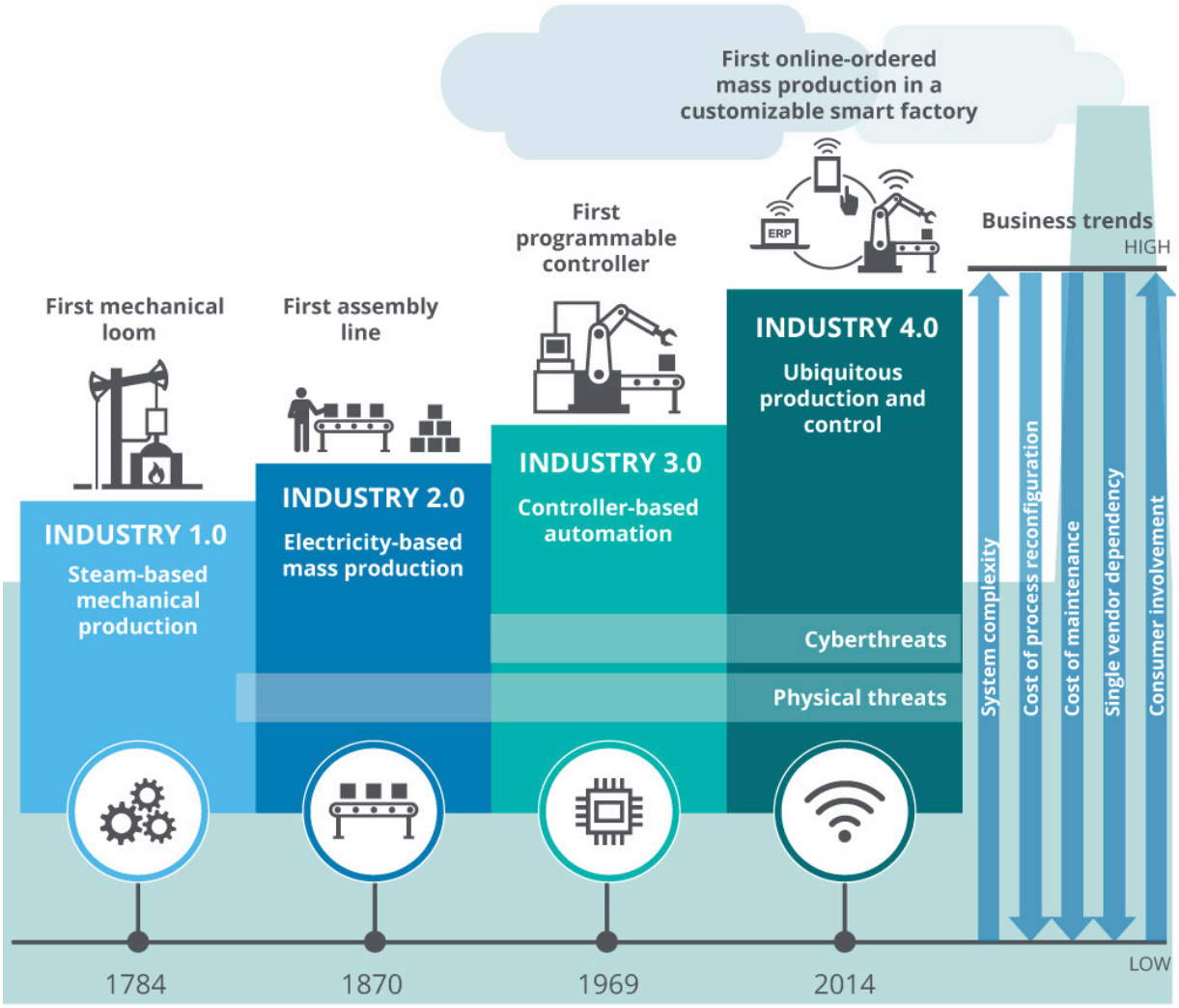
Industry 4.0 brings with it a new operational risk for smart manufacturers and digital supply networks. The interconnected nature of Industry 4.0-driven operations and the pace of digital transformation mean that cyberattacks can have far more damaging effect than ever before.

Manufacturers and their supply networks may not be prepared for the risks. Together, IIoT devices, cloud and increased connectivity create a massive attack surface that manufacturers have never dealt with before. It's far easier now for cybercriminals to infiltrate a manufacturer with the intent to spy, spread and steal.

"Recent reports about nation-state cyberattacks against U.S. utility control systems show that cybercriminals are intent on surreptitiously taking inventory of critical industrial assets and intellectual property to disrupt manufacturing business operations," said Vikrant Gandhi, industry director at the analyst firm Frost and Sullivan.

For cyber-risk to be adequately addressed in the age of Industry 4.0, manufacturers need to ensure that proper visibility and response capabilities are in place to detect and respond to events as they occur.

Manufacturing security operations now require automated, real-time analysis of entire networks to proactively detect and respond to in-progress threats before they do damage.



Source: Deloitte

Cyberattacker behaviors in manufacturing

The manufacturing industry exhibits a much higher volume of malicious internal behaviors. In many instances, there is a 2:1 ratio of malicious behaviors for lateral movement over command-and-control.

These behaviors reflect the ease and speed with which attacks can proliferate inside manufacturing networks due to the large volume of unsecured IIoT devices and insufficient internal access controls.

Some manufacturers have insufficient security access controls on production lines for business reasons. These controls can interrupt and isolate manufacturing systems that are critical for lean production lines and digital supply chain processes.

Many factories connect IIoT devices to flat, unpartitioned networks that rely on communication with general computing devices and enterprise applications. These digital factories have internet-enabled production lines to produce data telemetry and remote management.

In the past, manufacturers relied on more customized, proprietary protocols, which made mounting an attack more difficult for cybercriminals. The conversion from proprietary protocols to standard protocols makes it easier to infiltrate the manufacturing network infrastructure.

"The increase in industrial IoT devices exponentially increases the attack surface for manufacturers," said Jürg Affolter, CIO at Brugg Cables. "Implementing continuous monitoring of the internal network for attacker behaviors as well as additional access controls are important since an agent-based solution isn't possible for industrial IoT devices."

Command-and-control behaviors

The use of external remote access tools by cybercriminals is the most common malicious command-and-control behavior in manufacturing. External remote access occurs when an internal host device connects to an external server.

In this instance, the behavior is inverse from normal outbound client-to-server traffic. The client receives instructions from the external server, and a human on the outside controls the exchange.

While external remote access is common in manufacturing operations, it introduces risk. Cyberattackers also perform the same external remote access, but with the intent to disrupt industrial control systems.

Internal reconnaissance behaviors

IIoT devices can be used as a beachhead to launch an attack. Once an attacker establishes a foothold in IIoT devices, it is difficult for network security systems to identify the backdoor compromise.

Consequently, IIoT devices collectively represent a vast, easy-to-penetrate attack surface that enables cybercriminals to perform internal reconnaissance, with the goal of stealing critical assets and destroying infrastructure.

Internal reconnaissance behaviors that are common in manufacturing include internal darknet scans and SMB account scans. Internal darknet scans occur when internal host devices search for internal IP addresses that do not exist on the network.

> *"IIoT devices can be used as a beachhead to launch an attack."*

SMB account scans occur when a host device quickly makes use of multiple accounts via the SMB protocol, which can be used for file sharing, RPC and other lateral movement.

Manufacturing networks consist of many gateways that communicate with smart devices and machines. These gateways are connected to each other in a mesh topology to simplify peer-to-peer communication. Cyberattackers leverage the same self-discovery used by peer-to-peer devices to map-out a manufacturing network in search of critical assets to steal or damage.

Lateral movement behaviors

Lateral movement occurs when connected systems and devices communicate with each other across the network. In manufacturing, there is often a high level of activity associated with authentication, and SMB brute-force behaviors are common.

SMB brute-force behaviors occur when an internal host utilizes the SMB protocol to make multiple login attempts for the same user account, which most often fail. A high volume of automated replication might occur as a result, which indicates that an internal host device is sending similar payloads to several internal targets.

> *"IIoT systems make it easy for attackers to move laterally across a network."*

IIoT systems make it easy for attackers to move laterally across a manufacturing network, jumping across non-critical and critical subsystems, until they find a way to complete their exploitative missions.

It is critical to maintain visibility into all internal connected systems to understand which are legitimate and which are attackers propagating on the network.

Exfiltration behaviors

Data smuggling is one of the most prevalent exfiltration behaviors in manufacturing. With data smuggling, an internal host device controlled by an outside attacker acquires a large amount of data from one or more internal servers and then sends a large data payload to an external system.

IIoT network architectures also reflect this behavior because multiple sensors aggregate data at an edge gateway that sends the collected data to the cloud for monitoring and analytics. This IIoT architecture is common in manufacturing and does not normally indicate an attack.

> *"Data smuggling is a prevalent exfiltration behavior in manufacturing."*

Exfiltration behaviors are often associated with other threat behaviors in the attack lifecycle that point to an in-progress attack. It is critical to ensure that internal systems are sending data to the intended and approved external systems instead of to attackers who are trying to steal intellectual property, business plans and trade secrets.

AI-driven cyberattack detection and threat hunting

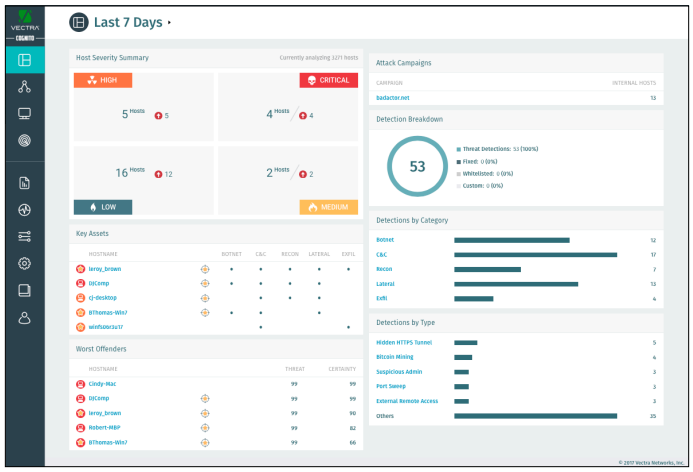
Comprehensive, enterprise-wide threat detection and coverage is mandatory in today's hostile data environments, and as smart manufacturing unleashes the next industrial revolution, the stakes have never been higher.

Vectra® is the world leader in applying artificial intelligence to detect and respond to advanced cyberattacks in real time.

Powered by AI, Vectra and its flagship Cognito™ threat detection and response platform automatically detect hidden cyberattackers and empowers threat hunters to conduct conclusive incident investigations. Cognito Detect™ and its equally powerful AI counterpart, Cognito Recall™, are the cornerstones of the Cognito platform.

The Cognito platform provides continuous, automated threat surveillance to proactively expose hidden and unknown cyberattacks that actively spread inside networks. Cognito continuously monitors and analyzes all network traffic – from cloud and data center workloads to user and IIoT devices.

Cognito automatically correlates threats with host devices under attack, presenting the security operations team with an intuitive view of the highest risk threats – and a trail of forensic evidence to launch conclusive incident investigations.



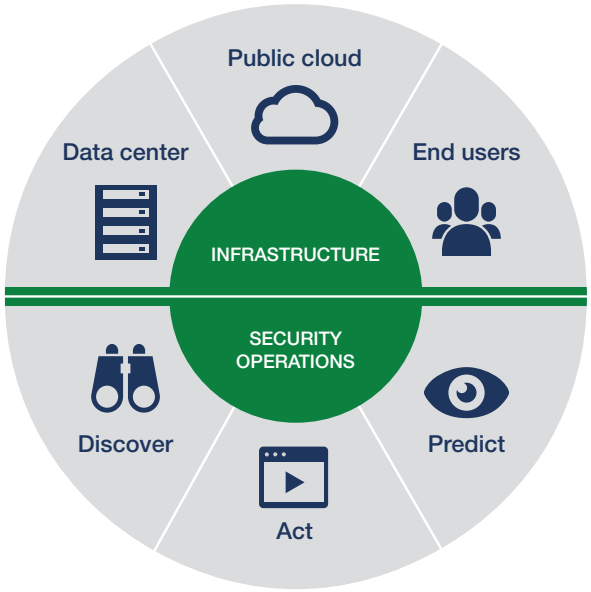
Attacker detections are instantly prioritized, scored and correlated to compromised host devices

Cognito uses the only source of truth during a cyberattack – network traffic. Only traffic on the wire – whether in private data centers, public clouds or converged IT/OT environments – reveals the truth with complete fidelity. Perimeter security only shows you what you've already seen, not the hidden attacks that were missed.

By combining machine learning, data science and behavioral traffic analysis, Cognito exposes command-and-control, internal reconnaissance, lateral movement and exfiltration behaviors. It even detects threats in encrypted traffic – without requiring decryption.

Cognito also identifies when trusted user credentials are compromised by an attacker. By tracking the internal Kerberos infrastructure to understand normal usage behaviors, Cognito detects the misuse of administrative credentials and abuse of administrative protocols like IPMI.

As a critical part of a well-coordinated security ecosystem, Cognito integrates with leading firewalls, endpoint detection and response, SIEMs, virtualization platforms, traffic optimization tools, and orchestration solutions.



Cognito artificial intelligence augments security operations and provides threat visibility into cloud and data center workloads and user and IIoT devices

People + AI = Security that thinks®

Manufacturing organizations will continue to be a top target of cyberattacks. Fortunately, the Cognito platform from Vectra enables security teams at these manufacturers to respond with unprecedented speed, accuracy and efficiency to detect and mitigate threats before they cause damage.

With the Cognito platform providing automated, real-time cyberattack detection and AI-assisted threat hunting, security teams can apply additional context and critical thinking. The combination of people and AI can find and stop threats faster, protecting manufacturers from data theft, espionage, and business disruption.

> *"Vectra automates attacker detections so we can respond faster to the most serious threats."*
>
> *Markus Müller-Fehrenbach*
> *Head of IT Infrastructure and Operations*
> *Vetropack Group*

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai