AGILEBLUE

Automation. Visibility. Confidence.

Manufacturing Organizations

Whitepaper

AgileBlue, 2021

Overview

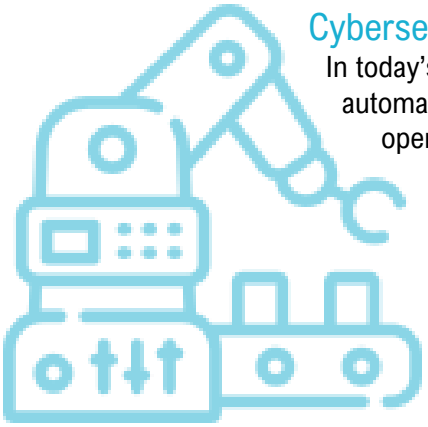
Mid-size manufacturers generally have a modest IT staff tasked with managing a complex IT environment. This means its engineers must assume several roles and have little time for hunting down security alerts generated by numerous security products. Cybersecurity is critically important for manufacturers when you consider their environments are automated with components that can be easily compromised for ransom.

Most IT staff admit their toughest challenge is keeping up with threats to the security of their IT systems and data. Cyberattacks are growing in number, intensity, and sophistication. At the same time, the talent that manufacturers need to defend against such threats is becoming harder to find and retain. Forward-looking companies look to utilize more resilient security programs through effectively monitoring and quickly responding to cyber and digital threats.

An outsourced security solution such as a SOC-as-a-Service provides proactive identification, management, and response to cyber and digital security threats. Cybercriminals are now capable of exploiting weaknesses at previously unseen speed and scale by rapidly acquiring new cyber weapons and continuously modifying their attack techniques. As threat actors continue to adapt and evolve, paying attention to cybersecurity strategy is paramount to manufacturers of all sizes.

Challenges at a Glance

- Cybercriminals target small and mid-size MFG's because Cybersecurity solutions are generally underfunded (E&Y)
- MFG's don't have the resources or talent to effectively monitor, detect, and respond to cyber threats (NAM)
- According to NAM, CEOs stated they are concerned about delays between breach and, incident detection, and response
- Manufacturers are at risk for automation disruption, Robotics interference and IP theft (NAM 2019 survey).
- Limited IT staff, cybersecurity expertise, and budget make manufacturers prime targets for money-driven hackers.



Cybersecurity Challenges for Manufacturers

In today's competitive landscape, manufacturers must protect their proprietary automated processes and intellectual property from theft. Manufacturing and logistics operations are highly dependent on IT systems functioning without errors or disruption and Industrial control systems (ICS) are vulnerable to attacks that require expert monitoring.

Additionally, with growing adoption of smart sensor technology, a continued rise in cyberattacks, and proliferation of connected devices, manufacturers are challenged with securing their assets and operations. SOC-as-a-Service keeps manufacturers critical infrastructure secure by delivering advanced detection, protection, and automated incident response.

Today's cybercriminals hold a strategic advantage, as they can launch attacks at a fraction of the cost–in terms of time, complexity, and resources–that manufacturers must typically spend to defend against them. The growing numbers of automation, mobile devices and ICS applications further exacerbates the problem in addition to:

- Expanded attack surface: Every endpoint, network device, server, ICS control or application expands the attack surface
- Hostile insiders: Weak or non-existent IT security standards for remote workers often lead to hostile rogue insiders jeopardizing your business
- Human error: Lack of appropriate internal security training and poor supply chain risk management lets even well-intentioned employees or third-party vendors create accidental exposure

Dedicated Security and 24/7 Monitoring to Combat Ransomware and Breach

According to the National Association of Manufacturers, small and mid-size manufacturers have done a historically poor job of improving the following which the NIST framework details:

- Cybersecurity governance
- Risk assessment
- Protection of network and data
- Detection of unauthorized activity and response
- User training
- Risks associated with vendors and third parties

Like many industries, Manufacturers have attempted to meet elements of this guidance by deploying traditional endpoint antivirus (AV) solutions or perimeter defenses like firewalls, assuming these approaches will be enough to make their problems "go away." Unfortunately, these solutions have consistently failed to keep them secure.

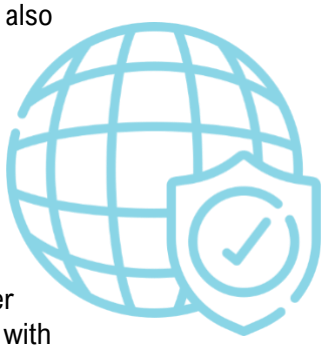
According to a 2021 Survey by Deloitte, Manufacturers should:

- Prioritize security of industrial automation, infrastructure, employee training, identity and access management, Applications, and their Data.
- Begin prioritizing cybersecurity of third parties, cloud security, and updating old industrial automation systems and IT environments.
- Strategize digitalization and adapting to industry 4.0, as well as protecting internet of things (IoT) devices.
- Stay up to date on compliance and changes in laws & regulations.

Here are the top three types of cyberattacks that small and mid-size manufacturers tend to struggle with, and the reasons why traditional approaches have often failed:

Ransomware is a type of malware that either threatens to block access to a victim's data, publish it, or destroy it unless a ransom in cryptocurrencies is paid. Manufacturers may install AV or endpoint protection platform (EPP) solutions on employee endpoints, but without having an expert team to carefully analyze their alerts and event log data, an attack can go unnoticed. These attacks have become particularly notorious for their ability to evade traditional endpoint controls, leaving most companies vulnerable as they operate without continuous network monitoring capabilities, real-time threat intelligence, or custom threat detection logic.

Attacks on unpatched servers and infrastructure are specifically designed to exploit weaknesses and vulnerabilities in servers and other Internet-facing systems. In a vast majority of such attacks, patches are publicly announced and made available. For appropriate defense, Manufacturers need access to advanced vulnerability scanning tools for system hardening and alerting. Ideally, they should also deploy continuous network monitoring tools with customized rules to detect anomalous scanning requests coming into Internet-facing entities, indicators of attackers probing the system.



Phishing attacks seek to obtain sensitive information such as usernames, passwords, social security numbers or credit card numbers. Attackers typically operate under the guise of a trustworthy entity, such as a reputable third party, or the login page for an email or messaging service. Email security solutions that offer real-time analysis of URLs in emails, email attachments, and web objects can help with detection. But email security solutions are often unable to flag an embedded malicious URL or attachment before the victim interacts with it. In such cases, companies without continuous network monitoring, Active Directory (AD) monitoring, or advanced monitoring for any deployed ICS and SaaS applications are left vulnerable.

A new approach for a secure future: adopting SOC-as-a-service

IT teams at Manufacturers only have a few hours to detect an intrusion, investigate the incident, estimate the severity and scope, determine what response actions are necessary, initiate the response, eject the attacker, and contain any damage. Given enough time, attackers can bury themselves deeper, start adapting their moves, and behave like an insider to make it look like whatever they're doing is just regular business activity. This makes detection at a later stage much harder and significantly impacts a company's ability to trace their path during an investigation. This is exactly why Manufacturers of all sizes need advanced threat detection and response capabilities with 24x7 security monitoring.

In the aftermath of most data breaches, IT teams find that attacks usually don't look like attacks at all, except in hindsight. Effective detection strategies depend on aggregating and correlating logs from critical components in an organization's network. Detecting patterns of anomalous activity and potential compromise requires the deep analysis of several critical log sources, including:

- Firewalls
- IDS/IPS
- Endpoint security (EPP, antivirus)
- Active Directory

- Email security gateways
- SaaS applications
- Cloud workloads

SOCs are staffed with trained security analysts who continuously monitor data centers and servers, user login activity, SaaS applications, cloud workloads, endpoints, and email systems. A SOC enables IT staff to correlate events across multiple, disparate systems, and extract actionable intelligence to aid effective threat detection and response. Unfortunately, its cost is well beyond the budget of most manufacturers. AgileBlue's SOC-as-a-service, CyberSOC, delivers the following capabilities at a simple and predictable monthly pricing model–essentially enabling smaller Manufacturers to take advantage of security operations. Included are:

- Fully managed, cloud based SIEM
- Machine Learning Engine
- External threat intelligence
- 24x7 monitoring and alerting
- Compliance reporting
- Cloud monitoring–AWS, Azure, Google Cloud
- Periodic external vulnerability scans

SOC-as-a-Service protects the following from threats so that you can focus on your manufacturing business:

- IT systems
- Robotics Automation
- ICS controls
- Confidential data

A SOC-as-a-service enables manufactures to address the listed security gaps that result in the cyberattacks covered in the prior section going undetected. Using a managed SOC service gives manufactures complete centralized visibility into their networks' security and the ability to leverage existing point products and security investments. It also creates access to regular vulnerability assessments and enables manufacturers to establish a detailed and customized incident response plan.

What's more, it helps manufactures provide strong evidence of security processes during control audits, avoid compliance penalties, insurance reviews and establish a new competitive differentiator, thereby increasing competitive differentiation during new business acquisition.

The time for manufactures to make strategic security improvements is now. Effective cybersecurity makes manufactures more prepared, more resilient, and better protected so that they can continue to fulfill their obligations and represent the needs of their customers.

About AgileBlue

AgileBlue is a managed breach detection company with an Autonomous SOC-as-a-Service for 24x7 monitoring, detection and guided response for cloud, digital infrastructures, and applications. AgileBlue

provides their clients with enhanced visibility regarding cyber risk via the AgileBlue analytics reporting dashboard. The company offers a proprietary risk scoring algorithm including industry comparisons and risk analysis trends. AgileBlue's Silencer technology significantly reduces false positives with a 95% confidence score on incident alerts based on their proprietary machine learning and user behavior analytics.

Ready to protect your company? Contact Us.