BlackBerry | Cybersecurity

OPERATIONAL TECHNOLOGY ENVIRONMENTS INSIGHTS GUIDE

ESTABLISHING A SELF-DEFENDING MANUFACTURING FLOOR

BlackBerry | Cybersecurity

Introduction

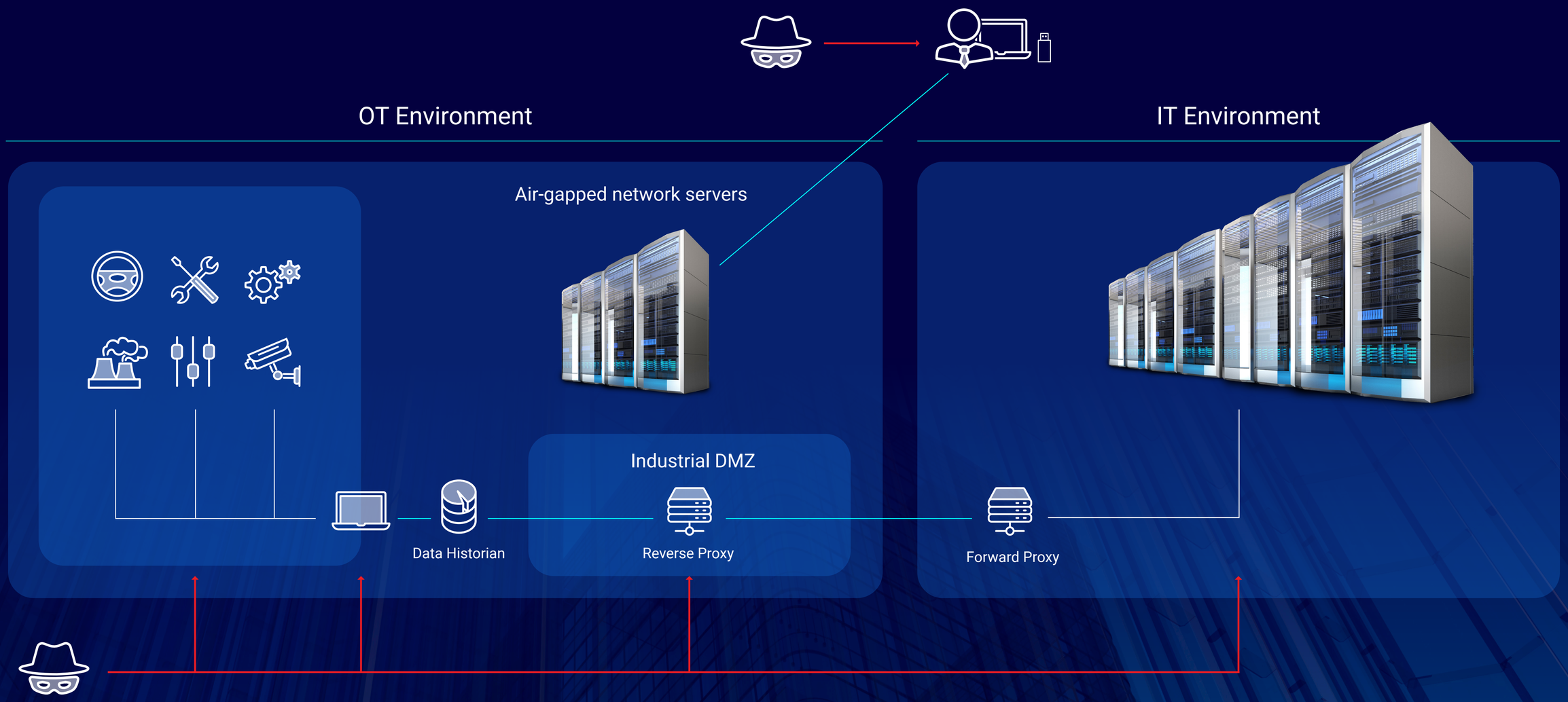
The manufacturing industry is undergoing a transformation to “Industry 4.0,” in which greater digitization, automation, and connectivity, including IoT and robotics, deliver new opportunities for production efficiency.

Such fundamental transformation doesn’t happen quickly: significant time and resources are needed to evaluate, design, purchase, configure, test, deploy, and finally transition to new systems. Most organizations are undergoing a phased transition, in which legacy devices and software will remain in operation for the foreseeable future.

At the same time, manufacturing is facing an unprecedented number of cyberthreats. Securing legacy hardware and software, including air-gapped systems, presents additional security challenges, and the same transformative technologies that enable Industry 4.0 create a larger attack surface to protect. IT and OT integration, and greater connectivity present new entry points and lateral paths between systems for different kinds of attacks. And, manufacturers must secure these complex environments in the face of a worldwide cybersecurity skills shortage.

To protect mission-critical production systems, manufacturers will benefit from a “self-defending” manufacturing floor with proactive threat detection and response that doesn’t require constant manual updates. The ideal self-defending manufacturing floor protects all OT, IoT, robotics, production, control, and IT systems with a single, powerful security solution that is flexible to defend the vast range of current assets and scalable to easily support future technology investments.

BlackBerry | Cybersecurity



Security Challenges in Manufacturing Environments

According to the Cybersecurity and Infrastructure Security Agency (CISA), the critical manufacturing sector reports more attacks on integrated control systems (ICS) than any other critical infrastructure sector.[1] Manufacturing is an attractive target for threat actors because of an increasingly complex attack surface and low risk tolerance: a cyberattack that slows or stops production can easily result in millions of dollars of loss.

Increasing Digitization and Automation

Manufacturing digitization and automation continue to grow, with some experts estimating that global industry could reach more than 500 robots per 10,000 manufacturing employees.[2] While new technologies increase efficiency, they also expand an organization's attack surface by adding potentially vulnerable equipment, including embedded systems and third-party software that must be secured to the manufacturing OT environment.

Legacy Devices and Systems

While the use of newer technologies is growing, many manufacturing environments continue to maintain legacy technology in the form of older devices, protocols, and operating systems that are reliable, cost-effective, and would require significant capital and downtime to replace. Unfortunately, these older assets can be challenging to secure. Siloed legacy systems designed to be air-gapped and physically isolated are now connected through OT integration, which exposes these vulnerable systems to a range of threats. Securing legacy devices requires a comprehensive program that includes applying firmware security patches, installing software updates, and limiting access to authorized users only.

Rising Numbers of Supply-Chain Attacks

Security vulnerabilities throughout the digital supply chain are a significant concern: while interconnectivity with vendor and customer systems can boost efficiency and lower costs, it also expands the attack surface and provides new entry points for threats to enter and proliferate throughout the manufacturing ecosystem. Manufacturers are especially vulnerable to attacks that originate in the digital supply chain because complex OT assets are difficult to secure. In 2022, the number of supply-chain attacks is estimated to have increased by 633 percent.[3] Digital supply chain attacks lead to real-world supply chain problems, as interrupted production affects not only suppliers and customers, but also transportation, logistics, and other interdependent providers throughout the industry.

OT Cybersecurity Skills Shortage

Much has been written about the growing cybersecurity skills shortage, which is currently estimated at 3.4 million globally with deficits of approximately 436,000 in North America and more than 317,000 in Europe, the Middle East, and Asia.[4] Cybersecurity professionals with specialized knowledge of industrial operations may be even more difficult to find. Most manufacturers will benefit from security solutions that reduce the need for administrator intervention and proactively protect and defend any kind of ICS and OT on the manufacturing floor.

3 https://www.csoonline.com/article/3677228/supply-chain-attacks-increased-over-600-this-year-and-companies-are-falling-behind.html

The Growing Manufacturing Cyberthreat

Because of the vital role of manufacturing around the world, more threat actors are focusing their efforts on the IoT and OT systems. According to the FBI, manufacturing is among the top industries targeted by cyber criminals.[5] For example, in 2022, dozens of automotive industry manufacturers publicly acknowledged cyberattacks including ransomware, data theft, and trojans.[6]

Manufacturers often rely on a just-in-time (JIT) supply-chain strategy to maintain a vast ecosystem of vendors and parts, which creates an extremely large attack surface. Because manufacturing may be slowed or stopped if needed components and materials are not immediately available, a successful cyberattack anywhere in the supply chain can effectively halt production. Instead of directly targeting larger manufacturers, which may be heavily fortified against intrusions, malicious adversaries may instead attack their vendors, especially those with less cybersecurity.

Overall, manufacturing organizations are vulnerable to the same tactics, techniques, and procedures (TTPs) as other industries, including ransomware, phishing and spear phishing, trojans, and credential and data theft. Other TTPs that can impact manufacturing include exploiting Internet-accessible hardware with weak authentication and preloading malware into necessary third-party software to provide initial access. Even fully air-gapped environments can be compromised by malicious or unwitting insider threats (e.g., insertion of an infected USB drive) and by infected software upgrades, updates, and patches.

The trend toward increasing IT/OT integration presents new paths for attackers to access the OT environment. As more OT and IT systems become connected, manufacturing organizations that fail to fully secure both environments are exposing a sizable attack surface and increasing both the likelihood and potential damage of a cyber assault.

Manufacturing Cybersecurity Outlook

73%

Number of manufacturers reporting an attack within the past 12 months[7]

$2 million

Average ransom payment for manufacturing organizations, compared to an average $800,000 across all other sectors[8]

87%

Increase in ransomware attacks on industrial firms in 2022[9]

$1.3 million and 8,000 hours

Estimated three-year savings for manufacturer that implements BlackBerry® endpoint protection[10]

BlackBerry | Cybersecurity

Building Operational Resilience

For manufacturers, the risks of cyberattacks are significant. Business-critical data, including intellectual property, customer information, and logon credentials, can be exposed or lost. Financial losses can be extreme, and business disruption can also affect suppliers, service providers, and customers throughout the industry's supply chains. To defend against growing threats, manufacturing organizations need solutions that:

- Detect and respond to known and unknown threats early in the attack chain
- Expand security throughout OT and ICS without increasing administrative burden
- Do not slow production

The Self-Defending Manufacturing Floor

An innovative cybersecurity model for the manufacturing industry is the "self-defending" manufacturing floor that relies on powerful AI to monitor and respond to cyberthreats. Unlike signature-file-based systems, which require continual updates and can only detect threats in the current database, a self-defending system can detect, analyze, and respond to both known and unknown or zero-day threats.

Checklist: Designing a Self-Defending Manufacturing Floor

☐ Comprehensive endpoint security

The solution must identify, manage, and protect every OT endpoint and connection to cover legacy and modern systems that may be air-gapped, Internet-connected, or anywhere in-between.

☐ Prevention-first defense

Proactive self-defense requires an AI-based solution that automatically blocks known and unknown threats in real time so they never enter your ecosystem.

☐ Imperceptible performance impact

No matter how many endpoints are in the manufacturing environment, the solution should offer an ultra-lightweight agent that operates with no detectible impact on performance, even on legacy systems.

☐ Scalable protection for future assets

An effective self-defending solution supports modernization and expansion without the need to "rip and replace," protecting future IT and OT assets through on-premises, hybrid, and cloud-native deployment.

☐ Maximum uptime

To ensure continuity of operations, a self-defending solution will automatically update itself and eliminate the need for manual patches and signature updates.

☐ Streamlined administration

Even in complex environments, the solution should simplify investigations and reduce response times with a holistic view of the enterprise, simplified and customized workflows, and alert grouping and prioritization.

☐ Effective protection for air-gapped environments

Air-gapped environments aren't invulnerable to security threats: The solution must ensure that upgrades, updates, patches, and removable media cannot compromise air-gapped systems.

☐ Superior offline protection

Air-gapped environments receive the same protection as online environments.

Cylance Endpoint Security for the Self-Defending Manufacturing Floor

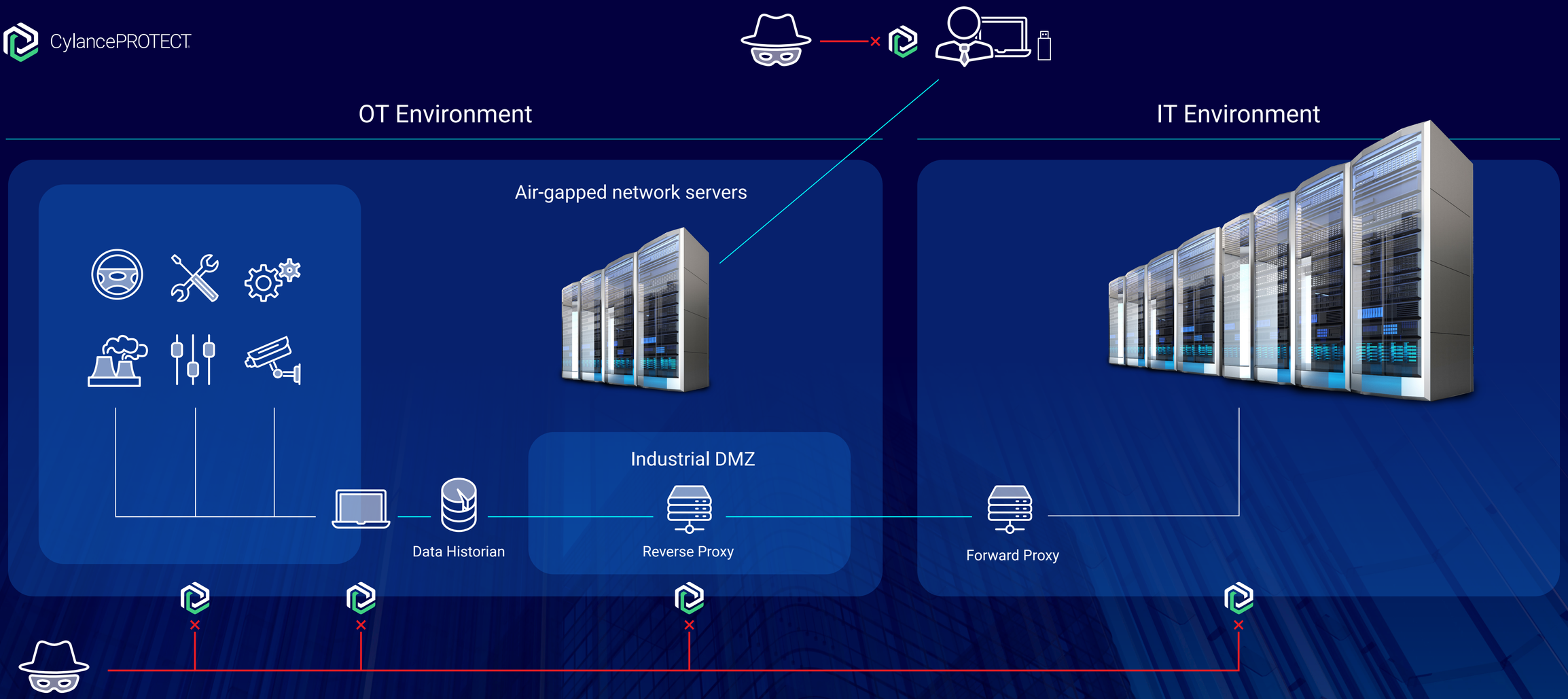
Cylance® endpoint solutions from BlackBerry deliver AI-based protection for all OT assets that minimizes complexity, delivers proven security, and enables uninterrupted evolution and growth. CylancePROTECT® endpoint protection enables manufacturers to mitigate the ever-growing risk of cyberattacks while decreasing costs, with benefits that include:

- **Superior support for legacy and air-gapped systems**. CylancePROTECT offers the broad support for legacy OT systems, ensuring that older and air-gapped assets are protected as effectively as online environments.
- **Minimal impact on performance**. CylancePROTECT relies on a lightweight agent designed to deliver complete endpoint security without affecting operations, even on older systems.
- **Equal Protection for Offline and Online Environments.** CylancePROTECT defends all device types and operating systems both offline and online.
- **Easy management.** CylancePROTECT offers a single management console that simplifies security setup and maintenance and eliminates the need for signature file updates. The solution streamlines investigation and response security and reduces noise and alert fatigue so staff can quickly and easily understand and respond to threats.
- **Maximum uptime**. AI-based CylancePROTECT is always running and always up to date, minimizing routine interruptions for updating files as well as disruptions due to active threats. The solution simplifies analyst investigations and reduces response time to support ongoing operational continuity.
- **Scalability**. CylancePROTECT can scale and expand to continually protect vital assets as manufacturing technologies change and grow.

> “One of the chief benefits of BlackBerry in ICS is our ability to ensure a preventative state without having to constantly update the endpoint agent or rely on cloud connections. This is of particular value for offline endpoints and air-gapped networks, but the benefits go deeper.”
>
> **Nathan Jenniges,** Vice President of Product Strategy, Cybersecurity

BlackBerry | Cybersecurity

CylancePROTECT



BlackBerry | Cybersecurity

Case Study: Energy Company Secures Air-Gapped OT and ICS Assets with BlackBerry

A U.K. energy provider sought a strategy to secure operations at power stations where some systems were up to 40 years old. The heterogenous, primarily air-gapped environment included ICS, process control management, and PLCs as well as laptops used to program and configure systems. The company's goal was to secure their assets without requiring time- and resource-consuming manual updates.

To protect and defend their OT and ICS assets, the company chose CylancePROTECT. The BlackBerry solution was deployed on endpoints within the standalone air-gapped network environment. A single secure endpoint was allowed to connect to the company's IT network to support real-time threat monitoring and response.

CylancePROTECT enabled the company to eliminate old-fashioned signature file updates and deliver proactive AI-based protection against cyberthreats. When the Office for Nuclear Regulation reviewed the company's cybersecurity provisions, they responded positively to the CylancePROTECT solution.

[1] https://www.cisa.gov/sites/default/files/publications/19_0830_cisa_insider-threat-programs-for-the-cm-sector-implementation-guide.pdf
[2] https://www.globalxetfs.com/industrial-robotics-predictors-suggest-continued-growth-in-2023/
[3] https://www.csoonline.com/article/3677228/supply-chain-attacks-increased-over-600-this-year-and-companies-are-falling-behind.html
[4] https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx
[5] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
[6] https://www.blackberry.com/content/dam/bbcomv4/global/pdf/0408-Threat-ReportV17.pdf
[7] https://prod.ucwe.capgemini.com/wp-content/uploads/2022/06/Cybersecurity-in-Smart-Factories_Web-2.pdf
[8] https://www.securityweek.com/industrial-ransomware-attacks-new-groups-emerge-manufacturing-pays-highest-ransom/
[9] https://www.bloomberg.com/news/articles/2023-02-14/ransomware-attacks-on-industrial-firms-increased-by-87-in-2022
[10] https://www.blackberry.com/us/en/campaigns/2022/na/forrester-tei-report-cylanceprotect

BlackBerry Intelligent Security. Everywhere.

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 215M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry | Cybersecurity