PARTNER FORTINET

BEST PRACTICES GUIDE:

Safeguarding Operational Technology Infrastructure

Our **recent study** found that cybersecurity in operational technology (OT) ranks as a top-5 business risk. At least 61% of respondents reported incidences of data breaches in the last 12 months, 43% of which resulted in operational outages affecting productivity, as well as other business outcomes.

Evidence of blind spots to complex threats was born out in the high variability between companies in both tracking protocols and security capabilities. Two in five manufacturing leaders acknowledge that "undefined policies, procedures and best practices" still rank among the top barriers to effective response.

To help manufacturers truly understand the risks to their OT, this best practice guide offers recommendations and leading practices for OT prevention, detection, and response.

The study and this guide are produced by the Manufacturers Alliance for Productivity and Innovation (MAPI) in conjunction with Fortinet.

Identifying Leading Practices and Technology Partners

The complex nature of cybersecurity threats today requires solutions that integrate people, processes, and technologies. Employees, third-parties, and anyone who accesses data and control systems must follow critical frameworks, policies, and protocols. As one MAPI member explained, *"we should be adhering to standard frameworks like the NIST framework, and taking a true risk-based approach to how we're going to go after ensuring that we're at a security posture that we deem appropriate for our business."*

People, process, and technology inputs are also highly interdependent in the OT security environment. Technology and know-how are critical to elevating security protections. A majority of manufacturers surveyed (60%) do rely on external (contracted) resources. Most commonly they use a mix of both internal and external support when responding to OT security breaches, rather than going it alone.

Integrating third-party security providers for security strategy on the front-end is important too. Providers typically compete with either a platform of solutions or as point solutions designed for a focused task. A platform solution provides an architecture to support legacy and industry-specific solutions, as well as an ecosystem of products and suppliers that are already integrated. By comparison, point solutions are typically single-function products that solve a specific need but are often not integrated, which may imply additional work to roll up data to inform decision-making.

Regardless of the specific solution, technologies and network security stand to benefit from incorporating leading practices that promote greater visibility, control and continuous monitoring – what Fortinet has identified as the OT "security fabric." As a leading solutions provider in the space, Fortinet has called attention to many principles in OT cybersecurity best practice, including:

- Identifying assets, classifying them, and prioritizing value
- Segmenting the network dynamically
- Analyzing traffic for threats and vulnerabilities
- Securing both wired and wireless access

Our research, published in the report, "**Securing Critical Operational Technology in Operations,**" has further identified a low incidence in the manufacturing industry on specific tracking protocols and security capabilities. These form the basis for the selected practices highlighted in this guide. While not exhaustive, they represent a set of areas that may separate leading manufacturers from the rest when it comes to securing critical infrastructure.

> *"We assessed our largest and oldest factory because we figured we'd get a worst-case analysis. That really was extremely helpful in helping us put together the high, moderate, low-risk areas for us to focus."*
>
> *– Global manufacturing executive*

Prevention

Effective prevention mitigates cyber risk. In the area of prevention, must-have practices include:

- ❒ **Firewalls between the IT/OT networks** – prevent unwanted network connections while whitelisting approved connections. Consider firewalls that provide "traffic inspection" on the network, such as intrusion protection services (IPS) to detect known vulnerabilities.
- ❒ **Specific access protocols** – introduce purpose-built technologies to accommodate complex SCADA/ICS systems and provide full network visibility, control, and protection with advanced firewalls and authentication (e.g., tokens).
  - ❒ **Multifactor authentication** – require two or more separate factors for verification to make it more difficult for intruders to steal login credentials. Ensure encryption and authentication for all wireless OT networks.
  - ❒ **Role-based access control (RBAC)** – restrict network access based on an employee's role within an organization, for example, their authority, responsibility, and job competency level.
  - ❒ **Internal network segmentation** – restrict access and movement across a network by implementing firewalls to segment and layer "zones," such that one failure in the network can be contained and not affect other parts of the network.
- ❒ **Security compliance management and monitoring (e.g., cybersecurity audit)** – conduct a security assessment to set a baseline and action plan for continuous improvement in management and monitoring. Periodic auditing of employees, architecture, and technology capabilities can uncover vulnerabilities and provide actionable results.
- ❒ **Training and education, especially on phishing** – train employees on the tools and resources to protect the company against malware from phishing, a stubbornly common source for security breaches.

Detection

"Every so often we do some comprehensive testing across the board that involves things that are network-based, or application services, on our customer portal or our web presence. In the course of this, we include plant sites since we're partnered up with all kinds of physical security, and we test that too for more of a continuous view."

– Infrastructure and security executive

Effectiveness of detection should be measured in the ability to monitor for known vulnerabilities, such as remedying incidents before they are breaches. Detection also should cover unknown threats and anomalies. In the area of detection, must-have practices include:

- ❒ **Asset discovery and understanding of the operating environment** – discover and keep track of all active and inactive applications across the cloud, virtual, mobile, and on-premises environments to allow for monitoring of vulnerabilities and intrusions.
  - ❒ **Traffic analysis employing user and entity behavior analytics (UEBA) and machine learning (ML)** – extend visibility and understanding of an active environment with known threats (previously discovered) as well as unknown threats using advanced analytics.
  - ❒ **Security information and event management (SIEM) capabilities** – manage system configuration, detect threats, and review and log for auditing both to learn about breaches and produce reporting.
- ❒ **Vulnerability assessment and management scanning** – define the attack surface fully and ensure active device and traffic profiling. Deploy software solutions for automated processes to discover, analyze, and report on vulnerabilities in networks, infrastructure, and applications.
- ❒ **Other tools for security analysis, monitoring, and assessment** – use a centralized network analysis tool for visibility and intelligence on known and unknown threats.
  - ❒ **Sandboxing** – detect threats on the OT network and automate quarantines to prevent them from doing damage.
  - ❒ **Deception** – use "honeypots" to detect hackers active in the network to reveal them to the Security Operations Center (SOC) team.

Response

> *"A successful response is quickly identifying the problem and figuring out the root cause so we can lock it down, isolate it, quarantine it, or eliminate it. As it pertains to a particular breach, it's also identifying what was lost or compromised, and then having a quick turnaround time with legal, audit, or somebody else to find out what the appropriate response would be from the company point of view."*
> *– Information security executive*

The effectiveness of the response should be measured by the ability to neutralize the event without causing operational downtime. In the area of response, must-have practices include:

❐ **Process documentation** – create and update documented response policies and protocols and ensure standards for implementation, auditing, and pressure testing over time.

❐ **Incidence response (IR) planning** – test policies and procedures to help employees respond to and recover from network security incidents, including data breaches. For IR services, know who you would call when this happens so you are not doing your discovery and evaluation when you've been hacked.

❐ **Visibility of security status** – apply network analysis tools to provide real-time intelligence.

❐ **Remote management of physical security** – configure remote connectivity for OT management securely by mitigating risks/vulnerabilities with parties that further expand the attack surface.

❐ **Endpoint detection and response (EDR) technologies and incident response (IR)** – mitigate threats and automatically start the restoration process while keeping the endpoint online and productive. This can keep the factory up and running even if a ransomware virus becomes active.

❐ **Security orchestration, automation, and response (SOAR) technology** – an emerging and evolving practice, SOAR technology allows for data collection on security threats from multiple sources and responds automatically to remedy them without human assistance.

Recommended Resources

- MAPI and Fortinet: Securing Critical Operational Technology in Manufacturing
- Fortinet: State of Operational Technology and Cybersecurity Report

About the Authors

David Beckoff

VP, Product Development and Insights, MAPI

David Beckoff is VP, Product Development and Insights at MAPI, where he is responsible for association research, benchmarking programs, and special events for the manufacturing community. Prior to joining MAPI, he served as Research Director at Gartner and led cross-industry studies on topics including data analytics, digital transformation, customer experience, and talent development.

Richard K. Peters (Rick)

CISO, Operational Technology North America, Fortinet

Rick brings the Fortinet OT-CI team more than 37 years of cybersecurity and global partnering experience working across foreign, domestic, and commercial industry sectors at the National Security Agency (NSA). As Fortinet's Operational Technology North American CISO, he delivers cybersecurity defense solutions and insights for the OT/ICS/SCADA critical infrastructure environments.

Prior to Fortinet, Rick led development of cyber capability across Endpoint, Infrastructure, and Industrial Control System technologies at the agency.

Peter Newton

Senior Director of Products and Solutions, Fortinet

Peter Newton is a Senior Director of Products and Solutions at Fortinet, where he oversees the Secure Access, OT, and IoT solutions. He brings 20 years of experience with computer networking and security, working at both chip-level and system-level solutions for companies including AMD, Netgear, Silver Spring Networks, and Fortinet. Prior work experience includes being an officer in the US Navy. Peter holds a Bachelor's of Science in Electrical Engineering from Rice University and a Master's in Business Administration from the University of Texas at Austin.

FORTINET®

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future.

For more information, visit **fortinet.com**.

MAPI

Founded in 1933, the Manufacturers Alliance for Productivity and Innovation is a nonprofit organization that connects manufacturing leaders with the ideas they need to make smarter decisions. As the manufacturing leadership network, its mission is to build strong leadership within manufacturing to drive the growth, profitability, and stature of global manufacturers.

For more information, visit **mapi.net**.