Media Contact:	Investor Contact:	Analyst Contact:
Travis Anderson Fortinet, Inc. 408-235-7700 pr@fortinet.com	Peter Salkowski Fortinet, Inc. 408-331-4595 psalkowski@fortinet.com	Brian Greenberg Fortinet, Inc. 408-235-7700 analystrelations@fortinet.com

Fortinet Report: Threat Actors Are Increasingly Targeting OT Organizations

Nearly one-third (31%) of OT organizations reported more than six intrusions in the last year, up from 11% the year before

SUNNYVALE, Calif., May 29, 2024

John Maddison, Chief Marketing Officer at Fortinet
"Fortinet's 2024 State of Operational Technology and Cybersecurity Report shows that while OT organizations are making progress in strengthening their security posture, teams still face significant challenges in securing converged IT/OT environments. Adopting essential tools and capabilities to enhance visibility and protections across the entire network will be vital for these organizations when it comes to reducing the mean time to detection and response and ultimately reduce the overall risk of these environments."

News Summary
Fortinet® (NASDAQ: FTNT), the global cybersecurity leader driving the convergence of networking and security, today announced the findings from its global 2024 State of Operational Technology and Cybersecurity Report. The results represent the current state of operational technology (OT) security and highlight opportunities for continued improvement for organizations to secure an ever-expanding IT/OT threat landscape. In addition to trends and insights impacting OT organizations, the report offers best practices to help IT and OT security teams better secure their environments.

While this year's report indicates that organizations have made progress in the past 12 months related to advancing their OT security posture, there are still critical areas for improvement as IT and OT network environments continue to converge.

Key findings from the global survey include:

- **Cyberattacks that compromise OT systems are on the rise.** In 2023, 49% of respondents experienced an intrusion that impacted either OT systems only or both IT and OT systems. But this year, nearly three-fourths (73%) of organizations are being impacted. The survey data also shows a year-over-year increase in intrusions that only impacted OT systems (from 17% to 24%). Given the rise in attacks, nearly half (46%) of respondents indicate that they measure success based on the recovery time needed to resume normal operations.
- **Organizations experienced a high number of intrusions in the past 12 months.** Nearly one-third (31%) of respondents reported more than six intrusions, compared to only 11% last year. All intrusion types increased compared to the previous year, except for a decline in malware. Phishing and

compromised business email intrusions were the most common, while the most common techniques used were mobile security breaches and web compromise.

- **Detection methods aren't keeping pace with today's threats.** As threats grow more sophisticated, the report suggests that most organizations still have blind spots in their environment. Respondents claiming that their organization has complete visibility of OT systems within their central security operations decreased since last year, dropping from 10% to 5%. However, those reporting 75% visibility increased, which suggests that organizations are gaining a more realistic understanding of their security posture. Yet more than half (56%) of respondents experienced ransomware or wiper intrusions—an increase from only 32% in 2023—indicating that there is still room for improvement regarding network visibility and detection capabilities.
- **Responsibility for OT cybersecurity is elevating within executive leadership ranks at some organizations.** The percentage of organizations that are aligning OT security with the CISO continues to grow, increasing from 17% in 2023 to 27% this year. At the same time, there was an increase to move OT responsibility to other C-suite roles, including the CIO, CTO and COO, to upwards of 60% in the next 12 months, clearly showing concern for OT security and risk in 2024 and beyond. Findings also indicate that some organizations, where the CIO is not outright responsible, there is an upward shift of these responsibilities from the Director of Network Engineering to the Vice President of Operations role, which illustrates another escalation of responsibility. This elevation into the executive ranks and below, regardless of the title of the individual overseeing OT security, may suggest that OT security is becoming a higher-profile topic at the board level.

Best Practices

Fortinet's global 2024 State of Operational Technology and Cybersecurity Report offers organizations actionable steps for enhancing their security posture. Organizations can address OT security challenges by adopting the following best practices:

- **Deploy segmentation.** Reducing intrusions requires a hardened OT environment with strong network policy controls at all points of access. This kind of defensible OT architecture starts with creating network zones or segments. Teams should also evaluate the overall complexity of managing a solution and consider the benefits of an integrated or platform-based approach with centralized management capabilities.
- **Establish visibility and compensating controls for OT assets.** Organizations must be able to see and understand everything that's on the OT network. Once visibility is established, organizations must protect any devices that appear to be vulnerable, which requires protective compensating controls that are purpose-built for sensitive OT devices. Capabilities such as protocol-aware network policies, system-to-system interaction analysis, and endpoint monitoring can detect and prevent the compromise of vulnerable assets**.**
- **Integrate OT into security operations and incident response planning.** Organizations should be maturing towards IT-OT SecOps. To achieve this, teams must specifically consider OT with regard to SecOps and incident response plans. One step teams can take to move in this direction is to create playbooks that incorporate the organization's OT environment.
- **Embrace OT-specific threat intelligence and security services.** OT security depends on timely awareness and precise analytical insights about imminent

risks. Organizations should make sure their threat intelligence and content sources include robust, OT-specific information in their feeds and services.
- **Consider a platform approach to your overall security architecture.** To address rapidly evolving OT threats and an expanding attack surface, many organizations use a broad array of security solutions from different vendors, resulting in an overly complex security architecture. A platform-based approach to security can help organizations consolidate vendors and simplify their architecture. A robust security platform that is purpose-built to protect both IT networks and OT environments can provide solution integration for improved security efficacy while enabling centralized management to enhance efficiency.

Report Overview

- The Fortinet 2024 State of Operational Technology and Cybersecurity Report is based on data from a global survey of more than 550 OT professionals, conducted by a third-party research company.
- Survey respondents were from different locations around the world, including Australia, New Zealand, Argentina, Brazil, Canada, Mainland China, France, Germany, Hong Kong, India, Japan, Mexico, Norway, South Africa, South Korea, Spain, Taiwan, Thailand, United Kingdom, and the United States, among others.
- Respondents represent a range of industries that are heavy users of OT, including: manufacturing, transportation/logistics, healthcare/pharma, oil, gas, and refining, energy/utilities, chemical/petrochemical, and water/wastewater.
- Most of those surveyed, regardless of title, are deeply involved in cybersecurity purchasing decisions. Many respondents are responsible for operations technology at their organization and/or have reporting responsibility for manufacturing or plant operations.

Additional Resources

- Read the full report to learn more about the state of OT security in 2024.
- Learn about how the Fortinet Security Fabric platform brings end-to-end security to organizations of all sizes to prevent ransomware across all points of entry.
- Learn more about Fortinet's commitment to product security and integrity, including this recent blog post on its longstanding commitment to responsible product development and vulnerability disclosure approach and policies.
- Learn about Fortinet's free cybersecurity training programs, which include broad cyber awareness and product training. As part of the Fortinet Training Advancement Agenda (TAA), the Fortinet Training Institute also provides training and certification through the Network Security Expert (NSE) Certification, Academic Partner, and Education Outreach programs.
- Learn more about FortiGuard Labs threat intelligence and research and Outbreak Alerts, which provide timely steps to mitigate breaking cybersecurity attacks.
- Learn more about Fortinet's FortiGuard Security Services portfolio.
- Follow Fortinet on X, LinkedIn, Facebook, and Instagram. Subscribe to Fortinet on our blog or YouTube.

About Fortinet

Fortinet (NASDAQ: FTNT) is a driving force in the evolution of cybersecurity and the convergence of networking and security. Our mission is to secure people, devices, and data everywhere, and today we deliver cybersecurity everywhere you need it with the largest integrated portfolio of over 50 enterprise-grade products. Well over half a million customers trust Fortinet's solutions, which are among the most deployed, most patented,

and most validated in the industry. The Fortinet Training Institute, one of the largest and broadest training programs in the industry, is dedicated to making cybersecurity training and new career opportunities available to everyone. Collaboration with high-profile, well-respected organizations from both the public and private sectors, including CERTs, government entities, and academia, is a fundamental aspect of Fortinet's commitment to enhance cyber resilience globally. FortiGuard Labs, Fortinet's elite threat intelligence and research organization, develops and utilizes leading-edge machine learning and AI technologies to provide customers with timely and consistently top-rated protection and actionable threat intelligence. Learn more at https://www.fortinet.com, the Fortinet Blog, and FortiGuard Labs.