FORTINET

POINT OF VIEW

Why CISOs Need an OT Security Platform

Meet Strategic Goals While Securing OT Environments

Executive Summary

Any company with industrial assets faces elevated cybersecurity risks from their operational technology (OT) environments. Although many CISOs have not been responsible for or prioritized OT in the past, they should examine their strategic goals of vendor consolidation and the convergence of their information technology (IT) systems with OT. An OT security platform can help CISOs meet immediate cybersecurity needs and offer the flexibility to help them meet their strategic goals in the future.

Recent cyber events such as the Clorox attack have led to operational losses due to production stoppages.[1]

The Evolution of Security Teams

At many organizations, CISOs are now in charge of OT cybersecurity. This change is relatively recent, so many IT teams haven't seen the unique devices and communication protocols typically used in OT environments. IT security policies also generally didn't have to consider the operational priorities of personnel safety and production reliability. But now, as IT and OT security teams are combined, they must collaborate to meet security requirements across IT and OT systems.

Implementing firewalls, network segmentation with switches, and basic access controls and logging are common techniques used to secure IT and OT. But OT environments include a new realm of security challenges, potential solutions, and vendors that may be new to IT teams. Because OT security is relatively new, many of the vendors in this environment are new as well. In a rush to meet new OT security demands, a number of new, specialized products have appeared, along with an increase in the number of vendors that teams need to assess, implement, and manage.

Tackle OT Security Challenges

The lack of security and network personnel continues to plague industry and asset owners while cybersecurity risks intensify. The specialization of OT exacerbates the gap in security personnel. Compounding the OT security personnel deficit, securing OT was not a top-level priority in the past, so OT security funding for solutions and personnel was limited, leading to small and overwhelmed OT teams.

As OT risk has risen, there has been an increase in oversight, budget, and personnel (in the form of non-OT specialists) being thrown at the OT security challenges. For a CISO, taking on new OT challenges and expending vital resources is the first step to initiating change and securing OT. Over time, however, CISOs must determine who will operate these solutions to ensure operational continuity. CISOs must look for opportunities to optimize and converge IT and OT solutions and personnel to alleviate staffing shortages.

As they construct and deploy their OT security strategies, CISOs should consider an OT platform approach. An OT security platform that is an extension of an IT platform enables IT/OT convergence and the optimization of security solutions and the personnel required to operate the platforms. This platform approach allows for centrally managing security and network solutions in both IT and OT networks. Extending zero-trust security methods to the OT platform also improves OT security while decreasing the need for additional personnel. The ability to create a joint IT/OT security operations center while safeguarding production-related security decisions and actions is the culmination of IT/OT convergence.

According to Gartner, "Security platform consolidation, zero trust strategies, and generative AI are key developments for this Hype Cycle. Security and risk management leaders should consolidate security platforms and adopt suitable emerging technologies to boost efficiency and gain wider security visibility."[2]

Reduce Vendor Sprawl

One way to limit the chaos of choices and vendors is to look for a platform specific to OT. Using an OT security platform promotes vendor consolidation. An OT security platform has solutions to make the first connections to the factories or infrastructure. Also, it includes more advanced solutions like zero-trust capabilities and OT-specific security operations (OT SecOps) to support teams as their OT security program matures.

The solutions in an OT security platform should be powered by the latest OT threat intelligence and be able to integrate with existing and new solutions. Ideally, an OT security platform helps ensure ease of solution deployment and operation and uses all available OT security data in its suite of solutions.

Support IT/OT Convergence

As common security solutions in an OT security platform bridge the IT/OT gap and enable operations across both networks, it can help optimize resources in terms of budget and personnel. Merging an organization's IT and OT platforms promotes IT/OT convergence strategies.

CISOs should evaluate vendors based on their ability to provide an OT platform. Many organizations already have an IT platform because IT security is more mature and less operationally sensitive. However, the OT market is less mature, and few OT platforms exist in the varied OT vendor landscape. Because of the unique requirements of OT security, questions related to finding an OT platform can be critical, unlike IT strategies, which can more easily be altered later. Although CISOs can certainly manage IT and OT platforms together, the most critical decisions hinge on the correct selection of an OT platform.

Consolidation and Convergence Is Achievable

To mitigate production and reliability risks, many CISOs are taking on new responsibilities for securing OT production environments or critical infrastructure. When making initial assessments and exploring the OT vendor market, CISOs must keep their corporate strategies of vendor consolidation and IT/OT convergence in mind. To meet their short-term and long-term goals, CISOs should consider an OT platform. By taking this platform approach, vendor consolidation is inherent, and IT/OT convergence is achievable.

[1] Reuters, Clorox, reeling from cyberattack, expects quarterly loss, October 4, 2023.

[2] Gartner, Hype Cycle for Workload and Network Security, July 31, 2023.

FORTINET

www.fortinet.com