ONAPSIS

ERP Security for Heavy and Discrete Manufacturing

Cyber attacks targeting critical ERP, product innovation, and supply chain applications within the heavy and discrete manufacturing industry can have far-reaching financial and reputational impacts. A successful attack could delay key digital transformation projects, interfere with business continuity and product safety, or put company intellectual property (IP) at risk. With the number of cyber attacks targeting manufacturers aggressively growing, organizations are challenged to protect their critical systems and ensure the safety of their products while meeting accelerated demand for digitization and sustainability.

39% of manufacturers experienced a breach in last 12 months[1]

$4.5M = average cost of data breach for manufacturing industry[2]

34% of manufacturers say theft of intellectual property is their top cyber threat[1]

Key Risk Factors

Direct ERP Attacks on the Rise

Cyber attacks targeting manufacturing are on the rise. Successful attacks on ERP systems can be particularly devastating, with the potential to disrupt supply chains, interfere with product safety and delivery, and result in loss of employee PII or company IP.

More Digitization and Interconnectivity

COVID-19-induced supply chain instability and increased global competition are driving a need for more digitization and interconnectivity between business processes and systems, so organizations can be more resilient and respond more quickly to changing supply and demand.

New Models and Processes Needed to Support Sustainability

Facing both regulatory and consumer pressure, manufacturers are adopting new service-based models, Industry 4.0 technologies, circular supply chains, and green manufacturing processes to reduce emissions and create greener products.

Key Challenges

Security Is Often an Afterthought in Digital Transformation

The need for supply chain digitization and faster product innovation is driving digital transformation at unprecedented speed, often at the sake of security. The tendency has been to bolt on security after the fact, which leads to unaddressed risk, project delays, and cost overruns.

Under-Resourced Teams

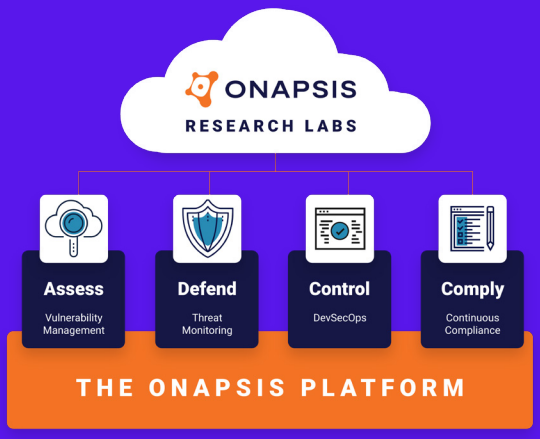
Workforce shortages, particularly in cybersecurity, mean teams must balance high priority digitization initiatives with ensuring resiliency and integrity of ERP, product innovation, and supply chain systems and data. This can be particularly challenging since many security teams lack experience with these systems.

Limited Visibility for Security Teams

Limited or restricted visibility into ERP applications and assets across complex and interconnected landscapes results in the inability to effectively protect systems supporting digital supply chains, product innovation, other business-critical operations, and the massive amount of data within these systems.

[1] Cyber Risk in Advanced Manufacturing, Deloitte
[2] Cost of a Data Breach Report 2022, IBM Security

Solution:
Onapsis Provides a Better Approach to ERP Security



Fortunately, securing your complex ERP landscape doesn't have to be complicated, even with all the advanced threats and attacks out in the wild. That's where Onapsis comes in. As the undisputed experts in business application security with the most prolific threat research team for SAP and Oracle, Onapsis has been on the frontlines securing the world's leading heavy and discrete manufacturers for over a decade now. With Onapsis, you get complete 360 degree security for your critical ERP applications, helping you:

- ☑ Automate security, so you can avoid delays and audit findings and focus on core transformation tasks, while ensuring your critical systems and data stay protected
- ☑ Gain research-driven analysis and focused threat intel from industry experts, so even teams new to ERP can quickly and effectively understand and act on risk
- ☑ Integrate with ticketing systems and SIEMs, so ERP can be brought into existing processes and SOC playbooks

Case Study

F500, $120B Automobile Manufacturer Builds SAP Vulnerability Management Program, Reduces MTTR and Improves Patching Process

Challenge: A history of manual patching processes created a backlog of SAP Security Notes, and their existing vulnerability management tools didn't provide visibility into other vulnerabilities within SAP, leaving their critical systems exposed. Following news of a critical severity vulnerability in SAP, the Board of Directors tasked the CISO with strengthening their SAP cybersecurity program to minimize their attack surface.

Solution: Onapsis provided comprehensive vulnerability management capabilities that allowed these new-to-SAP security teams to better comprehend and minimize their attack surface while more easily identifying direct SAP threats. The automobile manufacturer gained the visibility and context they needed to reduce investigation and remediation times and achieve greater risk reduction with significantly less effort.

75%
Reduction in mean time to remediate (MTTR) for SAP vulnerabilities

90%
Spent validating SAP Notes were applied correctly

300+
hours/month saved on SAP vulnerability management efforts

Learn more about **how Onapsis helps heavy and discrete manufacturers protect the systems and data supporting their ERP**, digital supply chains, product innovation, and other business-critical operations.

ONAPSIS

onapsis.com/heavy-manufacturing