ERP Security for
Retail / Fashion Manufacturing

ONAPSIS

Cyber attacks targeting critical ERP, supply chain, and e-commerce applications within the retail manufacturing industry can have far-reaching financial and reputational impacts. A successful attack could delay key digital transformation projects, interfere with business continuity and the ability to deliver quality products to consumers, or put customer personally identifiable information (PII) at risk. With cyber attacks targeting retail on the rise, organizations are challenged to protect their critical systems and data while meeting accelerated demand for digitization and increasing privacy regulations.

75% year-over-year increase in ransomware attacks targeting retail[1]

39% of manufacturers experienced a breach in last 12 months[2]

$4.5M average cost of data breach for manufacturing industry[3]

Key Risk Factors

Direct ERP Attacks on the Rise

Cyber attacks targeting retail are on the rise. Successful attacks on ERP systems can be particularly devastating with the potential to disrupt supply chains, interfere with product quality and delivery, interrupt e-commerce, and result in loss of employee or consumer PII.

More Digitization and Interconnectivity

COVID-19-induced supply chain instability and shifting consumer expectations 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.

Expanded E-Commerce and Digital Sales

As more retail manufacturers go direct-to-consumer or enhance their e-commerce experiences to address evolving market demand, protecting consumer PII must be top of mind. Failure to do so could result in significant financial loss due to reputation damage or compliance violation (e.g., GDPR, CCPA).

Key Challenges to ERP Security

Security Is Often an Afterthought in Digital Transformation

The need for supply chain digitization and innovative, integrated e-commerce solutions 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 can lead to unaddressed risk, project delays, and cost overruns.

Under-Resourced Teams

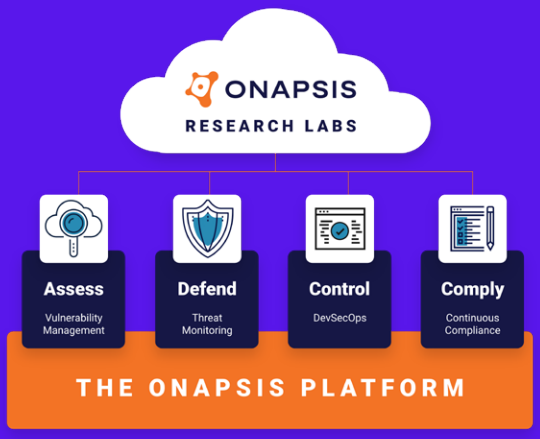
Workforce shortages, particularly in cybersecurity, mean teams must balance high priority digitization initiatives with ensuring resiliency and integrity of ERP, e-commerce, and supply chain systems and data. This can be particularly challenging since many security teams lack experience with these systems.

Limited Visibility for Security Teams

Limited or restricted visibility into ERP applications and assets across complex and interconnected landscapes results in unaddressed risk to the systems supporting digital supply chains, e-commerce, and other business-critical operations, as well as limited protection of the data within these systems.

[1] The State of Ransomware in Retail 2022, Sophos
[2] Cyber Risk in Advanced Manufacturing, Deloitte
[3] 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 retail 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 security can quickly and effectively comprehend and act on risk
- Integrate with ticketing systems and SIEMs, so ERP can be brought into existing processes and SOC playbooks

Case Study

F1000, $5.5B Apparel Manufacturer Eliminates SAP Cybersecurity Blind Spot, Brings ERP Events into the SOC to Reduce MTTR and Improve Incident Response Times

Challenge: The CISO, newly tasked with overseeing SAP security, had little experience with SAP and knew their existing security tools (e.g., Tenable vulnerability management, Splunk SIEM) didn't provide the support they needed.

Solution: Onapsis provides comprehensive vulnerability management that translates SAP security issues into risk, allowing new-to-SAP teams to easily identify, understand, and respond. Continuous threat monitoring from Onapsis can be integrated with Splunk so SOC teams gain an early warning system and pre-patch protection against cyberattacks targeting their critical SAP applications.

83%

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

40

hours/week saved by eliminating manual data extraction and collaboration

73%

In incident response times due to Splunk integration

Learn more about **how Onapsis helps retail manufacturers protect the systems and data supporting their ERP, digital supply chains, e-commerce,** and other business-critical operations.

ONAPSIS

onapsis.com/retail-manufacturing