



Fortune 250 Biotechnology Company **Builds SAP Cybersecurity Program, Reduces Mean Time to Remediate (MTTR) by 83%**



Industry:
Biotechnology



Company Size:
20K+ employees; >\$20B revenue

“A threat to our SAP applications is a threat to the patients that rely on our products. With Onapsis we can be proactive with our SAP security and keep our critical applications - and patients - safe. Their vulnerability assessments allow us to understand and act on the risk within our landscape, while their continuous threat monitoring ensures we have pre-patch protection and compensating controls in place until we can apply the appropriate patch or fix.

Global Lead of SAP Operations, F250 Biotechnology Company

Challenge

No visibility into vulnerabilities or suspicious activities that put critical supply chain and manufacturing applications - and patient safety - at risk

One of the world's leading independent biotechnology companies depends on SAP for their supply chain, manufacturing, international trade, and other business-critical operations. Knowing that a “threat to SAP is a threat to the patients that rely on their products”, they knew they needed to harden their applications against internal and external threats. But, their already under-resourced teams didn't know where to start. They had a growing backlog of patches, but no easy way to prioritize them. They tried to leverage their existing vulnerability management technology, but realized it didn't sufficiently support SAP. They wanted to bring SAP events into their SIEM so they could be incorporated into their incident response processes, but they lacked the threat intelligence and monitoring technology to do so. Unhappy with the SAP gaps in their existing security solutions, processes, and internal knowledge, they sought a third party technology that would give them the visibility and context they needed to help them better understand and manage their SAP attack surface.

Solution

Onapsis automated vulnerability scans provide actionable visibility into risk within critical SAP applications, while its powerful threat monitoring acts as an early warning system for potential cyberattacks

The biotech company found their ideal solution with Onapsis, whose security technologies are designed specifically for ERP systems like SAP. The automated scans, rich research-backed results, and remediation guidance provided by Onapsis Assess offsets the organization's lack of internal SAP security expertise and has enabled them to finally build a strong vulnerability management program for SAP. Now, they can quickly understand the true risk to their critical applications and they're armed with the context they need to prioritize and act on it.

With Onapsis Defend, the organization has enabled continuous threat monitoring for SAP, leveraging over 2,000 detection rules, anomaly scoring, and mitigation guidance from the industry-leading Onapsis Research Labs. Defend acts as an early warning system, alerting the chemical company of unauthorized changes, misuse, or cyberattacks targeting their SAP applications. With Defend, the company has also gained compensating controls and pre-patch protection because the unique, proactive threat intel that powers Defend allows them to monitor for potential exploit activity before patches are released (zero-day vulnerabilities) or have been applied (known, unpatched vulnerabilities). Given their growing backlog of patches and their lengthy patching processes, having some protection before fixes can be applied has been a key benefit for the organization.

“With Onapsis, we can now quickly identify and act on risk to our critical SAP systems. Integrating with our existing IBM QRadar solution has further accelerated our response times and given our SOC teams much-needed visibility into threats affecting our critical applications.”

Global Lead of SAP Operations, F250 Biotechnology Company

Results

Using Onapsis Assess and Defend, the Biotechnology company has experienced:

83% Reduction in Mean Time to Remediation (MTTR)

96% Reduction in remediation time for emergencies

75% Improved incident response times

75% improved incident response times and 83% reduction in remediation time thanks to Onapsis automation and intelligence

With Onapsis Assess, the organization is able to automate their vulnerability checks and measure the security risk of each vulnerability so they can prioritize fixes. Step-by-step technical solutions and an integration with ServiceNow ensures the SAP teams handling resolution receive timely assignments and the instructions they need to effectively mitigate the vulnerability. This has helped them reduce their remediation time from more than six months to less than one (less than a week for emergencies). Integrating Onapsis Defend with their existing IBM QRadar instance means their SOC teams receive immediate notifications of suspicious or malicious activity targeting their SAP applications, including insight into root cause and remediation recommendations. Bringing SAP security events into existing incident response workflows and the rich context included with each alert has significantly reduced forensic investigation time and resulted in seventy-five percent improvement in incident response times.

Learn more about **how Onapsis helps organizations protect their most critical systems: onapsis.com.**

