reco + EXELA PHARMA SCIENCES

Exela Leverages Reco to Reduce its Expanding Attack Surface Area and Manage Risk

Exela Pharma Sciences is an award-winning, fast-growing US-based integrated specialty pharmaceutical company, founded in 2005. It develops and manufactures proprietary and generic sterile injectable products to address the unique needs of healthcare providers, improve patient experience, and ease drug shortages.

Before Reco

Exela was growing rapidly. Acquiring new customers, expanding to new facilities, and increasing its product offerings was great for business, but it created challenges for the security team. They didn't have the people, processes, and tools to keep up with that growth. With highly confidential data spread across Veeva CRM and Veeva Vault, SAP, and Microsoft 365 (M365), Exela needed a way to manage and control risks across SaaS applications in order to keep the organization safe from damaging breaches.

Lack of Visibility

Exela initially relied on ingesting logs from Microsoft into its SIEM solution to gain visibility into its M365 email environment. However, the sheer volume of data, combined with limited resources and expertise, made it challenging to sift through the information and extract valuable insights. As a result, Exela soon abandoned this initiative.

Data Exposure

As Exela grew, more users and applications were added to its infrastructure to support expanding business operations. Without visibility into who was accessing what, what was being deployed, and what permissions existed, there was an increased risk of data getting into the wrong hands.

Adherence to Compliance Frameworks

As a pharma sciences company that manages highly sensitive information like medication formulas, patents, and dosage labels, Exela is regulated by the Food and Drug Administration (FDA). It maps to NIST CSF 2.0 and Center for Internet Security (CIS) Benchmarks controls v8 in order to appease the FDA regulators that pay Exela regular visits. Lacking visibility into its SaaS ecosystem, Exela was missing a crucial component needed to accurately report on its compliance status.

Step 1

Discovery

Exela deployed Reco and immediately began to see value. With visibility into Microsoft 365, Veeva, SAP and all connected applications, Exela realized its attack surface area was even greater than it was previously aware of. Stale accounts, overpermissioned roles, and passwords without expiration were among some of the risks that were uncovered. Additionally, what was thought to be under 100 applications was actually 268 applications connected to Exela's email domain.

Some key findings included:

- 218 shadow applications not configured with SSO
- 2 administrator accounts did not have MFA connected to M365 critical infrastructure
- 179 stale accounts across M365, Veeva, and SAP
- Over 100 guest accounts connected to M365 or Veeva had been stale
- 27 Veeva users had not accessed for 90 days, triggering an opportunity for licensing review

Step 2

Mitigation and Remediation

Once discovery was completed, Exela used intelligence provided by Reco to improve its security posture.

Data-Driven Roadmap

Thanks to Reco's vendor ranking score, which provides outside-in insight into the degree of risk associated with each application, Exela was able to align its remediation plans with activities that would have the most impact. Working closely with Customer Success, the Exela team began improving its security posture and implementing new posture checks that would reduce configuration drift in the future. Customer Success also helped with security awareness procedures to ensure new employees used security best practices.

Remediation

In partnership with Customer Success, and leveraging Reco's 'How to Fix' feature, Exela began remediation. As a result, it immediately strengthened its SaaS security posture. Some changes included:

- Enforced MFA for all administrators
- Set up SSO across the SaaS ecosystem
- Removed risky applications
- Removed guest accounts for stale identities
- Increased posture score by 13% in 30 days
- Built automation that requires all public files in M365 to be reviewed before they're made public
- Change passwords for users who share their corporate credentials in SaaS apps

> It's great to have good technology, but it's even better to have people behind the technology that are supportive and passionate about helping you accomplish your business goals. I can't say enough about the team at Reco and how they've supported us
>
> **Aaron Ansari**
>
> CISO at Exela

Step 3

Additional Support

One of the biggest benefits for the Exela team is how quickly Reco can provide support for additional applications through the Reco SaaS App Factory . Using a low-code/no-code development approach, Reco adds 3-5 applications per week to support customers' growing needs. As a result Exela was able to get support for FreshService, its ITSM solution, and integrate Reco alerts into its IT operations workflow.

Result

Exela has been able to more effectively manage risk as it grows while easing the stress that comes along with all the security question marks it previously dealt with.

Increased Efficacy of Security Awareness Training

The Exela security team was able to use the intelligence provided by Reco to increase its culture of security. For example, the Human Resources (HR) department often books travel for executives through Marriott.com. (It s important to note that Marriott has had several breaches in the last two years.) Using Reco, Exela discovered that many HR employees had been using the same login credential combinations for Marriott that they were using to access M365 and critical applications at Exela.

Empowered with this information, Exela was able to not only remediate these risks but also use this data to create teachable moments for HR employees. By understanding the potential business impact of their actions, nontechnical employees could become more security-conscious and better advocates for security in their department.

Reduced Risk of a Breach

Many of the misconfigurations Exela discovered through Reco were many years old, for example, a Veeva user was created three years prior and never decommissioned. As it turns out, the employee that was responsible for creating and decommissioning that user no longer worked at Exela, so the account ended up flying under the radar.

It was empowering for Exela to have observability into risks that had been piling up over the years so it could go back and clean things up. Deprovisioning SaaS, changing risky passwords for users, and retiring old accounts were among some of the remediation activities performed. As a result, Exela's security posture improved and now it can focus on remediating new risks quickly as they arise.

> Now that we use Reco we've reduced our attack surface area and we have the tools we need to deprovision SaaS and also change passwords for users who share their corporate credentials in SaaS applications.We have reduced both the stress and the risk that comes with our business growth because we have a handle on what's happening across our SaaS deployments and our technology users
>
> **Ansari**

> “
>
> We decided to invest in SaaS Security over other more traditional types of security because of the growth of SaaS that empowers our business to be able to operate the way that it does. It's just something that can't be ignored anymore or put off
>
> **Ansari**

Visibility and Observability

The Exela team uses app discovery and posture checks on a daily basis to keep a tight handle on its security posture and reduce shadow applications. By sending high and critical alerts through its SIEM to the security team, risks can be addressed immediately, reducing corporate exposure. Exela now has the visibility, control, and intelligence needed to protect the business from a SaaS perspective.

About Reco

Reco is the leader in Dynamic SaaS Security — the only approach that eliminates the SaaS Security Gap driven by SaaS Sprawl — the proliferation of apps, AI, and identities; the challenge of keeping their configurations secure amidst constant updates, and the challenge of finding threats hidden within an ever-growing number of events. Dynamic SaaS Security by Reco keeps pace with this sprawl, no matter how fast it evolves, by covering the entire SaaS lifecycle. It tracks all apps, SaaS-to-SaaS connections, Shadow SaaS, AI Agents, and Shadow AI tools, including their users and data, and adds support for new apps in days, not quarters. Reco maintains airtight posture and compliance — even as apps and AI Agents are added or updated. And it also ensures accounts remain secure, access privileges are minimized, and alerts are provided for critical threats. This comprehensive picture is generated continuously using the Reco Knowledge Graph and empowers security teams to take swift action to effectively prioritize their most critical points of risk. Reco uses a low-code/no-code approach to add a new SaaS integration in 3-5 days.

Learn more or book a demo