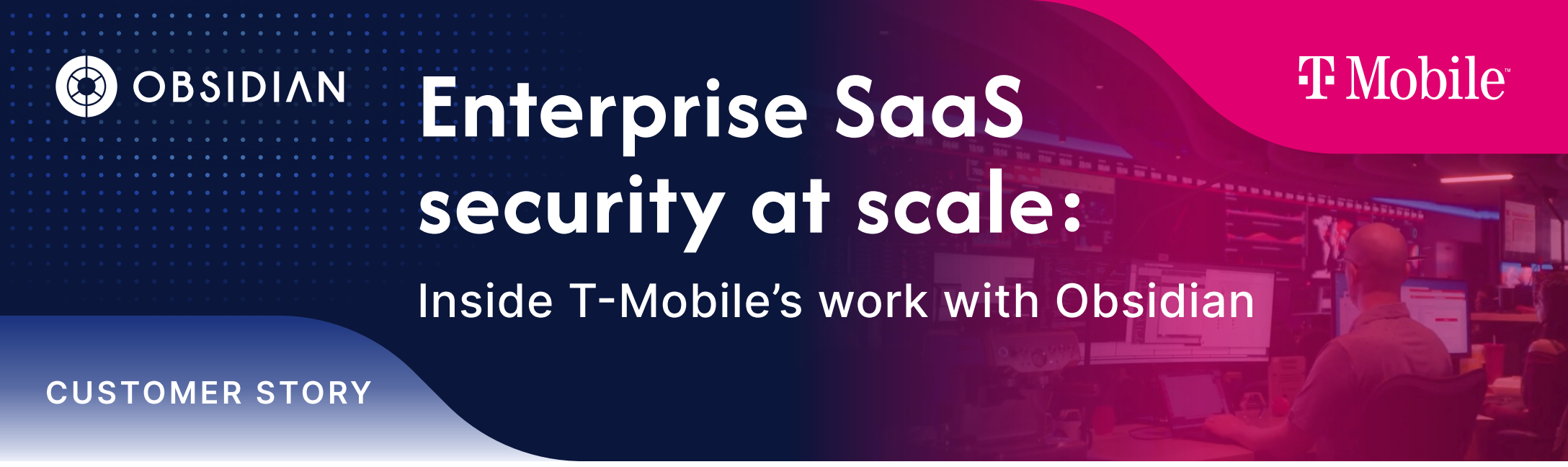
OBSIDIAN

T-Mobile

Enterprise SaaS security at scale:

Inside T-Mobile's work with Obsidian



CUSTOMER STORY

T-Mobile is dedicated to upholding the highest standards of cybersecurity and continually invests in its technologies, teams, and systems to better safeguard its environment against security risks.

The complexities of SaaS

T-Mobile has embraced SaaS to drive business and innovation, which means protecting the customer, employee, and workforce data that flows through those apps is critical. At T-Mobile's scale, SaaS spans many vendors, business units, workflows, and use cases. As SaaS adoption grows across teams, maintaining consistent visibility and control is essential.

In a complex environment with a large number of SaaS apps, T-Mobile set out to become more instance-aware and better manage SaaS configurations. Rather than layering multiple point solutions, T-Mobile prioritized a single, comprehensive platform capable of securing their broad SaaS ecosystem end-to-end and integrating seamlessly into their existing defense stack.

KEY STATS

100+

tenants monitored with centralized visibility.

100%

compliance with remediation SLAs for critical alerts

85%

reduction in manual SaaS security work on key CRM instances

> **Securing SaaS is a little different. It's not our infrastructure. We're relying on a partner's infrastructure and they have lots of complexity in the environment. We need to make sure we get the knobs and dials right, and there's many different platforms, which all have their particularities of how they're configured and operated."**

Mark Clancy
SVP, Cybersecurity

The Obsidian Security solution

Leveraging Obsidian's agentless, pre-built SaaS connectors, as well as strong collaboration with Obsidian support teams, T-Mobile onboarded Obsidian across their SaaS ecosystem and multiple business units in what was one of the fastest SaaS security deployments among large enterprises.

T-Mobile implemented Obsidian's posture management and alerting capabilities to help enforce security standards across its broad SaaS ecosystem and gain more visibility and real-time alerting. When T-Mobile reviews a connection, the cybersecurity team can quickly understand misconfigurations, the identities involved, and the potential risk. From there, T-Mobile connected Obsidian's actionability workflows to the company's existing IT and security stack to help drive rapid remediation at enterprise scale.

Beyond surfacing misconfigurations, T-Mobile leverages Obsidian to gather real-time insights into shifting risks across their SaaS landscape. As new risks emerge, Obsidian customer success teams proactively share relevant signals, allowing the team to validate exposure and respond quickly. T-Mobile uses this rapid signal-to-action loop to help maintain a proactive security posture that keeps pace with the speed of SaaS adoption.

> **"This is a very diverse environment and being able to use a single tool that gives us that visibility as well as the security controls is super important to us."**
>
> **Koveh Tavakkol**
> Senior Manager, Cybersecurity

Empowering a security-first culture

At T-Mobile, security is a shared responsibility, not just a challenge that security and IT teams are tasked with managing alone. Obsidian works with T-Mobile to provide app teams visibility and guidance, which strengthens their active role in keeping the company secure.

Through Obsidian's fine-grained role-based access control (RBAC), app owners have their own dashboards, offering visibility into app posture, best practices, and actionable steps to reduce risk.

> **"Our app owners were excited about Obsidian. The platform gives them visibility into their posture management and best practices. When you give your app owners that level of understanding, you can help foster the due diligence and accountability that's critical for security**
>
> **Alexandar Mihajlov**
> Senior Manager, Cybersecurity