EINPRESSWIRE

Palo Alto’s Salesforce Breach Points to a Bigger Problem

Centraleyes Launches Emerging Threat Response Playbook for Zero-Day and CRM-Driven Security Events

NEW YORK, NY, UNITED STATES, September 4, 2025 /EINPresswire.com/ -- Palo Alto Networks confirmed this week that it too was a victim in the ongoing wave of CRM-based breaches affecting major enterprises. The attacker gained access through a third-party AI integration between Salesforce and Drift, a chatbot built by Salesloft. Hackers, tracked as UNC6395, exploited stolen OAuth tokens granted to third-party applications like Drift to export sensitive business information, bypassing multi-factor authentication controls and leveraging deep organizational access.

Similar attack methods were reportedly used against Zscaler, Cloudflare, SpyCloud, and others, all targeting their Salesforce environments through embedded apps. And to be clear, these aren’t strictly Salesforce or CRM breaches. They are breaches of an ecosystem of third-party tools with deep organizational access but little to no scrutiny.

What’s striking isn’t just that an industry giant like Palo Alto was breached. It’s that it happened after Cloudflare, Zscaler, and others had already been hit using the same method. When the warning signs were already clear, why weren’t more companies ready to act? The inability to rapidly map internal and vendor-wide exposure highlights a deeper, systemic challenge: sprawling integrations leave organizations struggling to identify who’s at risk and where decisive action is needed.

When a zero-day threat emerges in SaaS environments, security teams must pivot urgently. The true bottleneck is not typically firewall or endpoint delays, but the slow, manual process of determining:

- Which business units and vendors use the compromised app

- What OAuth access was active at the time of breach

- Who needs to take action, and how quickly

In emerging threat situations, the stuffed-up bottleneck often isn’t a firewall or a forensic delay.

It’s organizational sprawl. It’s the time it takes to figure out who’s exposed, who needs to act, and what information is missing across multiple teams and third parties.

Centraleyes fills that critical early gap with automated ESE (Emerging Security Events) workflows that bring the entire ecosystem into focus. The platform allows you to mobilize dozens or hundreds of teams and vendors instantly, with structured, trackable outreach that gets you the answers you need.

Centraleyes Emerging Security Events to the Rescue

Centraleyes helps organizations close the gap between breach notification and coordinated response. The Emerging Security Events feature, available through the Centraleyes 3rd Party Risk module, enables security and risk teams to act within minutes of an emerging incident.
Using a guided wizard, teams can launch a targeted exposure assessment as soon as a threat becomes known. The platform sends automated, customized questionnaires to internal entities and third-party vendors. These notifications include clear action items and direct requests for relevant information.

______
The Salesforce integration breach reported today by Palo Alto was not the direct result of a platform vulnerability or missed alert. It happened because attackers took advantage of trusted access. Once an OAuth token is issued, most organizations lack the tools to monitor how that access is used across departments, subsidiaries, and vendors.

Centraleyes is an AI-powered GRC platform that places governance and risk management at the center of security. When a third-party threat emerges, Centraleyes enables teams to act quickly, engage the right people, and drive coordinated action across the enterprise. With breaches now targeting SaaS integrations at scale, rapid enterprise response is essential. Centraleyes offers security teams the automation, visibility, and agility required to navigate today’s interconnected risk landscape.

Jacob Zakay
Centraleyes
+1 212-655-3023
email us here
