When Even Security Vendors Get Hacked, **Who Can You Trust?**

LeapFrog®

When Even Security Vendors Get Hacked, Who Can You Trust?

In cybersecurity, trust used to be simple: if your vendors were secure, you were secure. But the recent breach involving the Salesloft Drift integration has shattered that illusion. This wasn't just a technical hiccup – it was a full-blown supply chain attack that compromised over 700 organizations, including elite security firms like Cloudflare, Zscaler, and Palo Alto Networks.

The Drift Breach: A Blueprint for Modern Supply Chain Attacks

The attack began with the theft of OAuth tokens from Drift, a chatbot service acquired by Salesloft. These tokens granted attackers trusted access to customer Salesforce environments, bypassing multi-factor authentication and traditional perimeter defenses. Once inside, the threat actor, tracked as UNC6395, executed bulk-sensitive data exports from Salesforce objects like Cases, Accounts, and Users.

According to Google Cloud's advisory, the attackers weren't only after contact info. They harvested AWS access keys, Snowflake tokens, and other credentials, positioning themselves to pivot deeper into victim environments. Cloudflare later confirmed that 104 internal API tokens were exposed through compromised support case notes – a stark reminder that identity is now the perimeter.

Even Security Vendors Aren't Immune

This breach didn't just hit startups or under-resourced teams. It infiltrated the CRM systems of Zscaler and Palo Alto Networks, exposing business contact details, licensing data, and internal case records. These are companies that build the very tools SMBs rely on to stay safe, and they were blindsided.

The implications are clear: the vendor trust model is broken. And with supply chain attacks surging 431% between 2021 and 2023, according to Axis Insurance, the risk is only growing.

What SMBs Must Do Now

If you are an SMB leader, this isn't a cautionary tale — it's a call to action. You can't afford to assume your vendors are secure. You need to:

- **Implement zero-trust beyond your perimeter:** Treat every integration, API, and token as potentially compromised.
- **Demand visibility from vendors:** Ask for audit trails, scoped permissions, and breach disclosure protocols.
- **Deploy third-party risk management:** Continuously assess vendor security posture and monitor supply chain activity.
- **Partner with an MSSP like Leapfrog Services:** We help SMBs enforce layered defenses, monitor integrations, and assume breach, so you are protected even when your vendors are not.

Executive Call to Action

Trust is no longer a given. It's a strategy.

Every organization must demand visibility from vendors and implement zero-trust beyond its own perimeter.

At Leapfrog, we have spent over 25 years helping SMBs leap ahead of threats, not just respond after the damage is done. Our layered security frameworks are designed to enforce zero-trust, monitor your supply chain, and manage third-party risk with precision and speed. If you're ready to take control of your vendor exposure and build defenses that assume breach, reach out today and ask about our Ring of Security CyberRisk Assessment. Let's turn trust into strategy — and move from awareness to action.

If you would like to learn more about the strides Leapfrog takes to offer our clients seamless and secure IT environments, reach out today. Please call 866-260-9478 or contact us at sales@leapfrogservices.com.