interfuture

BUSINESS **IT** SECURITY

Interfuture Security News

September has been an exciting month: we've had a new selection of content released, including vertical video guides, images that explain process and concepts, as well as news updates and LinkedIn carousels - check it all out via the links in the footer!

In this edition we go over what security teams monitor and go over one of the most significant data breaches in recent memory.

As always, any feedback or queries please contact us via our social media channels or on our website.

Key Point

Remember, you should only be using your work devices for work related things: we won't necessarily share what we see - unless it is illegal, poses a threat to the device or a threat in general - but we will judge you for enjoying a streaming binge on company time!

Also, this monitoring helps keep you compliant with the latest regulations regarding cyber security.

Monitoring Masters

At **Interfuture Security,** we are constantly keeping watch over our clients' devices, to spot threats and stop them before they cause issues. What do we monitor?

Web browsing history: we can see what URLs you visit, how much time you spend on certain websites and what sort of site you are visiting.

Installed plugins and extensions: we monitor browser extensions and software installations.

Application use: we can tell what apps are opened, for how long, and background processes.

File access and transfers: we know what files are opened, which have been edited, and which have been downloaded. If you plug in a USB device, we can tell, and we can also track any cloud storage interactions.

Email and messaging: we can look at company email content, metadata like timestamps and sender addresses and the use of unauthorised messaging apps.

Network traffic: we can look at IP addresses and domains that have been contacted, data volume transferred and VPN usage.

Login and access logs: we can see login times, locations, failed login and privilege escalation attempts.

In doing this, we to keep you protected. It may feel like it is spying, but it is much better than the alternative!

Taken Tokens Turmoil

In August of 2025, **Salesloft** – a company that provides tools to help sales teams manage relationships with their customers – had their **Drift** product targeted by a cyber attack, impacting all the companies using it, but particularly **Salesforce**.

Salesloft Drift is an AI powered chatbot that these companies had enabled on their websites to talk to visitors and help convert them into customers. Hackers managed to steal **OAuth** tokens (think of them like your personal keycards, but for getting into apps) from **Drift**, allowing them to access hundreds of companies' **Salesforce** data, and other connected services.

The cyber criminals, tracked as **UNC6395**, then logged in to **Salesforce** and other applications as if they were genuine users, running queries to extract data, searching for credentials to launch further attacks and deleting logs to avoid detection.

Salesforce and **Google** have much more robust security: instead, bad actors targeted **Drift,** as third-party integrations often have a lot of access to important data, but without the same security in place.

Customer support tickets, contact details, **AWS** access keys, VPN credentials and **Snowflake** database tokens were stolen by the attackers. Initially it was believed only **Salesforce** was impacted, but it is any platform connected to **Drift** (**Google Workspace, Slack, Amazon S3,** and **Microsoft Azure**).

Here are some of the companies that were impacted (over 700 in total):

- **Cloudflare** – data was accessed, including 104 API tokens
- **Zscaler** – contact info and support case content stolen
- **Palo Alto Networks** – internal case details leaked
- **SpyCloud, Tanium, PagerDuty – Salesforce** data compromised
- **Google** – some **Workspace** accounts accessed
- **Adidas, Allianz Life, Qantas** – victims of related social engineering attacks

In response, **Salesloft** have revoked all **Drift** tokens, removing **Drift** from **Salesforce's AppExchange** and **Salesforce** disabled all **Drift** integrations. **Cloudflare** rotated all credentials and launched incident response teams while **Google** is investigating the cause of the hack.

How's the re-view?

Interfuture Security is still yet to receive a review: why not leave one and you can be the first! It would mean the world to our hardworking team and you would have bragging rights over all of our other clients.

Please leave a review here!

★★★★★