AppOmni

Preventing SaaS Breaches

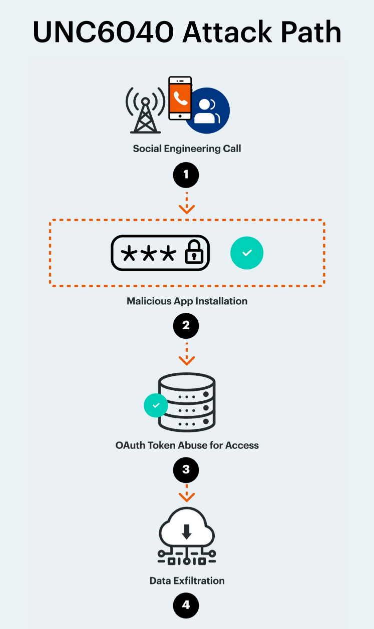
Identify, Detect, Protect, Respond

Groups like Scattered Spider, UNC6040, and UNC6395 are systematically exploiting SaaS weaknesses across every industry. On the surface, their attacks look similar; they are exploiting the SaaS supply chain and abusing OAuth connections to bypass traditional defenses.

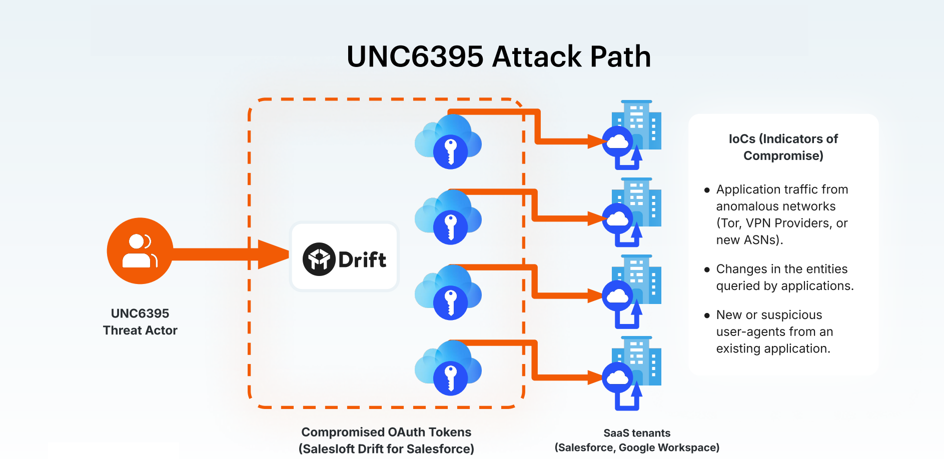
An effective defense can only be mounted by understanding the key nuances of each attacker's playbook. To stop these advanced threats, security teams must **Identify, Protect, Detect,** and **Respond** to SaaS threats across their entire ecosystem.

SaaS Attack Chain at a Glance

Modern attackers have been exploiting SaaS connected applications, permissions, and limited detections.



UNC6040 Attack Path



UNC6395 Attack Path

UNC6395 Threat Actor
Drift
Compromised OAuth Tokens (Salesloft Drift for Salesforce)
SaaS tenants (Salesforce, Google Workspace)

IoCs (Indicators of Compromise)

- Application traffic from anomalous networks (Tor, VPN Providers, or new ASNs).
- Changes in the entities queried by applications.
- New or suspicious user-agents from an existing application.

Recent Breaches

UNC6395

- Targets: 700+ organizations
- App(s) Impacted: Drift, Salesforce, Google, AWS, Snowflake
- When: Early-mid summer ’25
- How: OAuth abuse

UNC6040 (ShinyHunters)

- Targets: Big tech
- App(s) Impacted: Salesforce
- When: Early-mid summer ’25
- How: Vishing, OAuth token abuse, connection of malicious app

Scattered Spider

- Targets: Insurance, media, and transportation industries
- App(s) Impacted: CRMs
- When: Early-mid summer ’25
- How: Vishing, OAuth token abuse

The expertise to prevent breaches

Recent Breach TTPs	Capabilities Needed to Prevent	AppOmni
Initial Access Attackers use social engineering, compromise trusted third-party apps, and abuse OAuth tokens to gain initial access and bypass MFA.	**Identify** • SaaS shadow SaaS and shadow AI • Discover third-party connections	✓
Privilege Escalation & Lateral Movement They exploit SSO misconfigurations and overly permissive accounts to gain administrative rights and pivot to other connected apps.	**Prevent** • Misconfigs by continuously monitoring permissions and configs of apps and users • Data exposure, ensure secrets are stored correctly • Unauthorized connections via VPN, TOR, or IPs	✓
Exfiltration Attackers user anomalous behavior such as VPNs, TORs, or IPs from various locations to exfil sensitive data.	**Detect** • Anomalous behavior with User Entity Behavior Analytics (UEBA) such as: • High volume API requests • Anomalous user logins • OAuth activity from VPNs/TORs • Normalization of SaaS logs	✓
	Response • Stepped up authentication through Shared Signals with IdPs • Search normalized logs • SIEM/SOAR/ITSM integrations	✓

A complete framework to secure all of your SaaS Apps

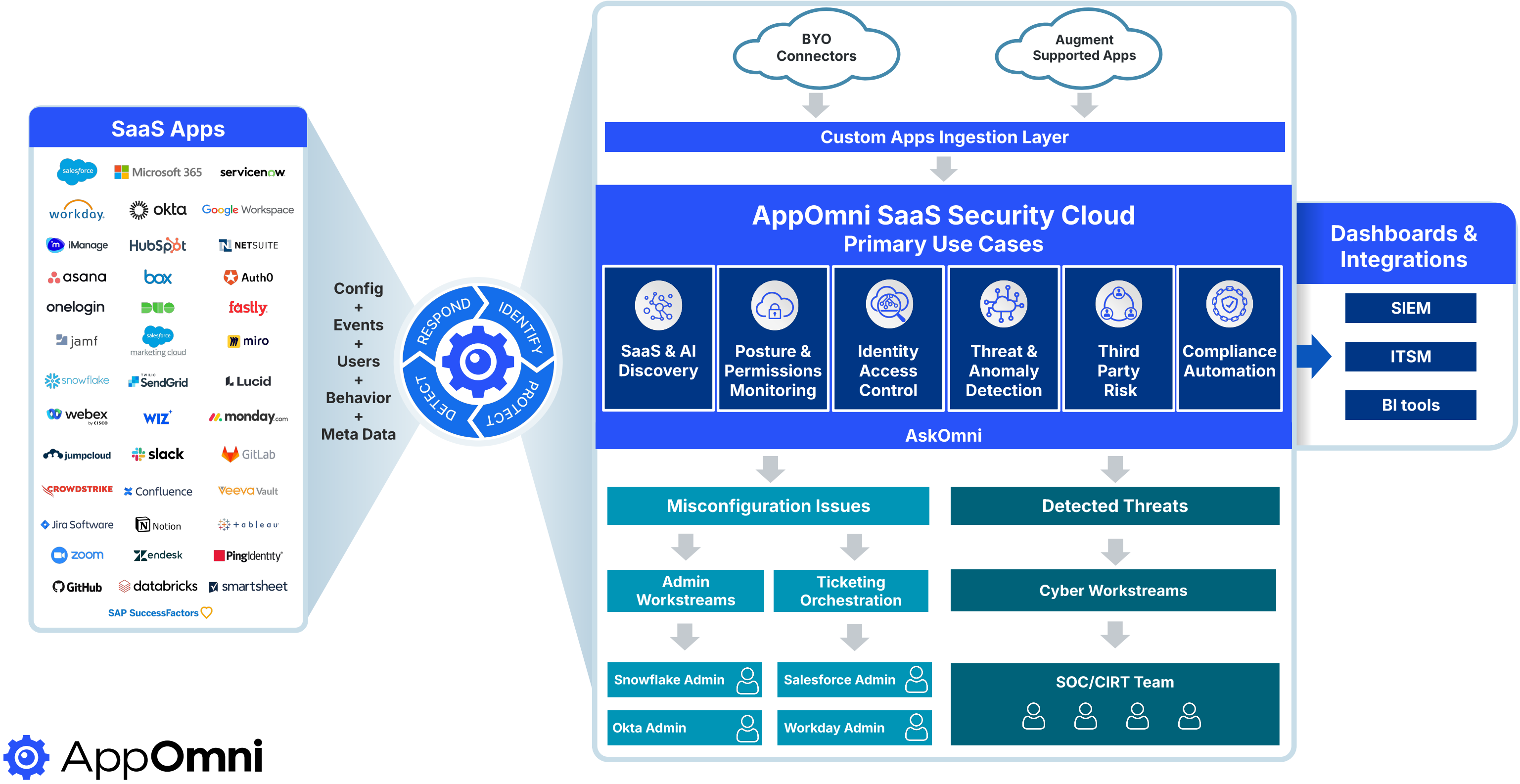
Identify
Shadow SaaS & AI

Protect
SaaS Apps

Detect
SaaS Threats

Respond
And Remediate Fast

The AppOmni Platform



AppOmni