SaaS Alerts
A Kaseya COMPANY

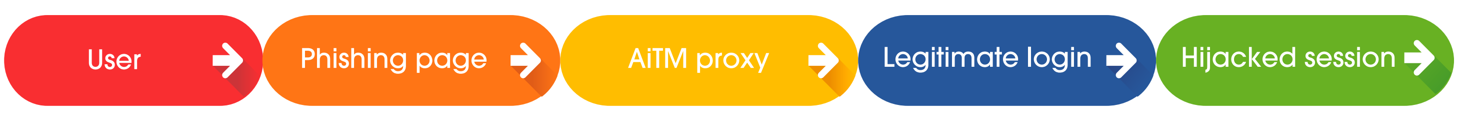
AiTM Attacks

How They Work and How to Stop Them

Adversary -in-the-Middle (AiTM) attacks have become a growing concern for businesses. They allow malicious actors to modify information, exfiltrate data and impersonate executives, even if multifactor authentication (MFA) is enabled.

What is an AiTM attack?

AiTM is a phishing tactic in which attackers insert themselves between a user and a legitimate service (like Microsoft 365 or Google Workspace). The attacker intercepts and potentially alters data in real-time, bypassing MFA and capturing session cookies to hijack accounts even after login.


User → Phishing page → AiTM proxy → Legitimate login → Hijacked session →

How attackers exploit trust with AiTM tactics

STEP 01

Targeted phishing email

The attacker lures a user with a deceptive email impersonating the Microsoft 365/Google Workspace login.

STEP 02

Proxy-based phishing page

A fake login page mimics the real one but sits behind a proxy controlled by the attacker.

STEP 03

Real-time MFA bypass

The proxy relays MFA credentials to the actual login page, giving the user the illusion of success.

STEP 04

Session cookie theft

The attacker captures session cookies that allow them to impersonate the user without needing credentials again.

STEP 05

Persistent access

Attackers now have ongoing access to SaaS applications — undetected.

Why IT professionals should be alarmed

Financial damage

Hijacked accounts can authorize fraudulent payments.

Data exfiltration

Sensitive client or employee data can be stolen.

Compliance violations

Unauthorized access leads to regulatory violations.

Lateral movement

Attackers pivot from SaaS apps into your broader IT stack.

Warning signs of an AiTM attack

- Multiple logins from new geolocations
- MFA prompts at odd hours
- Sudden permission escalations in SaaS apps
- Session timeouts without user input
- Credential phishing reports from employees

How SaaS Alerts stops AiTM

Session monitoring

Detect suspicious login patterns, abnormal file sharing and session hijacks.

Automated alerting

Get notified of credential reuse, anomalous IPs and MFA failures.

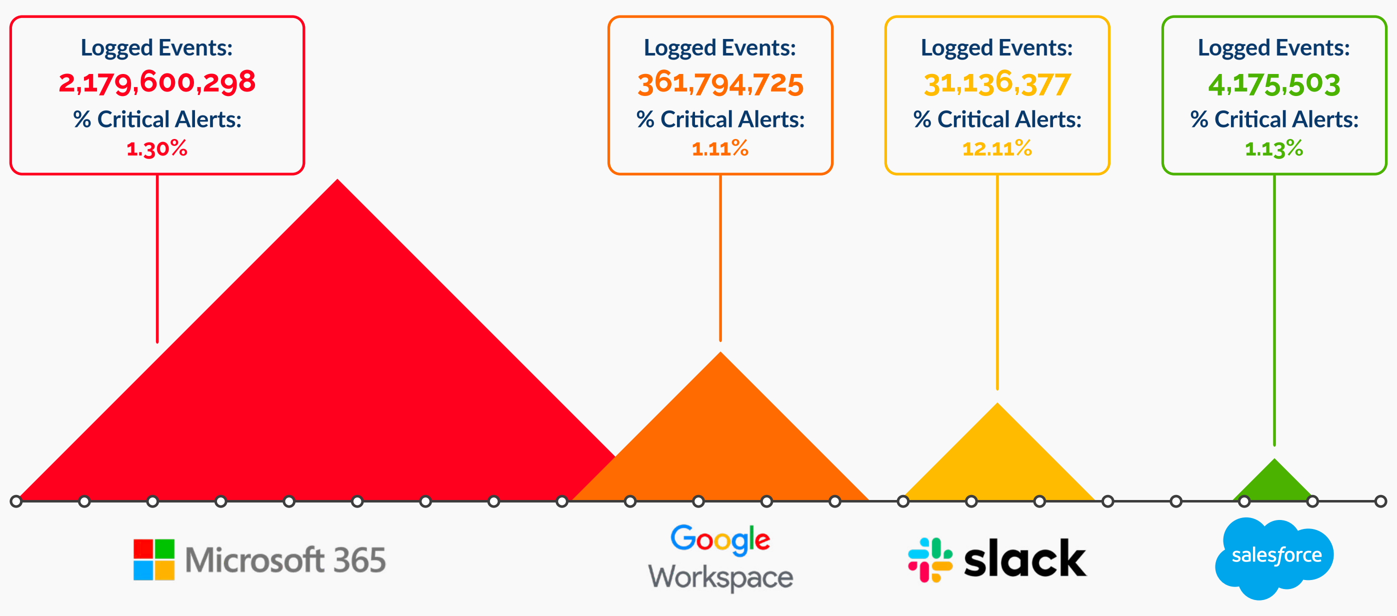
Audit-ready reports

Showcase rapid detection and response to demonstrate value and meet compliance requirements.

Auto-remediation

Kill active sessions and revoke access instantly.

Most commonly targeted SaaS apps



*The stats above are from the **2025 SASI Report**, based on a comprehensive analysis of SaaS security data from over 43,000 SMBs and nearly six million end-user accounts (including guest accounts), spanning from January 1 to December 31, 2024.*

Your SaaS environment deserves real-time protection

SaaS applications are vital to business operations. SaaS Alerts doesn't just monitor your most critical SaaS environments for abnormal behavior in real-time — it also responds. When threats are detected, our platform can **automatically trigger remediation actions**, like disabling compromised accounts and blocking new login attempts. This automation dramatically reduces response time, minimizes risk and helps IT teams maintain business continuity without manual intervention.

Book a demo

to discover how SaaS Alerts strengthens SaaS security, or

Start a free 14-day trial.

SaaS Alerts
A Kaseya COMPANY