DATA SHEET

proofpoint

PROOFPOINT SAAS PROTECTION

KEY BENEFITS

- The best threat protection for SaaS apps
- Integrated data protection, risk-based access control and analytics
- Third party applications control
- Vendor-neutral protection
- Automated policy-based response actions
- Award-winning customer support

Enterprises are embracing a wider range of software-as-a-service (SaaS) applications as part of a wider digital transformation. They need a new, integrated approach to preventing threats, safeguarding their information, and meeting compliance requirements.

Office 365, G Suite, Salesforce.com, Box, are just a few of the SaaS apps that have become a standard in the modern enterprise. The average enterprise sanctions 15 cloud apps—and a dizzying array of third-party add-ons that connect to them. Securing it all is more challenging, and critical, than ever.

Cyber attacks target people and the way they work. Much of that work unfolds over email. And now, more of it is expanding to SaaS apps. These apps contain sensitive data and often share it with connected add-ons. This shift presents new security and compliances challenges.

Proofpoint SaaS Protection helps you deploy SaaS apps with confidence. Get proven protection from advanced threats and risk-aware data protection for SaaS applications. Our integrated approach even covers third party add-ons. With powerful analytics, you can can limit user access or alert your security team based on ever-changing risks.

INDUSTRY-PROVEN ADVANCED THREAT PROTECTION

We offer the industry's timeliest, most accurate threat intelligence. It's also the industry's broadest range of threat data, spanning email, mobile apps, social media, network, and SaaS apps. This insight connects the dots between activity and behavior across all the tools your people use.

Cross-communication channel risk insights

Attacks that start with email can easily cross over into SaaS-powered collaboration apps that let users share, download and upload sensitive data. That makes connected insights across these vectors critical. If someone in your environment has been exposed to phishing or malware, for instance, we can step up authentication safeguards in SaaS apps based on that user's risk.

Detecting malware and non-malware based threats

Prevent threats from infiltrating your content within SaaS apps (such an uploaded Word file with a URL link to credential phishing site). With predictive and real-time sandboxing, static code analysis, and threat insights, we quickly detect and mitigate threats. We detect known threats, threats that use advanced malware, and even threats that don't use malware at all.

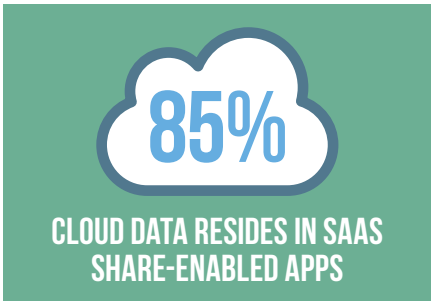
THIRD PARTY ADD-ON CONTROLS

Users who grant permission for third-party apps to connect into your SaaS applications may unknowingly expose your organization to security and compliance risks. We give you the visibility and controls to decide whether you want to allow user-installed applications—and which ones to ban.

INTEGRATED DATA PROTECTION, VISIBILITY AND RESPONSE

Data protection

Protect your data in SaaS apps and meet compliance requirements with built-in classification templates such as PCI, PII, PHI and more. You can also create your own templates. Either way, you define the rules. Based on your policies, you can encrypt, quarantine, or leverage data context controls. These steps can lessen the risk of overly broad permissions, workers who share sensitive data into private accounts, mass data exports, and more.



Automated response informed by risk-based access control and analytics

Your people access data from many locations, networks, devices, and clients. Users may have standard end-user or administrative privileges. They may be exposed to a threat in the moment through a specific attack channel. Whatever the context, each of these elements informs analytics on user behavior to establish a session risk score.

You can use our robust templates and policy set for risk-based authentication to prevent unauthorized or risky access. This includes alerts, set-up authentication, privilege reduction and more. You can also integrate your existing identity-management solution to respond to the session-risk score.

Usage analytics identifies anomalous behaviors

Usage analytics identifies risky behavior to prevent exposure, deletion, or other unwanted actions on your data.

SaaS app discovery

Detect unknown SaaS applications being used in your environment by analyzing information from firewalls and proxies.

COMPLETE TRANSPARENCY

We apply the same level of scrutiny and protection across the vast range of SaaS apps you use. We help protect Office 365, G Suite, Salesforce, and more. You get the same vendor-neutral deep assessment for third-party add-ons. If something appears risky, you can expect total transparency, fast and objective identification, and effective response.

LEARN MORE

Embrace SaaS applications with confidence with SaaS Protection. Backed by our award-winning global support organization, half of the Fortune 100 rely on us to protect their people, data, and brand. Contact a Proofpoint representative for a free threat assessment or to learn more.