# SAAS SECURITY SOLUTION CHECKLIST

**SaaS applications have provided tremendous value to end users due to their easy setup and collaboration capabilities.** However, because the typical SaaS environment is invisible to network administrators, enterprise security tools designed to protect internal data centers, servers and workstations can't effectively protect SaaS applications or prevent data leakage. Securing SaaS applications largely includes classifying different groupings of applications in order to understand what they are doing and how to control them, as well as setting zones of trust to control access. The goal for your SaaS security implementation should be to end up with a set of well-defined and enforced application and usage policies for sanctioned, tolerated and unsanctioned SaaS applications and to protect the data they house.

The grouping of applications is based on how much trust the organization has in each application and how it is treated based on the different levels of trust:

**Sanctioned** – These apps provide IT teams the confidence to sanction and allow majority access based on the security measures the vendors take. They are likely SOC 2 compliant and commonly use encryption and/or single sign-on.

**Tolerated** – These are apps that an organization doesn't necessarily trust at the same level as sanctioned apps but has to let people use, either because a partner or vendor is using that app or they are in the process of migrating out of that app to a sanctioned one.

**Unsanctioned** – These apps are potentially dangerous and known to expose organizations to data theft and malware risks. An organization doesn't want people using them, doesn't trust individuals to use them, and often there isn't a legitimate business purpose for using them.

# INFO & INSIGHTS

Some of the challenges in securing SaaS applications include: handling end users who sign up for cloud applications without the approval or governance of IT departments, monitoring and/or blocking the use of unsanctioned applications, and a lack of visibility into data residing in the cloud.

This checklist provides a breakdown of the most essential criteria that should be a part of your SaaS security solution. Implementing a solution that offers these features will provide greater control, visibility, policy management and enforcement of your applications and protect your organization from data exposure:

- ☑ Complete visibility across all user, folder and file activity – providing detailed analysis that helps you transition from a position of speculation to one of knowing exactly what's happening at any given point in time.
- ☑ Identify which applications are being used in order to create policies that can specify the application, regardless of port and encryption.
- ☑ Retroactive analysis of data exposure that doesn't just look at data in-line but also from the creation of the SaaS account itself, no matter how long ago that was.
- ☑ Deep analytics into day-to-day usage that allow you to quickly determine if there are any data risks or compliance-related policy violations.
- ☑ Granular, context-aware policy control that provides you with the ability to drive enforcement and the quarantine of users and data as soon as the violation occurs.
- ☑ Advanced threat protection to block known malware and identify and block unknown malware.
- ☑ Real-time threat intelligence on known and unknown threats to prevent new SaaS-based insertion points for malware "in the wild."
- ☑ Deploy solutions and provide functionality without affecting user experience or causing performance degradation.

In using these criteria when searching for your next SaaS security solution, you will be able to choose a platform that provides the most comprehensive and robust protection for your organization. Securing your SaaS applications – and ultimately your organization's data – requires a complete end-to-end platform that includes industry-leading next-generation firewalls for your network, a cloud security service to protect your SaaS applications, and advanced threat intelligence to protect against known and unknown threats. To learn more about SaaS security and how to choose the right platform for you, read the Choose the Right Platform for Securing SaaS white paper and the Securing SaaS For Dummies book.