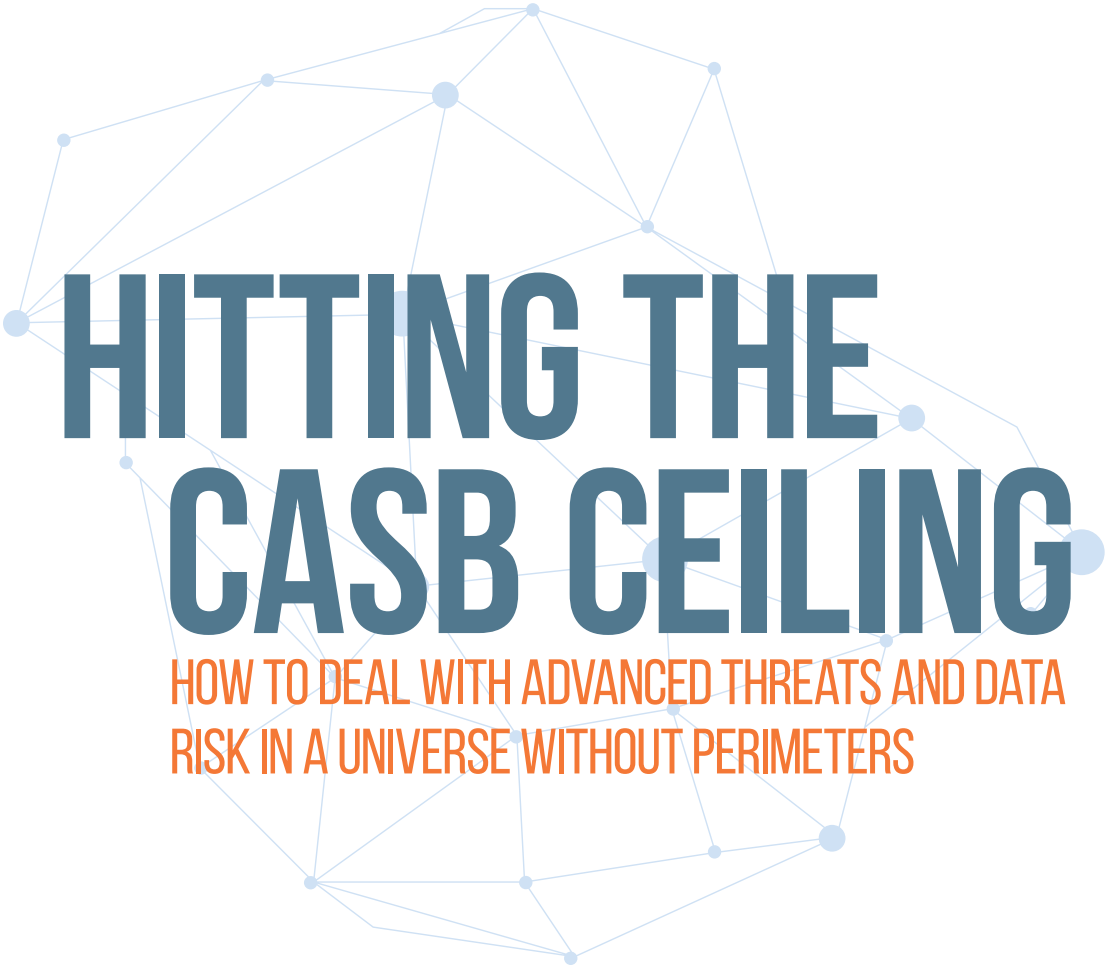
WHITE PAPER

proofpoint.



HITTING THE CASB CEILING

HOW TO DEAL WITH ADVANCED THREATS AND DATA RISK IN A UNIVERSE WITHOUT PERIMETERS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In the early stages of every technology lifecycle, user adoption peaks ahead of security concerns, creating a window of exposure. It's where risk—and opportunity for bad actors—are at their highest. Such is the case with SaaS and cloud technologies.

Cloud- and SaaS-based threats are growing more frequent and advanced. Bad actors are realizing just how easy it is to get users to compromise their sensitive information and accounts. The recent Google Docs phishing attack[1] and OneLogin data breach[2] are just two recent examples. Such attacks are growing not only more common, but more sophisticated and disruptive.

Conventional network-focused security and compliance tools weren't built for modern infrastructure such as the cloud, SaaS, and new digital channels. And they don't help organizations prevent or detect these risks—or respond effectively when they occur.

WHERE CASBS FALL SHORT

Cloud access security brokers (CASBs) arose several years ago to help organizations find "shadow IT" cloud services being used in their environment. Basic cloud compliance and security features came later.

But with limited security features and little focus on advanced threat protection or data loss prevention (DLP), CASBs aren't enough for the next wave of threats.

Some CASBs support leading SaaS apps such as Office 365 and G Suite. But few, if any, detect email threats that compromise other vectors. This is a critical gap; Exchange Online or Gmail is the primary SaaS workload, followed closely by file sharing.

Consider a seemingly benign email that asks you to reset your Outlook web app (OWA) password, log in to your Google account to view a shared document, open Salesforce to see new sales opportunities.

These are everyday email requests, a normal part of doing business. But they're also common forms of credential phishing. And in countless breaches, they've proven highly effective at compromising the data in your SaaS apps. Credential phishing by email is how 91% of all cyber attacks start.[3]

CASBs lack email threat detection and coordination. That means every attack has a greater chance of reaching valuable cloud applications and resources. Because they can't recognize account compromise at the point of attack (in most cases, email), they can't anticipate compromised SaaS accounts. All too often, that gap results in data loss and damage across every SaaS application a company uses—email, collaborative or otherwise.

[1] Adi Robertson (The Verge). "Google Docs users hit with sophisticated phishing attack." May 2017.
[2] Brian Krebs (Krebs on Security). "OneLogin: Breach Exposed Ability to Decrypt Data." June 2017.
[3] Steve Zurier (Dark Reading). "91% of Cyberattacks Start with a Phishing Email." December 2016.

HOW TO SECURE YOUR SAAS INFRASTRUCTURE

To protect your SaaS apps, the people who use them, and the data they contain, you need security beyond what CASBs can provide. An effective SaaS security solution must:

- Connect the dots across the digital channels you use for early warning signs
- Protect users and data from advanced threats that spread through SaaS apps
- Contain threats and minimize critical data loss with integrated threat insights
- Control the risk of third-party apps and ecosystems
- Prioritize risk with user behavior analytics
- Protect data from risky logins with real-time access controls
- Deploy and adapt quickly through a flexible architecture

Proofpoint SaaS Protection secures data in your SaaS apps to protect the way your people work. We combine threat detection, data-loss prevention (DLP), third-party app control, access control, and analytics to help you safeguard Microsoft Office 365, Google's G Suite, and more.

To learn more, visit www.proofpoint.com/us/products/saas-protection.

INTRODUCTION: DIGITAL TRANSFORMATION GOES MAINSTREAM

Today's digital transformation is changing the way we do business. Organizations are moving to the cloud, software-as-a-service (SaaS) platforms, and new digital channels to become more efficient, agile, and responsive to customers.

Your people collaborate with one another across devices and borders through cloud-based infrastructure you don't actively manage. And your business processes run on SaaS platforms you don't own.

Within this changing infrastructure model, effective collaboration and business processes rely on new kinds of connections that people need to trust implicitly.

In the early stages of every technology lifecycle, user adoption peaks ahead of security concerns, creating a window of exposure. It's where risk—and opportunity for bad actors—are at their highest.

SaaS and cloud technologies are no different.

DISRUPTING THE TRANSFORMATION

These new infrastructure models are solidly mainstream. Office 365 alone has an estimated 100 million active users Office 365[4], and countless other SaaS apps are a big part of today's workplaces.

Unfortunately, cloud- and SaaS-based threats are also becoming routine. Attacks on SaaS services and corporate SaaS users growing more frequent and advanced. Bad actors are realizing just how easy it is to get users to compromise their sensitive information and accounts. The recent Google Docs phishing attack[5] and OneLogin data breach[6] are just two recent examples. Such attacks are growing not only more common, but more sophisticated and disruptive.

Conventional network-focused security and compliance tools weren't built for modern infrastructure such as the cloud, SaaS, and new digital channels. And they don't help organizations prevent or detect these risks—or respond effectively when they occur.

[4] Trefis. Team (Forbes). "In Microsoft Earnings Performance, Growth In Cloud Boosts Revenue Once Again." January 2017.
[5] Adi Robertson (The Verge). "Google Docs users hit with sophisticated phishing attack." May 2017.
[6] Brian Krebs (Krebs on Security). "OneLogin: Breach Exposed Ability to Decrypt Data." June 2017.

THE RISE OF CASBS

In an attempt to protect assets in this new landscape, cloud access security brokers (CASBs) arose several years ago. Initially, they focused on "first-wave" issues such as revealing "shadow IT," cloud services being used without the formal endorsement of the IT department. CASBs later added basic cloud compliance and security capabilities.

But with limited security features and little focus on advanced threat protection or data loss prevention (DLP), CASBs aren't enough for the next wave of threats.

No regulated firm—or any firm exposed to any significant risk, for that matter—can afford to ignore cloud-based threats. That's because bad actors are opportunistic. They will compromise the weakest link in your security chain, finding the easiest route to their objectives.

Effective SaaS security solutions protect you by monitoring for threats and unauthorized access from all major entry points. At the same time, they reveal where your most sensitive data is located and who has access to it. Together, these capabilities can help you detect compromised accounts early, respond faster, contain the damage from breaches.

This guide explains the limitations of CASBs for security and how to build a security solution built for new risks and today's complex IT infrastructure.

CASB'S MAJOR BLIND SPOT

Some CASBs tout their support for leading SaaS apps such as Office 365 and G Suite. But few, if any, detect email threats that compromise other vectors. This is a critical gap; Exchange Online or Gmail is the primary SaaS workload, followed closely by file sharing.

Consider the following email requests:

- Reset your Outlook web app (OWA) password
- Log in to your Google or Box account to view a document your colleague shared
- Log in to Salesforce to see the new sales opportunities

These are everyday email requests, a normal part of doing business. It's easy to see why this kind of email credential phishing is so effective at compromising the data in your SaaS apps. In fact, credential phishing by email is how 91% of all cyber attacks start.[7]

That is why coordinated awareness of email attacks is a dependable early warning to a broader campaign. Cross-vector visibility predicts compromise more reliably than techniques such as user behavior analytics in nearly every case.

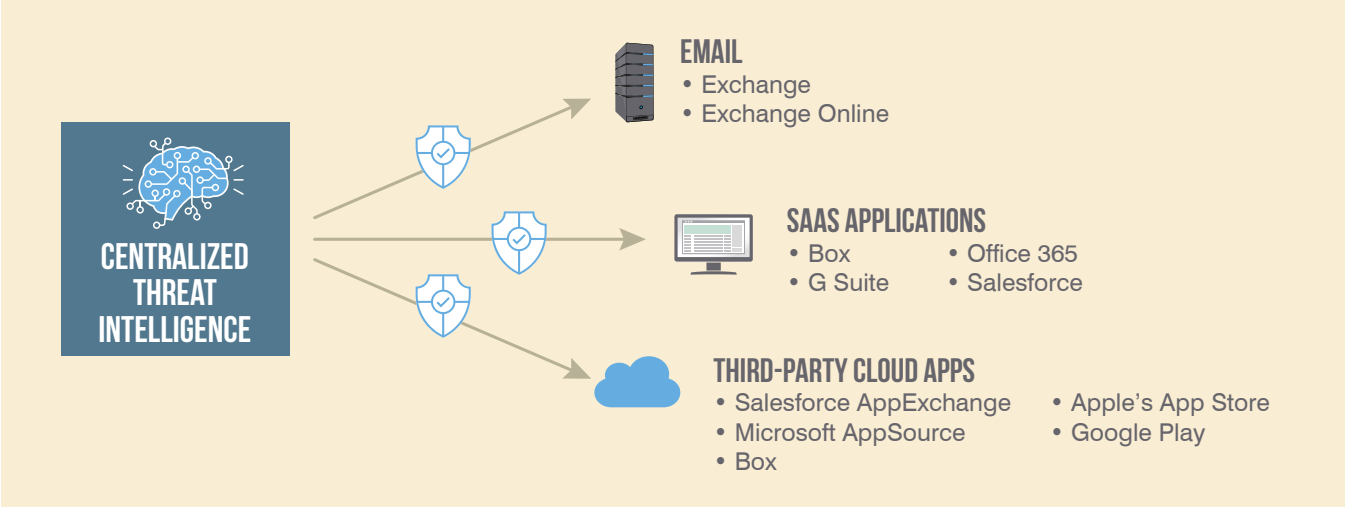
Unfortunately, CASBs lack email threat detection and coordination. That means every attack has a greater chance of reaching valuable cloud applications and resources. Because they can't recognize account compromise at the point of attack (in most cases, email), they can't anticipate compromised SaaS accounts. All too often that gap results in data loss and damage across every SaaS application a company uses—email, collaborative, or otherwise.

[7] Steve Zurier (Dark Reading). "91% of Cyberattacks Start with a Phishing Email." December 2016.

HOW TO PROTECT YOUR SAAS APPS

To protect your SaaS apps, the people who use them, and the data they contain, you need security beyond what CASBs can provide. An effective SaaS security solution must:

- Connect the dots across the digital channels you use for early warning signs
- Protect users and data from advanced threats that spread through SaaS apps
- Contain threats and minimize critical data loss with integrated threat insights
- Control the risk of third-party apps and ecosystems
- Prioritize risk with user behavior analytics
- Protect data from risky logins with real-time access controls
- Deploy and adapt quickly through a flexible architecture



CONNECTING THE DOTS FOR EARLY WARNING

Responding quickly to threats is critical to containing the damage they can do. The sooner a threat is detected, the less harm it does, the less likely it will spread, and the less expensive it is to resolve.

Many advanced threat technologies can improve your response time and ability to prevent threats from reaching their targets. But the fastest and most efficient way to deploy these measures is to put them where the threats are. In most cases, that's email, whether attackers are targeting traditional infrastructure, SaaS apps, or hybrid environments.

Effective SaaS protection cannot be siloed. Instead, it must integrate with a proven and dedicated threat platform that identifies and eliminates threats at the email gateway—before they have a chance to penetrate your organization or SaaS resources.

Your solution should identify external threats from multiple vectors in a cross-channel fashion. For example, if malicious URLs or malware are detected in files within a SaaS repository, the solution should be able to identify and remove them. This capability makes you more aware of threats and more prepared to stop them.

PROTECT USERS AND DATA FROM ADVANCED THREATS THAT SPREAD THROUGH SAAS APPS

The more users collaborate via SaaS apps, the more these apps become an effective vector of attack. And compromised accounts aren't your only worry. Consider the following scenarios:

- A malicious document on OneDrive spreads to all your employees through enterprise file sync and share (EFSS)
- A supposed "customer" sends a malicious attachment into your support portal to social engineer your support personnel to click

Today's threats emerge and spread too quickly to rely on reputation-based protection. Malware can be modified and disguised to avoid signature based protection. Malicious URLs and files may be too new to easily flag as malicious. Recent global attacks highlight the inherent weakness of conventional security.

To protect from modern attacks, look for multiple layered technologies that go beyond reputation-based solutions to protect, detect, and resolve advanced threats. These include proactive sandboxing, predictive defense, dynamic threat analysis, and deep threat intelligence.

MINIMIZE CRITICAL DATA LOSS WITH INTEGRATED THREAT INSIGHTS

At minimum, a SaaS protection solution should classify sensitive data for data loss prevention (DLP). It should know where sensitive data is located. And it should identify the type of data (such as PCI, PII, PHI, GDPR) to help you understand your risks.

An ideal solution combines data protection insight and threat insight. If something gets through, for example, your email solution should be able to alert a SaaS protection tools of potentially compromised accounts. An effective SaaS protection solution knows which employees received and activated a weaponized email. And it can tell you which user accounts are most likely compromised.

Your solution should also draw upon its combined knowledge of threats and sensitive data. That means recognizing which accounts have access to which data. And it should provide insight into which resources, applications, and content are most at risk. With this information, security teams can quickly prioritize which accounts need attention to minimize sensitive data loss and contain any damage.

ANATOMY OF A SAAS ATTACK: GOOGLE DOCS PHISHING CAMPAIGN

A phishing attack in early May 2017 started with an email that tricked Gmail users into giving a malicious third-party app access to their Google accounts (both email addresses and contacts).[8]

It leveraged OAuth, an open and widely used authentication standard for third-party services. OAuth is designed to let apps access users' accounts without the users having to provide their login details—a seemingly secure way of connecting different apps and services together.

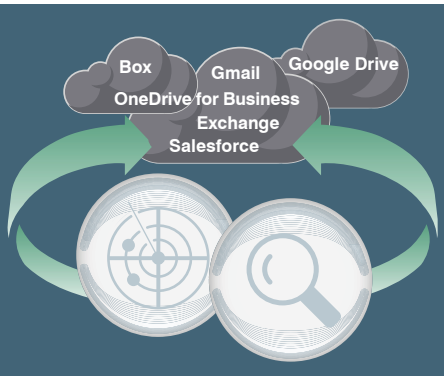
The Google attack was different from a traditional phishing scheme. Rather than asking for users' credentials directly, it gained access through a legitimate Google service in a typical fashion, giving users a false sense of security.

The damage was limited. It gathered emails and contacts and then spread itself like a classic worm. While it did delete a few emails for some users, the attack could have been much, much worse

An effective solution would have stopped the malicious app from enabling risky permissions and provided enriched insight condemning the original phishing email. Subsequent deliveries would be marked as malicious, blocking further attempts and notifying administrators of the attempt.

[8] Adi Roberston (The Verge). "Google Docs users hit with sophisticated phishing attack." May 2017.

COUPLING CROSS-CHANNEL THREAT DETECTION WITH SENSITIVE DATA VISUALIZATION AND DLP INSIGHT IS A CRITICAL CAPABILITY AND CHANGES THE GAME IN TERMS OF SAAS THREAT RESPONSE.



CONTROL THE RISK OF THIRD-PARTY APPS AND ECOSYSTEMS

Third-party cloud apps are mushrooming.[9] Demand for new apps continues to increase. And the sheer variety of cloud-based platforms and ecosystems has made third-party access difficult to control.

Google's Play, Apple's App Store, and Salesforce's AppExchange are all vendor-sponsored app platforms. And for the most part, they're filled with legitimate apps. But while these apps are implicitly blessed as part of the vendor's broader ecosystem, and thus perceived as safe, vetting can be erratic or skin-deep. Many third-party apps are major, well-built solutions. Many more are well-intended but poorly built, making them risky. And some are overtly malicious.

At the same time, rogue, non-sanctioned app stores often carry weaponized apps that expose your sensitive corporate data.

As shown by the spread of the Google Docs phishing attack, app stores have few checks or security controls to keep third-party apps from accidentally or maliciously accessing sensitive corporate data.

As a baseline, you should know what third-party apps your users have installed and what permissions were granted. And understanding the behavior of every third-party app is critical. You should know what these apps are doing with the data your users grant them access to.

Permissions and access should always be appropriate and proportional. Allowing LinkedIn, a legitimate business app, to access your corporate Gmail contacts to help spot business connections might be OK. But giving an unknown, third-party "print driver" app access to the same contact list and copying the entire list to its database is not. A printing app doesn't need your entire contact list to function. Granting that permission would more likely enable a phishing or malware attack than print your document.

With limited IT staff, organizations are also looking for ways to manage third-party app access into their corporate SaaS infrastructure in a way that's sustainable. On its own, maintaining a whitelist of approved third-party apps is tedious and doesn't scale. With thousands of apps available now (and counting), you need a solution that uses risk scoring with blacklisting and whitelisting to manage the risk of third-party apps at scale.

A final consideration relates to Microsoft. Along with its own native applications, an app store, and ecosystem, Microsoft also has a CASB. The problem: many of its native apps compete with third-party apps. For that reason alone, you should closely examine Microsoft's CASB support of third-party apps—especially for thoroughness and longevity. An ideal SaaS protection solution supports all industry SaaS applications equally without conflict. If you rely on third-party SaaS applications for critical aspects of your business, consider a vendor-neutral solution.

[9] Mobile Developer Population Reaches 12M Worldwide, Expected to Top 14M by 2020, Oct 5, 2016, Evans Data Corp

PRIORITIZE RISK WITH USER BEHAVIOR ANALYTICS

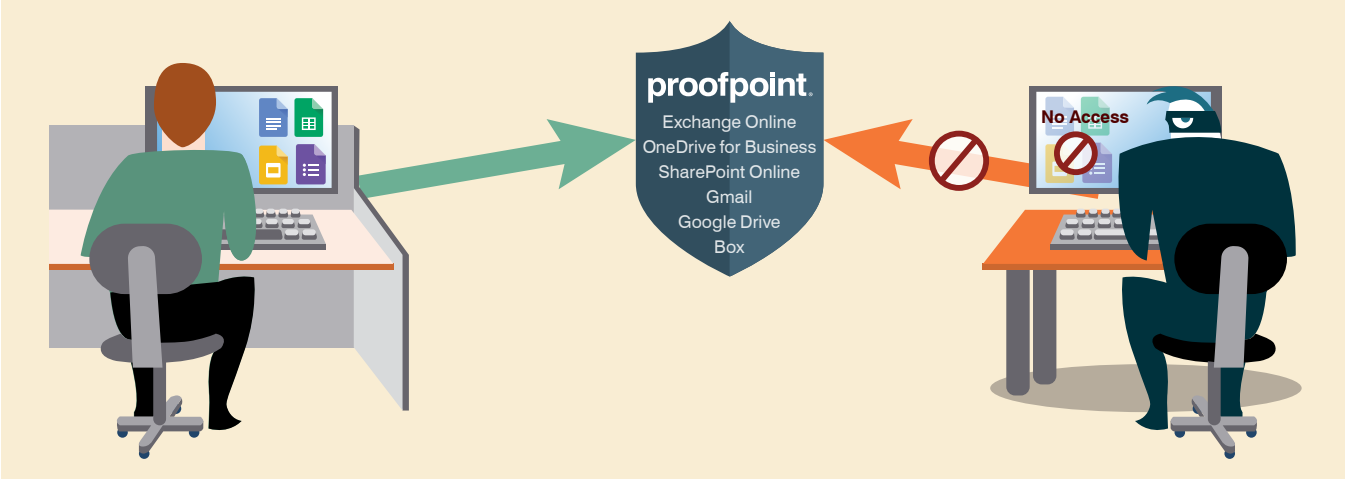
Beyond detecting threats, user behavior analytics (UBA) provides added insight into which accounts may be most at risk. In the event of a suspected breach or breach, UBA flags unusual account activity to help spot potential compromises and prioritize which accounts response teams should examine first.

No security tool can prevent every attack. Eventually, a threat will penetrate your organization. But with the right preparation, a successful attack doesn't have to result in widespread damage. At a minimum, administrators should monitor user behaviors across SaaS applications and use that information to establish safe, baseline behaviors. And they should always look for potentially malicious patterns.

SaaS protection solutions assess a variety of parameters about each user every time they log on: time of day, location, device, and so on. By comparing the dimensions of historic, legitimate sessions against a new unknown session, differences may be detected and scored for risk.

If a successful attack targets a user account through the user's email or SaaS account, then the added context from UBA (signs of anomalous behavior) can prioritize the account for follow up. The combination of condemnation and context is powerful. It helps prioritize alerts and alleviates alert fatigue experienced by so many response teams.

Using UBA to rank which accounts need immediate attention—among hundreds or thousands of potentially compromised users—is an excellent way to help response teams triangulate threats and focus attention efficiently and in a way that accounts for their true risk.



PROTECT DATA FROM RISKY LOGINS WITH REAL-TIME ACCESS CONTROLS

Contextual access based on user, location, device, network, app and more can help security teams spot suspicious activity. An effective solution reveals suspicious login events and, based on the risk factors, can enable the right level of access to sensitive data.

Real-time access controls are an effective way to prevent the impact of stolen credentials or third-party apps that use authorization as a backdoor to your data. Consider integrating capabilities if you have an existing identity-as-a-service (IDaaS) tool. If not, consider deploying two-factor authentication (2FA).

You can also use a risk-score to gauge a session's trust level and enforce which apps it can access and with which privileges (read, write, download). Look for flexibility that allows you to use an adaptive engine or take a policy-based approach.

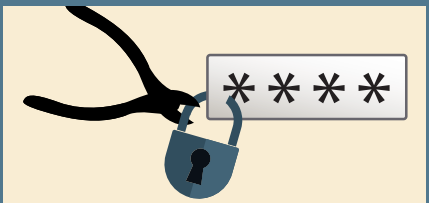
DELIVER PROTECTION WITH A FLEXIBLE ARCHITECTURE

SaaS protection tools use different modes of deployment. The best solutions are flexible, supporting whichever architecture is necessary to meet a customer's needs. The ideal solution may integrate to the SaaS application through APIs to track user activity; perform data discovery, analysis, and extraction; or leverage the growing array of API-based functions.

You may also need support for a forward-proxy architecture that provides sensitive data loss prevention or governs which apps are available. Or you may need reverse-proxy support to govern and manage sanctioned cloud resources (and prevent rogue entities from accessing your cloud services) with context to that access.

Focus on solutions that can provide the greatest flexibility. That way, you can meet future needs without disrupting operations or making new big-ticket purchases.

ANATOMY OF A SAAS ATTACK: GOOGLE DOCS PHISHING CAMPAIGN



A June 2017 attack on OneLogin was a serious breach that targeted SaaS infrastructure and exposed customer data.[10] The attack was particularly egregious for customers relying upon OneLogin for storing and supplying all usernames and passwords across a company's various applications.

While details are scarce, we know that a threat actor accessed Amazon Web Services API keys through a secondary service provider. The attacker then used those keys to penetrate and explore OneLogin's infrastructure for seven hours before being shut down.

During this time, the actor accessed database tables containing user and app information and encryption keys. With that information, the attacker could then decrypt customer data.

Experts are still piecing together what happened in the OneLogin attack. But credential compromise at the secondary service provider was the critical factor. Chances are, that provider was compromised through email, the source of most cyber attacks.

With the proper cross-channel threat solution in place, any phishing email would be blocked at the gateway, ending the threat there. And a cross-platform solution that shared breach insight among email and SaaS tools would immediately update the risk factor of all assets for the compromised account—cloud or otherwise. It would also trigger a proportional response to the threat. That might include shutting down access to any asset of the account and identifying exposed sensitive data right away.

[10] Brian Krebs (Krebs on Security). "OneLogin: Breach Exposed Ability to Decrypt Data." June 2017.

CONCLUSION AND RECOMMENDATIONS

Advanced threats, data protection, and third-party apps are top concerns preventing organizations from protecting SaaS apps with confidence. Here's a checklist of capabilities to look for and questions to ask potential vendors.

Implement cross-channel insight for early warning signs

Rapid response to threats is critical and best accomplished by detecting across multiple channels, leading with email detection integrated to SaaS applications and others. Does the solution:

- ☐ Support threat detection and removal across SaaS applications?
- ☐ Integrate threat detection and removal across SaaS applications and email?

Protect users and data from advanced threats infiltrating through SaaS apps

Relying on reputation-based protection to determine account compromise leaves major gaps. An effective solution must leverage advanced threat techniques. Does the solution:

- ☐ Detect credential phishes?
- ☐ Use proactive sandboxing?
- ☐ Employ predictive defense?
- ☐ Leverage dynamic threat analysis?
- ☐ Incorporate threat intelligence?

Mitigate critical data loss with integrated threat insights

Combining data insight together with threat insight can prioritize which accounts need attention and risk mitigation most. Does the solution:

- ☐ Combine data protection insight (data classification, access rights, incident content) together with threat insight?
- ☐ Integrate threats detected at the email gateway to alert you and your tools about user accounts and SaaS resources that need attention right away in a breach?

Control the risk of third-party apps and ecosystems

Third-party apps and ecosystems are a considerable source of potential threats. The vetting of third-party apps is inconsistent, making each app potentially dangerous. Does the solution:

- ☐ Assess the risk of access and permission requests from third-party apps?
- ☐ Provide a scalable and sustainable way to manage third-party app access on a granular level?
- ☐ Provide equivalent support for all apps or does it favor apps in its native ecosystem?

Prioritize risk with user behavior analytics

User behavior analytics (UBA) can predict risk through behavior and aid in resource response. Does the solution:

- ☐ Combine threat detection with UBA to assess the severity of an attack?
- ☐ Prioritize resource allocation in the case of a confirmed breach?

Protect data from risky logins by using real-time access controls

Real-time access controls apply appropriate controls based on session risk levels to protect SaaS resources. Does the solution:

- ☐ Compile and assess login parameters to determine session risk?
- ☐ Protect against stolen credentials or malicious third-party apps?
- ☐ Use session risk to determine which resources are available to users?

Deliver protection with a flexible architecture

Customers may need to satisfy a wide variety of use cases depending on the type of threat and SaaS resources used. Does the solution:

- ☐ Support API-based functionalities?
- ☐ Support forward proxy functions?
- ☐ Solution support reverse proxy functions?

Proofpoint SaaS Protection secures data in your SaaS apps to protect the way your people work. We combine threat detection, data-loss prevention (DLP), third-party app control, access control, and analytics to help you safeguard Microsoft Office 365, Google's G Suite, and more.

To learn more, visit www.proofpoint.com/us/products/saas-protection.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.