WEBINAR SUMMARY

July 1, 2021

black hat®

Attacking and Defending the Microsoft Cloud (Office 365 & Azure AD)

Maor Bin, CEO and Co-founder, Adaptive Shield
Sean Metcalf, Founder and CTO, Trimarc

in partnership with

ADAPTIVE SHIELD

TABLE OF CONTENTS

INTRODUCTION

On Thursday, July 1, 2021, Sean Metcalf, Founder and CTO of Trimarc, and Maor Bin, CEO and Co-founder of Adaptive Shield, joined the BlackHat webcast to discuss attack vectors in the cloud, and what companies can do to keep their applications and infrastructure safe in today's complex environment. They shared best practices and prioritization that can help organizations stay one step ahead in SaaS security.

> Most, if not all, companies are in the cloud or are moving toward the cloud. That means attackers are going after it.
>
> *Sean Metcalf, Founder and CTO, Trimarc*

As companies recognize the many benefits that cloud and software-as-a-service (SaaS) solutions provide, many organizations have shifted or are in the process of shifting operations into the cloud. For companies using Microsoft, this includes a move to the Microsoft Cloud, including Azure Active Directory (AD) and Microsoft Office 365.

Like other cloud and SaaS offerings, Microsoft's solutions are not immune to attacks, but applications and infrastructure can be secured against these attacks. Solutions like Adaptive Shield's SaaS Security Posture Management (SSPM) help security professionals protect the organization against attacks on what is often a complex environment.

KEY TAKEAWAYS

Microsoft Cloud Attack Vectors

Microsoft Cloud can be targeted by many different attack vectors. Azure AD user enumeration, password spraying, and token thefts are just some of the paths attackers take to breach the Microsoft Cloud environment. Organizations can and should take a number of steps to protect against these attacks.

Table 1: Common Microsoft Cloud attacks and defenses

Attack	What it is	Defenses
Password spraying	Using a list of commonly used passwords, the attacker attempts to authenticate against each user with one password before attempting the next password. Typically avoids lockout and other similar mitigations by limiting attempts.	Use Active Directory Federation Services (ADFS) to defend. • Enable Smart Lockout. • Block Legacy Authentication with ADFS Authorization rules. • Install Azure AD Connect Health with ADFS on ADFS servers to alert about common issues, bad password attempts, and risky internet protocol (IP) addresses.
Token theft	Attacks cloud administration via the web browser (either through attacker control or embedded code). Modifies a session token used for access; user does not see that the token is different.	• Only use Azure AD accounts (not synchronized). • Enforce multi-factor authentication (MFA) for all admin accounts, preferably with conditional access. • Use Privileged Identify Manager (PIM) accounts to manage all Azure AD roles as "Eligible," not "Permanent." • Protect cloud admin credentials with admin systems: – **OK:** Different web browser on user workstation – **Better:** Connect to admin server to perform cloud administration – **Best:** Separate admin workstation for cloud administration

Table 1: Common Microsoft Cloud attacks and defenses (continued)

Attack	What it is	Defenses
Elevate access	Attackers can grant permissions to other applications from Global Administrator roles in Azure AD. For example, a Global Administrator in Office 365 can be elevated to a User Access Administrator for all of Azure.	Understand how access elevation works, specifically how Azure AD Global Administrator has Azure Admin rights so that they can protect against this unanticipated attack path.
Tenant hopping	An attacker compromises one tenant to jump to another, often with privileged rights. As with "Solarigate," a compromised partner can be used to compromise other partners.	• Review and limit consented partner access. • Ensure only cloud admin accounts have high privileges on the tenant. • Use PIM, Privileged Access Management (PAM), and conditional access to lock down and protect the environment. • Review permissions regularly to ensure they are properly configured for the environment.

Microsoft has also introduced security defaults, which can be used to further protect cloud administration. This set of basic identity security mechanisms are automatically enforced when enabled, better protecting administrators and users from common identity-related attacks. These defaults should not be used with conditional access.

Best Practices: Defending Against Attacks on Microsoft Cloud

Organizations need to be proactive in their defense against attacks on Microsoft Cloud, both on-premise and in-the-cloud attacks. However, putting all security measures in place at once can be challenging. The table below breaks down security tasks into "do right now" and "do soon" to help organizations better prioritize.

Table 2: Security Checklists: Tasks to do right now and tasks to do soon

Do Right Now	• Require MFA for all cloud admin accounts. • Require PIM for all Azure AD roles. • Enable "Password Hash Sync" (Azure AD Connect). • Ensure all apps use modern authentication via the Azure Active Directory Authentication Library (ADAL) to connect to Office 365 services. • Enable mailbox activity auditing on all Office 365 mailboxes. • Conditional access: Block Legacy Auth (set to "Report" to identify potential issues). • Integrate Azure AD Logs with the organization's security information and event management (SIEM) software or use Azure Sentinel. • Deploy Azure AD Password Protection for the on-premise AD. • Enable ADGS Smart Lockout and configure Azure AD Connect Health for ADFS. • Ensure all users are registered for MFA.

Table 2: Security Checklists: Tasks to do right now and tasks to do soon (continued)

Do Soon	• Enable self-service password reset (SSPR). • Enable MFA for all users via conditional access or risk-based. • Disable legacy authentication entirely via conditional access. • Configure Fast Identify Online (FIDO) for admin accounts. • Follow admin account best practices for cloud admins. • Audit consented permissions for apps and user access to apps. • Review app permissions. • Monitor app registrations. • Review the recommendations in Microsoft Secure Score and implement as many as possible.

Cloud Vulnerability via Azure AD Connect

Threat actors often target the cloud through on-premise components that interact or interface with the cloud itself. With Microsoft Cloud, these attacks often leverage Azure AD Connect using one of the following attack areas:

Microsoft Pass-Through Authentication (PTA)

This authentication enables a user to sign on to both on-premise and cloud-based applications using the same passwords. When the server hosting PTA—usually the Azure AD Connect server—is compromised, it grants access to both on-premise and cloud applications, giving threat actors access to the cloud.

Azure AD Seamless Single Sign-On (SSO)

The SSO solution automatically signs users in when they are on corporate devices, connected to the corporate network. When compromised, the attacker can leverage SSO to access the cloud.

On-Premise Cloud Integration

Azure AD Connect service accounts are granted password hash sync rights. These can be compromised if a compromised account is a member of the Server Admins group or any of the Server Tier groups, or if it is delegated rights to modify groups in the Groups organizational unit (OU).

Defending Azure AD Connect, including the server and database components of the SQL Server database in use, can mitigate these attacks.

Best Practices for Defending Azure AD Connect

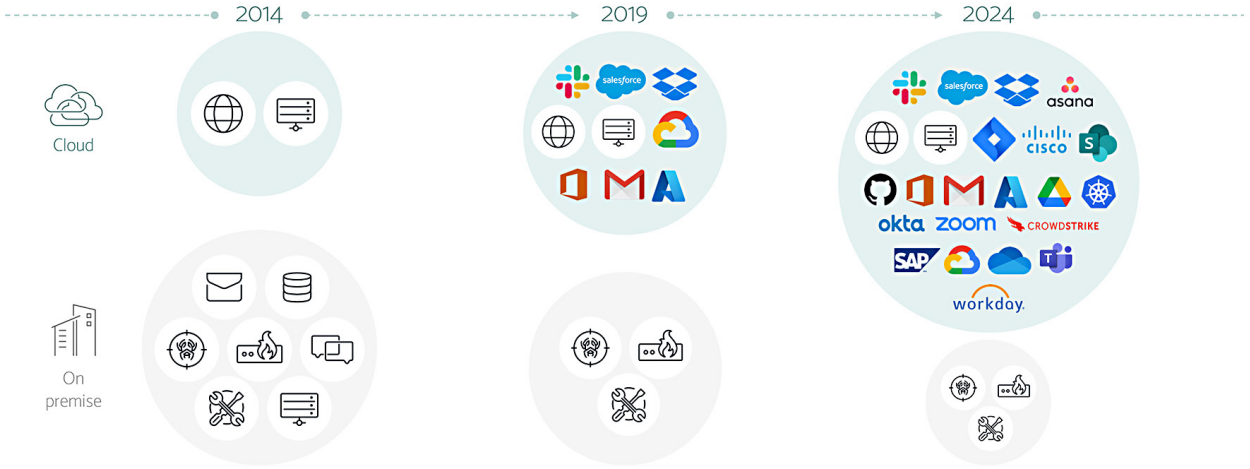
- Treat the Azure AD Connect Server, SQL server/database, and service accounts as Tier 0 (like domain controllers).
- Ensure that the Azure AD Connect server and SQL server/database is in the top-level admin OU.
- Limit the group policies that apply to Azure AD Connect-related systems.
- Restrict local admin rights on Azure AD Connect-related systems.

THE CISO'S GAMBIT: STAYING A STEP AHEAD OF TODAY'S SAAS SECURITY PROBLEMS

SaaS Complexity Leads to Misconfigurations and Mistakes

As more software-as-a-service (SaaS) and cloud-based applications and solutions are added, the complexity of SaaS increases. As seen in figure 1, on-premise is shrinking with the business tools of record moving to the cloud. The increased complexity exposes enterprises to misconfigurations and mistakes, creating security issues.

Figure 1: SaaS continues to grow, introducing complexity that creates security issues



In 2020, Gartner named a new category of cloud security—SaaS Security Posture Management (SSPM). Not covered by existing tools such as CSPM or CASB, the most recent addition to the hype cycle can continually assess security risks from the SaaS app estate.

Often left unsecured or handed over to less-trained employees who manage Marketing, Product, or Sales, SaaS errors such as misconfigurations, inadequate authentication protocols, insufficient identity checks, credential access, and key management leave companies at risk.

Common SaaS security problems include:

- **Each app and its settings are different:** Every app has unique settings, a distinct user interface (UI), its own "language", and other factors that can make it difficult to create defense mechanisms that work for all apps.
- **SaaS app environments are dynamic:** Every update and change can impact how configuration affects security.
- **Fractured visibility and management across apps:** There is no central visibility or management tool that is designed for all SaaS application figurations, so important security configurations can be missed.
- Shared responsibility is misunderstood: It isn't always clear to organizations what security components they are responsible for and what the vendor must secure.
- **Security teams are overloaded:** This is a problem especially when configuration management for each SaaS app is added to their list of responsibilities.
- **Improper configurations create breach risks:** Even one incorrect configuration can allow attackers access to the application and cloud.

Surveying the CISO Market

To understand how teams are currently dealing with their SaaS security posture, and what their main concerns are in handling SaaS tools, Adaptive Shield surveyed 300 InfoSecurity professionals from North America and Western Europe, in companies of 500+ employees. The survey was completed by Global Surveyz, an independent survey company, and the responses were recorded in May, 2021.

The results of the 2021 SaaS Security Survey Report present a picture of the urgent and growing need to secure this landscape. Security professionals recognize the issue at hand, and SaaS misconfigurations are a top concern. The more applications organizations onboard, the harder it becomes to keep them in check. However, with so much complexity, security owners can't help but hand over management to stakeholders with far less experience and know-how. As monitoring and maintenance spreads across departments, this creates an even greater risk of human error. The data indicates that SSPM has risen to the top of the operational agenda and that it has become a top priority for CISOs and security professionals.

Key findings of the report include:

Cloud Risk Ranking: SaaS Misconfigurations Are Considered a Top Threat

SaaS misconfigurations were reported among the top three risks that today's organizations are aware of, with 85% of companies calling out the threat. Interestingly, many of the other threats that are mentioned as a risk to today's security posture can also come as a result of misconfigurations, showing that indirectly, the threat level is even greater.

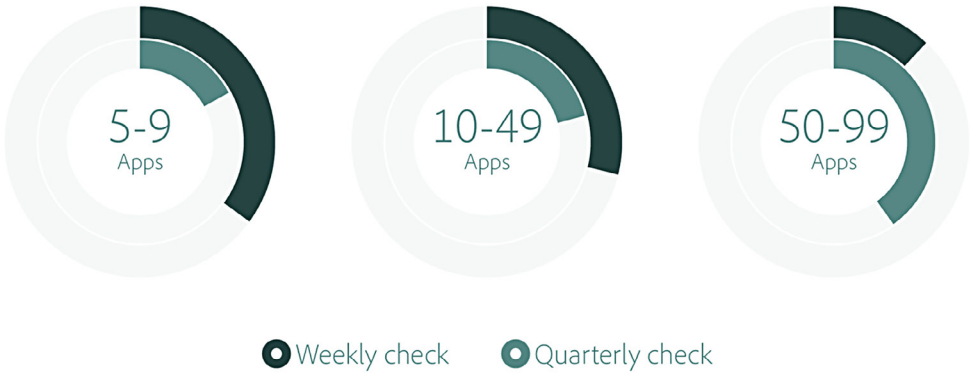
Figure 2: Cloud risk rankings

Risk	High	Medium	Low	None
Account hijacking	45%	35%	17%	3%
Data leakage	44%	27%	18%	10%
SaaS misconfigurations	**32%**	**29%**	**24%**	**15%**
Insufficient identity, credential, access and key management	32%	28%	21%	18%
Insecure interfaces and APIs	32%	26%	25%	17%
Phishing	32%	21%	24%	25%
Ransomware	30%	27%	24%	20%
Insider threats	29%	31%	26%	15%
Limited cloud usage visibility	29%	26%	28%	16%
Metastructure and applistructure failures	27%	38%	23%	13%
Weak control plane	26%	28%	31%	15%

The SaaS Security Paradox: As SaaS Use Grows, Security Checks Lessen

With SaaS misconfigurations considered a top threat, you would expect that the more SaaS apps a company has, the more regularly they would check them. In reality, the opposite is true. The more apps a company has, the less they check security settings and permissions for misconfigurations. Only 12% of companies with 50-99 applications check them weekly.

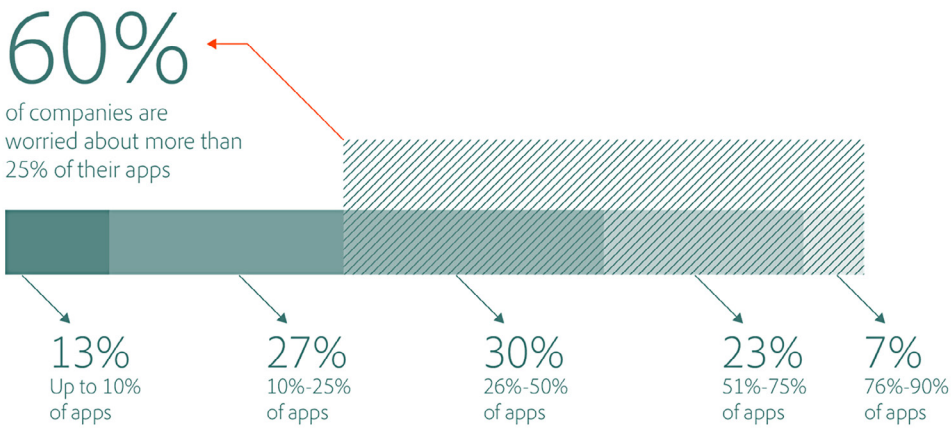
Figure 3: Configuration Checks' Frequency by Number of SaaS of Applications



Companies Struggle to Maintain Continuous SaaS Security Hygiene

Despite the majority of survey respondents (60%) reporting high concern with more than 25% of their SaaS app configurations, their frequency of reported checks remains low. One of the biggest challenges for security teams is the ability to configure the settings of all internal SaaS apps. Each app has different settings, a different user interface, its own terminology and its distinct complexities. Manually configuring settings for these disparate apps for hundreds to thousands of users is an impossible task.

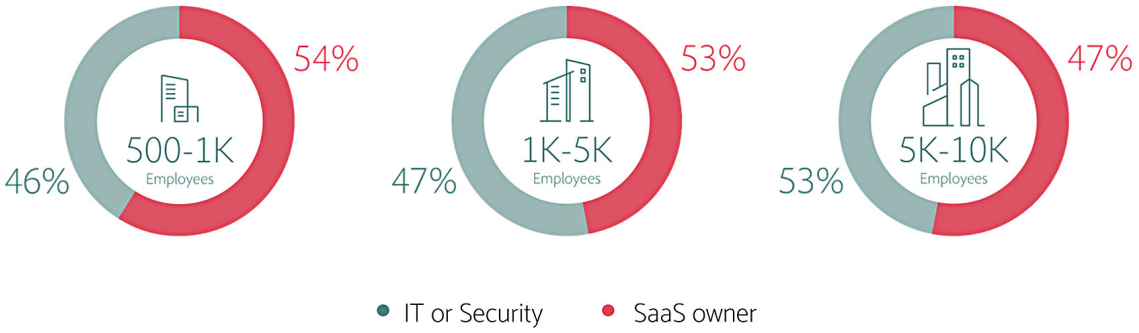
Figure 4: Configuration Checks' Frequency by Number of SaaS Apps



The Dispersal of Delegation: App Owners Find Themselves Responsible for Security

52% of companies report delegating responsibility over app security to the SaaS owner, who may be in departments such as Sales, Marketing, or Product, and is unlikely to be trained in security and compliance.

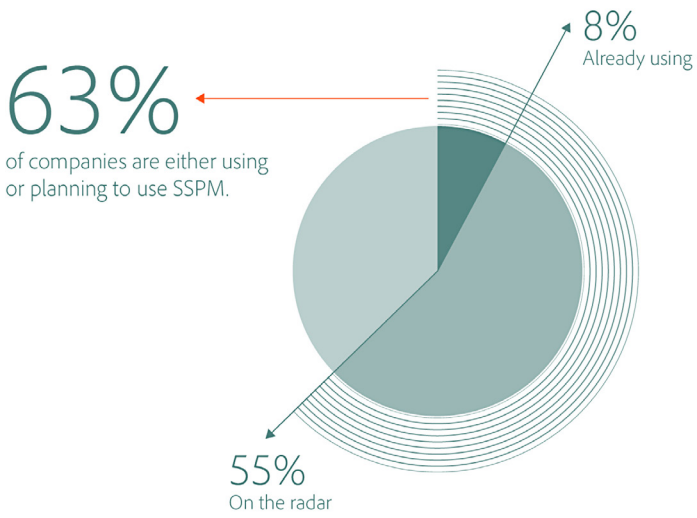
Figure 5: Configuration Checks' Frequency by Number of SaaS Applications



2021 Planning: Security Professionals See an Increasing Need for SSPM Tools

Security professionals recognize that securing the SaaS estate without a solution in place is not maintainable as SaaS apps become the system of record for most companies across all industries. SSPM provides an automated solution that can assess security risks and identify misconfigurations across an organization's SaaS estate, enabling continuous security hygiene through deep visibility, detection, and remediation. The majority of security professionals recognize the importance of SSPM to their SaaS security; 63% say their organizations are using or plan to use SSPM solutions in the near future.

Figure 6: SSPM Use and Plans



> You need to stay ahead and make sure that your security posture and native security configurations of all the different platforms your organization uses are aligned with your organization's policy.
>
> *Maor Bin, CEO and Co-founder, Adaptive Shield*

Effective SSPM solutions provide full visibility into the company's SaaS security posture, checking for compliance with industry standards and company policy. Some solutions even offer the ability to remediate right from within the solution. As a result, an SSPM tool can significantly improve security-team efficiency and protect company data by automating the remediation of misconfigurations throughout the increasingly complex SaaS estate.

Learn more about how you can secure your company's SaaS security now.

BIOGRAPHIES

Maor Bin

CEO and Co-founder, Adaptive Shield

A former cybersecurity intelligence officer in the IDF, Maor has over 16 years of experience in cyber-security leadership. He led SaaS Threat Detection Research at Proofpoint and won the operational excellence award during his IDF service. Maor holds a BSc in Computer Science and is the CEO and co-founder of Adaptive Shield, the SaaS Security Posture Management solution built to help security teams gain control over their SaaS app security and prevent vulnerabilities that could lead to leaks or breaches.

Sean Metcalf

Founder and CTO, Trimarc

Sean Metcalf is founder and CTO at Trimarc (TrimarcSecurity.com), a professional services company that focuses on improving enterprise security. He is one of about 100 people in the world who holds the Microsoft Certified Master Directory Services (MCM) Active Directory certification, is a Microsoft MVP, and has presented on Active Directory, Azure AD, and Microsoft Cloud attack and defense at security conferences such as Black Hat, BSides, DEF CON, and DerbyCon.