Are You Ready for a Breach in Your Organization's Slack?

Overview

As Slack becomes a dominant part of the infrastructure in your organization, it will increasingly become a target for attacks and at some point, it is likely to be breached — just like any other technology that we use. The impact of that breach, however, depends on how we prepare for it, by limiting its potential propagation and allowing for fast response.

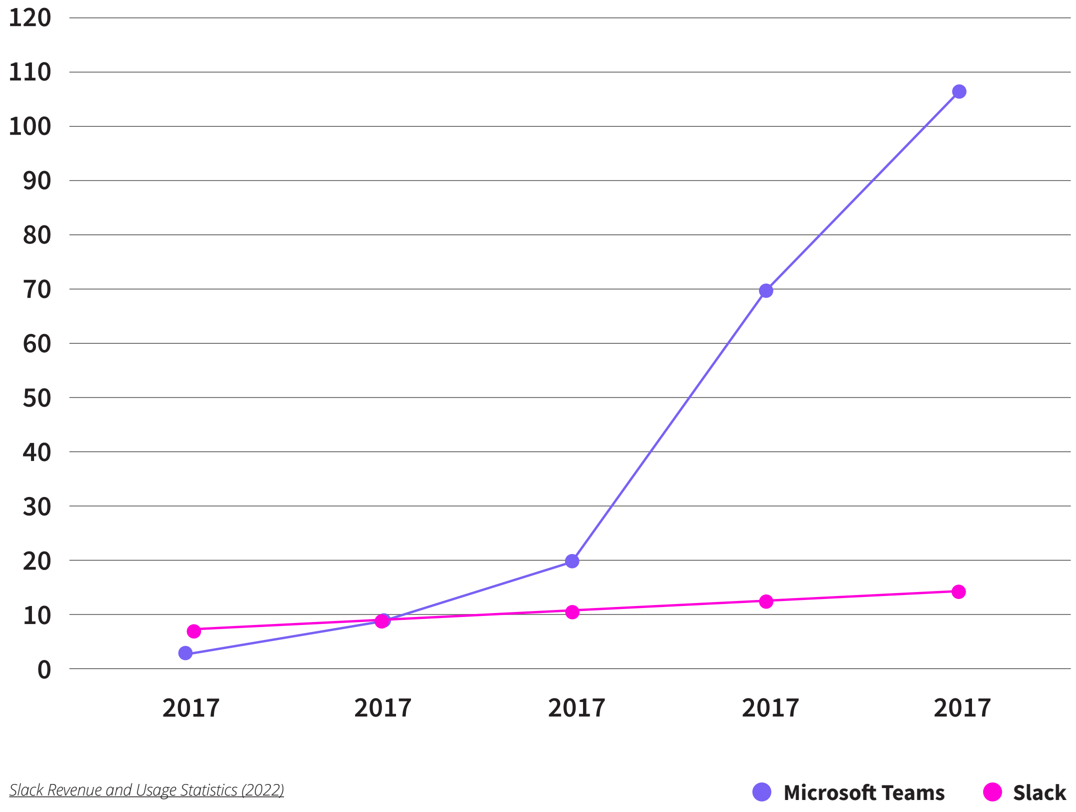
Slack (and similarly, Microsoft Teams) has gained immense popularity and adoption in the last few years, and there is a good reason for that — it is an amazing collaboration tool. This new experience, however, comes with the usual challenges of adopting new technologies, including security. While Slack itself is a secure platform, the way it is used by organizations can lend itself to various attacks: leveraging misconfigurations, insecure practices, supply chain attacks (through 3rd party apps), and user mistakes. The vast amount of data stored on Slack, as well the sensitivity of that data, makes the potential impact of such a breach extremely high. Furthermore, detecting and responding to Slack attacks can be difficult, due to limited available technology, processes, and skills.

Readiness can reduce the impact of potential Slack breaches. The time you spend now considering the potential challenges and security risks of a Slack breach and preparing for one will help you when it happens. This eBook provides an in-depth analysis of Slack risks as well as detection and response challenges, and actions you can take to reduce the impact and likelihood of potential Slack breaches.

Background

Over the last decade, Software as a Service (SaaS) platforms have become increasingly popular with enterprises, replacing traditional legacy corporate applications with modern, cloud-based solutions. This move has accelerated during COVID, and even the most conservative organizations are gradually migrating to SaaS applications. The shift to an as-a-service model offers many advantages over the need to maintain (and secure) legacy on-prem applications, yet it also introduces new risks and challenges.

Slack vs Microsoft Teams: Daily Active Users (DAUs) and Organizations



Slack Revenue and Usage Statistics (2022)

Slack has 12 million daily active users and 156,000 organizations subscribe to the app, but over 750,000 organizations use Slack

1.5 billion messages are sent on the service every week

There are 2,000 apps and 750 bots available in the Slack App Directory

According to Slack, 65 of the Fortune 100 use Slack in some capacity, including IBM, Amazon, PayPal, and Airbnb

Over 500,000 developers use Slack

While many of the potential risks and challenges in this space have been long known by cloud security practitioners, the recent Okta breach caught many in our industry by surprise. Okta is a critical SaaS infrastructure component, yet this breach demonstrated that most of the industry was poorly prepared for such an incident. Many organizations using Okta did not have the infrastructure to investigate and respond to a breach coming through Okta (regardless of whether the breach was due to an issue with Okta itself, or simply because LAPSUS$ was able to leverage it), and there was a lot of confusion once the breach became public. In the hours following the breach, we released internal research on Okta Log Investigation to support the community, which needed actionable information to conduct their own investigations.

While the Okta breach caught attention, it is just a timely example. Of the dozens of SaaS applications adopted by each organization, many are critical to the organization's infrastructure and hold extremely sensitive data. In most cases, these critical SaaS applications replace an existing critical infrastructure, such as corporate email or enterprise resource planning (ERP). While still introducing a new technology stack in many cases, this 1:1 replacement allows for (at the very least) some benchmarking regarding expected security controls, permissions, monitoring, and even communications culture.

Worldwide Public Cloud Services End-User Spending Forecast (Millions of U.S. Dollars)

	2020	2021	2022
Cloud Business Process Services (BPaaS)	$46,6066	$51,027	$55,538
Cloud Application Infrastructure Services (PaaS)	$58,917	$80,002	$100,636
Cloud Application Services (SaaS)	$120,686	$145,509	$171,915
Cloud Management and Security Services	$22,664	$25,987	$29,736
Cloud System Infrastructure Services (IaaS)	$64,286	$91,543	$121,620
Desktop as a Service (DaaS)	$1,235	$2,079	$2,710
TOTAL MARKET	**$313,853**	**$396,147**	**$482,155**

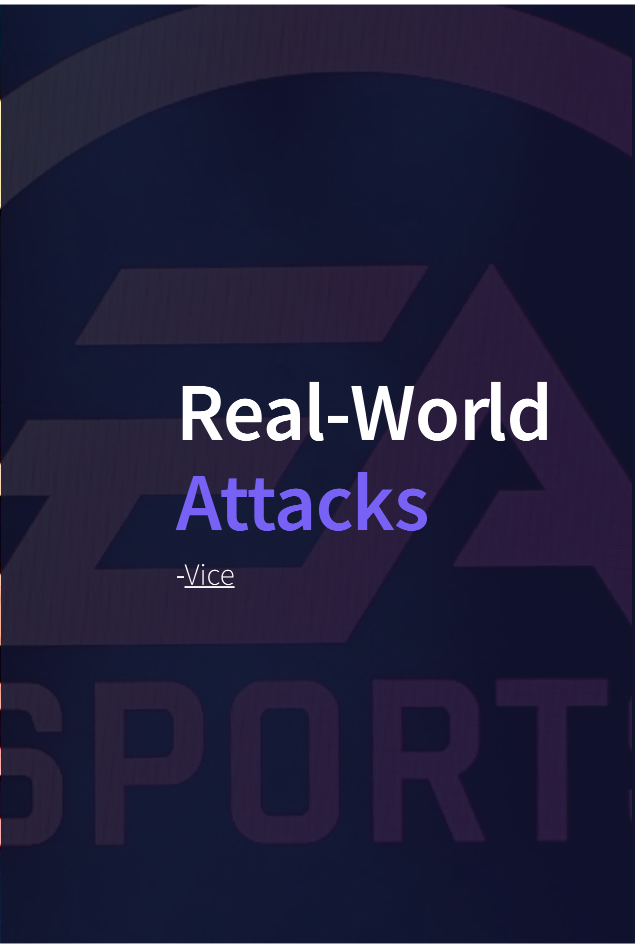
BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; SaaS = software as a service
Note: Totals may not add up due to rounding. **Source:** Gartner (August 2021)

The Slack Experience

Slack, on the other hand, represents an entirely new solution for most organizations. Very few companies had on-prem chat solutions, and even then, adoption was usually limited to the technology teams. Many teams today use Slack daily to coordinate and communicate across teams and time zones; most organizations moved to some form of hybrid work when the pandemic began, and Slack provides an important way for teams to work and collaborate efficiently regardless of physical locations.

This new experience, however, comes with the usual challenges of adopting new technologies — around culture, functionality, expected user behavior, and, of course, security. One of the most interesting cultural aspects of Slack usage is the place that it is taking in the organizational communication and knowledge management stack. For many, Slack has become the main communication channel within the organization, replacing email for most tasks. Moreover, Slack channels are becoming sources of knowledge and replacing knowledge management repositories.

As a result, we see more and more organizations where Slack is becoming one of the most sensitive collections of organizational data. Indeed, Slack contains far more sensitive information than the corporate email system or even an organization's internal knowledge management system.



Real-World Attacks

-Vice

In 2021, a group of hackers stole data from game publishing giant Electronic Arts (EA). The attack included tricking an employee to provide a login token by contacting them over Slack. The attack process began with purchasing stolen cookies that were sold online for $10 and using those cookies to gain access to an EA Slack channel. We all use cookies often, accepting cookie policies on most websites for all data to be stored. Some cookies save the login details of users, which could allow hackers to log into services as that person. In the EA breach, hackers accessed EA's Slack using the stolen cookie.

Once inside the chat, the attackers requested a multifactor authentication token from EA IT support to allow them to gain access to the corporate network. This allowed them the leverage needed to download the game source code. The group stole the source code for FIFA 21 and related matchmaking tools, as well as the source code for the Frostbite engine that powers games like Battlefield and other internal game development tools. In all, the hackers claimed to have extracted 780GB of data, and advertised it as for sale on a variety of underground forums. EA confirmed the data impacted in the breach.

The Slack Security Challenge

Before diving into the challenges, it is important to state — Slack is a secure platform. It offers great security capabilities, and Slack itself, as a vendor, invests substantial resources in securing its infrastructure, platform, and the software itself.

Nonetheless, like any other technology platform, Slack can serve as a basis for attacks, many of which do not require abusing a new vulnerability, but take advantage of built-in features, insecure usage, or misconfigurations. But while other collaboration and communication platforms (such as email) have been around for years and have an entire ecosystem of security solutions and best practices built for them, messaging apps such as Slack have only a very small subset of these security solutions and practices in place.

Before discussing how organizations can deal with such breaches, let's first examine some of the risks and challenges that Slack (or similar technologies) introduces. Probably at the top of that list is something that has nothing to do with technology, but rather (as always) with people.

The Slack culture is very open, collaborative, and trusting. It is so by nature, but it is that nature that makes it easier to attack. Years of phishing attacks have made us very suspicious of any out of the ordinary email, but very few users will ever suspect a message from a coworker on Slack. Therefore, compromising a single account in Slack can easily be leveraged to deceive other users and gain additional access. Furthermore, the open culture presents itself in Slack groups. Most organizations believe in leaving as many groups as possible public, encouraging participation and allowing users to search them (as part of the Slack as a Knowledge Base approach). However, many users don't think about the significance of that and post sensitive information in public Slack groups. Furthermore, the "casualness" of a Slack chat often makes people share more sensitive comments or even secrets, such as passwords or cloud Application Programming Interface (API) keys. Shared as part of a conversation, people never think about it being stored forever and forever — and accessible to a single compromised account.

Compromising a single account in Slack can easily be leveraged to deceive other users and gain additional access.

But culture is not the only problem. Like many other SaaS platforms, Slack offers an extensive marketplace of applications and allows you to build additional applications outside of this marketplace. Third party apps in SaaS platforms are a huge supply chain risk, creating an attack vector for pretty much any SaaS platform. Slack is no different. This risk, however, is further augmented when considering the culture of Slack usage. Many 3rd party apps will ask for extremely extensive permissions, but even the seemingly benign request to "read from all public channels," allows access to endless amounts of data. Data its original authors have not considered to be easily accessible outside the organization.

Daily Tools in the Slack app directory

zoom Microsoft Teams Outlook

Unfortunately, these examples are just the tip of the iceberg. Spending a few hours threat modelling how we use Slack required us to invest substantial efforts in securing our Slack. While almost all our Slack groups are private and we are extremely strict about which apps, if any, are given permissions to Slack, we still uncovered many additional potential risks, including issues around content filtering, lateral movement, 3rd party communication (Slack Connect), and many more.

Slack Detection & Response

Making things just a little harder, the Slack security challenge extends beyond the materialization (or prevention) of these risks. As Slack becomes a dominant part of the infrastructure in your organization, it will become a target for attacks, and as it becomes a target for attacks, at some point, it will be breached (just like any other technology that we use).

Organizations must be able to identify, contain, and respond to security incidents and breaches in a timely manner to reduce the impact to the bare minimum. Unfortunately, both the technology and practices required to do so for Slack are limited and in their infancy. For a start, Slack will only provide access to security logs to customers using its Enterprise (most expensive) tier. Without security logs, both detection and response are almost impossible. This is part of other advanced security features (such as SSO) that are not available in their standard and pro plans, leaving many medium to large organizations exposed.

But having access to the logs themselves is not sufficient on its own. Having the logs, or even streaming them to your security information and event management (SIEM) and security operations center (SOC) will not help without the relevant knowledge and understanding of those logs and how to identify attacks in them. With little to almost no out-of-the-box rules and information, most organizations simply lack the knowledge and skill to detect, investigate, and respond to Slack incidents or breaches.

Furthermore, what many users don't know is that (unlike some other SaaS technologies), Slack does not keep history or revisions of anything that has been erased. If an attacker can delete messages, these messages are gone forever. This can turn into an effective ransomware attack, which is hard to respond to without upfront preparations, predominantly backups.

Should I Stop Using Slack?! Definitely NOT!

Slack is an amazing platform that, ideally, makes your business work more efficiently. While the last few paragraphs may have been scary, it is part of the world we live in. Any platform we use — whether it is email, file collaboration, finance, or something else — is susceptible to risk and may be an attack vector. It is through understanding of these risks that we can become more secure and more resilient in facing those attacks.

Top 5 Things to Consider in Preparation for a Slack Breach

Here are the top five things to consider as you think about a potential Slack breach:

01

Private/Public Groups Culture

Defining a clear policy on what types of groups can be public and what types need to be private, enforcing it, and educating the users around it. It is not an easy shift, but nonetheless, it is an essential one for something that becomes critical infrastructure and a repository of data.

03

Backups for Slack

Backing up your Slack is essential if Slack serves as a knowledge management repository and a critical asset in the organization. Backups can be done through automation of Slack's export capabilities or using 3rd party vendors that offer this service.

02

Limited 3rd Party App Permissions

Restricting 3rd party apps to the bare minimum permissions is a necessary step in limiting the impact of a 3rd party breach. Sometimes it is better to simply give up on an app that is not necessary. At other times you can restrict the app to the minimum privileges needed to allow functionality. Many app vendors normally ask for excessive permissions without any real need.

04

Enable Advanced Security Features

Requiring multi-factor authentication (MFA) (directly or via SSO) is the bare minimum, but you can enable additional security features, including additional encryption, compliance, security management, and more when purchasing the Enterprise license for Slack.

05

Collect and Prepare Slack Logs (Forensics)

Collecting, analyzing, enriching, and preparing Slack logs makes it easier to quickly respond to an incident or a breach, so that it can be contained and eradicated as quickly as possible — and with minimal impact. Forensics analysis sits at the baseline of any major breach response. Through forensics analysis, incident responders can understand and block the entry path, assess the damage that has been done, and respond quickly and effectively.

Readiness can reduce the impact of potential Slack breaches

The time you spend now considering the potential challenges and security risks of a Slack breach and preparing for one will help you when it happens. The steps outlined above can help you reduce the impact, as well as the likelihood, of potential Slack breaches.

Mitiga's technology and services provide continuous, proactive breach investigation, lower the impact of cyber breaches, and optimize readiness for critical cloud and hybrid incidents. This readiness-first approach accelerates response and recovery time, increasing resilience when incidents occur. Mitiga's shared-responsibility model is unique. Unlike others, who charge additional fees for critical cloud incident response and recovery, Mitiga subscribers face no add-on fees.

For more information, visit www.mitiga.io or email us at info@mitiga.io

US +1 (888) 598-4654 | **UK** +44 (20) 3974 1616 | **IL** + 972-3-978-6654 | **SG** +65-3138-3094