

2024

# Okta Cyber Trust Report



# Identity under attack

Attacks during the last two years have highlighted critical vulnerabilities in Okta's cybersecurity defenses. As a leading Identity-as-a-Service (IdaaS) provider, Okta provides services to around 18,000 organizations and over a million end users. Each of those end users is a potential access point for bad actors.

The recent breaches began with the Lapsus\$ breach in January 2022, followed by the Oktapus phishing campaigns and **two** separate source code thefts. Major attacks on MGM and Caesars in September 2023 led to untold millions in damages and a breach of Okta's support unit in October 2023 placed 100% of their entire customer base at risk.

The attacks show a pattern of security shortcomings. Not only is Okta not providing the technical controls needed to impart true security to their clients—they are falling short of protecting their own resources.

Organizations can no longer rely solely on outsourcing to secure their Okta environments. Organizations like yours must actively engage in safeguarding their systems. That means proactively upgrading your security postures in response to the evolving threat landscape. Let's examine Okta's security weaknesses to help you understand how you can safeguard yourself against these risks.



## 2022

**JAN**

Okta breached by Lapsus\$

**AUG**Oktapus phishing campaigns  
breach multiple organizations**SEPT**

Auth0 source code stolen

**DEC**

Okta source code stolen

## 2023

**FEB**Oktapus smishing attack  
targets Coinbase**SEPT**MGM and Caesars Casinos breached  
via Okta AD Sync Connector**AUG**Okta notifies users of ongoing  
social engineering attacks**OCT**Okta's support unit breached,  
leading to admin session  
takeover**OCT**Okta discloses support unit  
breach actually affected all  
customers

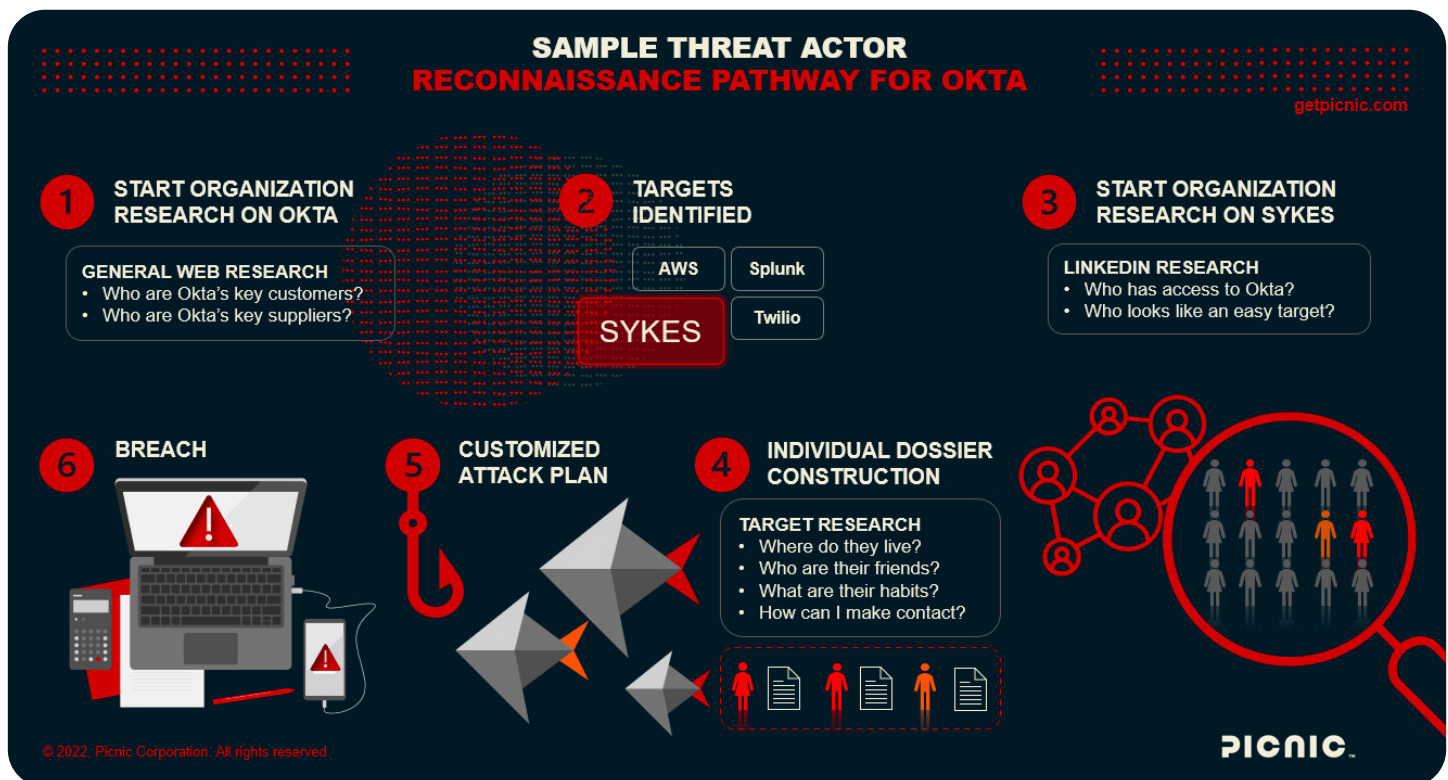
2022

JANUARY

# Lapsus\$: Forced to disclose after the fact

In January 2022, Okta experienced a significant breach when the Lapsus\$ hacker group gained access to a Sitel employee's machine. Sitel, contracted to handle customer service for Okta, became the gateway for the attackers. The breach initially went undisclosed by Okta. When Lapsus\$ publicly shared screenshots of Okta's internal systems, Okta was forced to admit the extent of the compromise.

The breach affected a confirmed subset of Okta's clients, [around 2.5%](#) of their customers. Okta's services remained unaffected, but the delayed disclosure raised questions about transparency and customer impact. This incident served as a stark reminder of the vulnerabilities inherent in third-party access and the necessity for rigorous security protocols.

Credit: [Picnic](#)

## Not so phishing-resistant: Oktapus campaigns

The Oktapus phishing campaign used basic phishing kits and caused significant breaches in over 130 organizations. Even low-skill cyber attacks can have devastating effects.

[Group-IB's investigation](#) revealed that the attackers' primary goal was acquiring Okta identity credentials and one-time codes used for multi-factor authentication (MFA) from individuals within targeted firms.

The method of attack was deceptively simple, yet alarmingly effective. Employees received SMS messages with links leading to counterfeit Okta authentication pages. Once there, the employees

unknowingly submitted their corporate credentials and one-time codes, which attackers then used to access corporate resources and carry out data theft.

This methodical approach allowed unauthorized access to sensitive information and the ability to make lasting changes for persistent access.

With 169 distinct domains compromised, the Oktapus incident serves as a critical lesson in the importance of advanced security measures and the risks of relying on phishable MFA, which the attackers sidestepped with ease.



## Not once: Auth0 source code stolen

---

Auth0, a subsidiary of Okta and provider of authentication services, announced a “security event” related to its code repositories. Auth0’s platform, which is used to authenticate over 42 million daily logins by enterprises worldwide, including notable firms like AMD and Siemens, experienced an unauthorized acquisition of code repository archives dating back to 2020 and earlier.

An external party alerted Okta to possession of Auth0’s code archives from October 2020 and earlier, or the breach may not have been discovered.

[Auth0](#) didn’t release details about the incident’s specifics, such as the method of data exfiltration and the exact nature of the “precautionary steps” taken to secure their systems. This omission left customers and other concerned parties questioning the timeline and the potential vulnerabilities in the archived code.

This breach continued the trend of vague updates and assurance that Auth0 “found no evidence of unauthorized access to our environments, or those of our customers, nor any evidence of any data exfiltration or persistent access.”

Transparent disclosures are particularly important for identity platforms that secure millions of consumers because it can provide organizations with clear paths to take to protect themselves or assess impact. The continued lack of transparency erodes trust between Okta and their customers at large.

## But twice: Okta source code stolen

---

Okta encountered another significant security breach when bad actors gained access to Okta’s private code repositories on GitHub. GitHub observed suspicious activity and promptly notified Okta.

Okta confirmed the attackers copied several repositories, specifically those associated with the company’s Workforce Identity Cloud (WIC) solution. The implications of the breach were considerable, given the critical nature of the stolen source code.

# 2023

FEBRUARY

## Oktapus smishing attack

The Oktapus smishing campaign targeted employees of the cryptocurrency exchange Coinbase. Despite MFA, the attackers acquired personal employee data from Coinbase.

Coinbase employees received SMS prompts urging them to log into their accounts. One employee complied, and the attackers gained their login details. The attackers then called the employee, posing as Coinbase IT staff, and extracted further credentials.

Coinbase contained the attack within minutes, preventing a major data breach. But the incident further highlighted the critical vulnerability Okta customers faced.

The attack served as a reminder that social engineering remains effective and highlighted the critical necessity for proactive cyber-defense systems that go beyond employee training.

## Never ending social engineering attacks

Between July 29 and August 19, 2023, attackers targeted many of Okta's US-based customers. The attackers attempted to manipulate IT service desk personnel into resetting MFA factors for highly privileged users. The attackers then exploited Super Administrator accounts to impersonate users within the organizations.

These attacks leveraged a commercial phishing kit known as Oktapus. The kit is equipped with pre-made fake authentication portals and a command-and-control channel via Telegram.

Researchers from [Palo Alto Networks Unit 42](#) and [Trellix](#) noted an expansion in the targeting patterns of the groups who use the kit, like the [Muddled Libra](#) group, which is believed to be behind the attacks.

The threat actors acquired passwords for privileged accounts or manipulated the authentication process through Active Directory (AD). With access to Super Administrator accounts, they could grant higher privileges to other accounts, reset authenticators, and even bypass second-factor requirements.



# 2023

SEPTEMBER

## MGM and Caesars: Okta integrations at fault

In September 2023, two large casino organizations—MGM Casinos (an Okta reference customer) and Caesars Entertainment—suffered breaches resulting in ransomware deployments, shattering the notion of bulletproof cybersecurity in casinos.

The casinos scrambled to regain control as hotel booking systems ceased to work for thousands of guests, casino payouts had to be made in cash, and tens of millions of dollars were being lost per day.

As investigations proceeded, both breaches abused a common element: the Okta Active Directory Sync integration.

Meant to reduce complexity, the Okta AD Sync utility allowed the use of AD passwords to access Okta SSO. Several red-team write ups showing how easy this utility is to exploit were publicly available before the breach occurred.

In a blog post a month before the breaches, Okta disclosed they observed a trend of recent attacks using a combination of social engineering, MFA reset bypass, and cross-tenant impersonation. While they disclosed the attacks, it appears they did little to stop future attacks.



## Impact of the Attack on MGM Resorts International

### Who orchestrated it?

BlackCat/ALPHV  
Ransomare Group



### Daily Revenue Loss

A potential loss of  
**\$8.4 million daily**



### Technical Impact

#### Server Encryption:

MGM's ESXi servers were targeted, paralyzing thousands of VMs integral to their daily operations.



### Long-term Implications

Potential damage to the brand's image, trustworthiness, and customer loyalty.



### Hospitality Systems Affected



#### Hotel Room Access:

Electronic keys became useless.



#### Reservation Systems:

Offline, causing guest challenges.



#### Gaming Operations:

Slot machines went offline.

### Key Takeaway

The MGM attack highlights the massive blow to a cyberattack can deliver to corporations. Business should see cybersecurity as more than just tech, it's vital for their overall strategy.



In its [K-8 filing](#), Caesars confirmed that someone stole customer driver's licenses and Social Security numbers from its customer loyalty database, which is a regulatory nightmare for any company. Caesars' K-8 filing also indicated that they paid a rumored \$15,000,000 ransom to prevent further leaks.

David Bradbury, Okta's CSO, [later confirmed](#) the

attackers breached three additional unnamed companies in similar attacks.

Okta's continued failure to protect the most crucial parts of the identity lifecycle (provisionment and recovery) shows a shocking disregard for identity management in the face of continued, unrelenting attacks.

## Estimations of losses associated with the MGM and Caesars breaches\*

Expenses	MGM	Caesars
Daily revenue lost	\$8.4M	\$8.4M
Downtime	10 days	Unknown
Ransom paid	No ransom paid	\$15M
Reputational damage	Widespread	Widespread
Regulatory overhead	Unknown	Unknown
Fines	Unknown	Unknown
Credit monitoring costs	Unknown	Unknown
Cyber insurance increases	Unknown	Unknown
Expenses	<b><u>At least \$100M</u></b>	<b>At least \$23M</b>
Cyber insurance coverage	\$200M	Unknown

\* The true cost of a breach is difficult to estimate due to disclosed facts and is typically not known until far after the breach has occurred and includes intangible damages such as reputational impact.

## Okta support unit breached

Okta encountered another breach when an unknown party compromised their support system. The breach was first detected by BeyondTrust on October 2nd. They alerted Okta immediately. Okta failed to take action, and the attackers targeted other customers.

Okta disclosed that breaches in customer environments are linked to [HTTP Archive \(HAR\) files](#). Okta suggested sanitizing credentials and cookies/session tokens within HAR files prior to sharing, but they don't offer a guide on how to complete the process. To close this security gap for our customers, Beyond Identity [developed a tool designed to sanitize HAR files](#).

The attackers stole login credentials from an Okta employee's personal Google account. They then used the credentials to access Okta's customer support system, gaining access to files related to 134 customers who had interacted with Okta's support.

Okta finally acknowledged the breach publicly on October 20th, stating that the stolen data could increase the risk of phishing and social engineering attacks on users.

The attackers also ran a report downloading names and email addresses of all 18,400 Okta customer support users, and some Okta employee information.

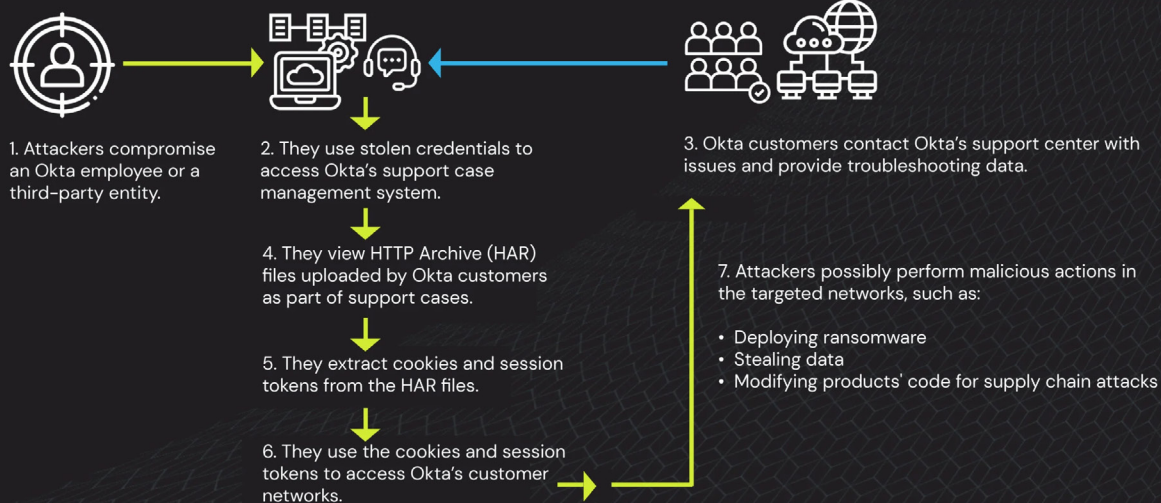
Okta stated that the report did not include user credentials or sensitive personal data. Despite this, the breach disclosed that 6% of Okta customers do not have MFA enabled for administrators, highlighting a significant vulnerability.

The incident underscored the necessity of phishing-resistant authentication, hardware-backed credentials, and device trust across all employees, contractors, and partners.

While there is no current evidence that the information obtained is being used maliciously, the potential for future exploitation remains a concern.



# OKTA BREACH FLOW



Credit: [Cyberark](#)

## What to do to protect yourself: Never trust, always verify

Never trust, always verify is the motto of zero trust security. Okta's track record of breaches does not live up to that expectation.

When the tool you count on to keep your organization safe proves to be a point of weakness, your entire security ecosystem fails.

What can you do to protect your organization? You can step into the future of identity and leave the attackers out in the cold.

**1. Go passwordless.** As we've seen from the Okta breaches, shared secrets can easily be obtained from users, captured on networks, or hacked from databases.

**2. Enforce phishing-resistance.** Remove the opportunity for attackers to obtain codes, magic links, or other authentication factors through phishing, smishing, adversary-in-the-middle, or other attacks.

**3. Validate both user and device.** When you make sure the requesting device is bound to an authorized user, you create yet another hurdle attackers have to jump through before they can even try to access your resources.

**4. Ensure device security.** Determine whether the devices logging in to your system comply with your security policies.

**5. Incorporate multi-dimensional risk signals.** Are you analyzing data from endpoints and security solutions with your policy engine? It's important to assess risks based on factors such as user behavior, the security posture of devices, and the status of the EDR.

**6. Continuously assess risk.** Your security infrastructure should continuously monitor every authentication to detect malicious activity.

**7. Integrate your security infrastructure.** Your authentication solution should integrate with a variety of tools in your security infrastructure to improve risk detection, accelerate responses, and improve audit and compliance reporting. If you use an SSO, especially Okta, you need to be ready to respond at the first sign of suspicious activity. You can assess your defenses for free with the [Okta Defense Kit](#).

## Free tools at your disposal

### Okta Session Analyzer

This free tool, which takes less than 30 minutes to use, helps you determine if you were impacted by an Okta breach that has already occurred or could occur in the future.

The Okta Session Analyzer is a Python tool for detailed analysis and security monitoring of Okta event logs, designed to identify and alert on anomalous activities indicative of security threats.

[Get the Okta Session Analyzer](#)

### HAR File Sanitizer

Know with confidence that your HAR files are clean and secure before sharing them with a third party, such as Okta Support.

This free tool removes sensitive information from HAR files, ensuring they can be shared confidently and without fear of compromising user data.

[Download the HAR file sanitizer](#)

Each of the Okta breaches is a reminder that your organization must remain continuously vigilant. It's time to take charge of your security rather than relying on an organization with constant breaches to be your gatekeeper.

Are you ready for the future of identity? We are.

[Contact us today and begin your journey.](#)

## BEYOND IDENTITY

Beyond Identity is revolutionizing digital access for organizations looking to improve protection against cyber attacks and deliver the highest levels of security for their workforces, customers and developers. Its suite of passwordless, phishing-resistant, and zero trust authentication solutions improves security and user experience. The platform delivers continuous risk-based authentication incorporating signals from the zero trust ecosystem to ensure only valid users and secure devices gain or maintain access to critical resources. Companies like Snowflake rely on Beyond Identity's highly available cloud-native platform to thwart attacks and advance their zero trust strategies. To learn more about Beyond Identity's FIDO-2 certified multi-factor authentication (MFA) solutions, visit [beyondidentity.com](https://beyondidentity.com) and stay connected with us on [Twitter](#), [LinkedIn](#), and [YouTube](#).

[Get a demo](#)

[beyondidentity.com](https://beyondidentity.com)

[info@beyondidentity.com](mailto:info@beyondidentity.com)

BEYOND  
IDENTITY