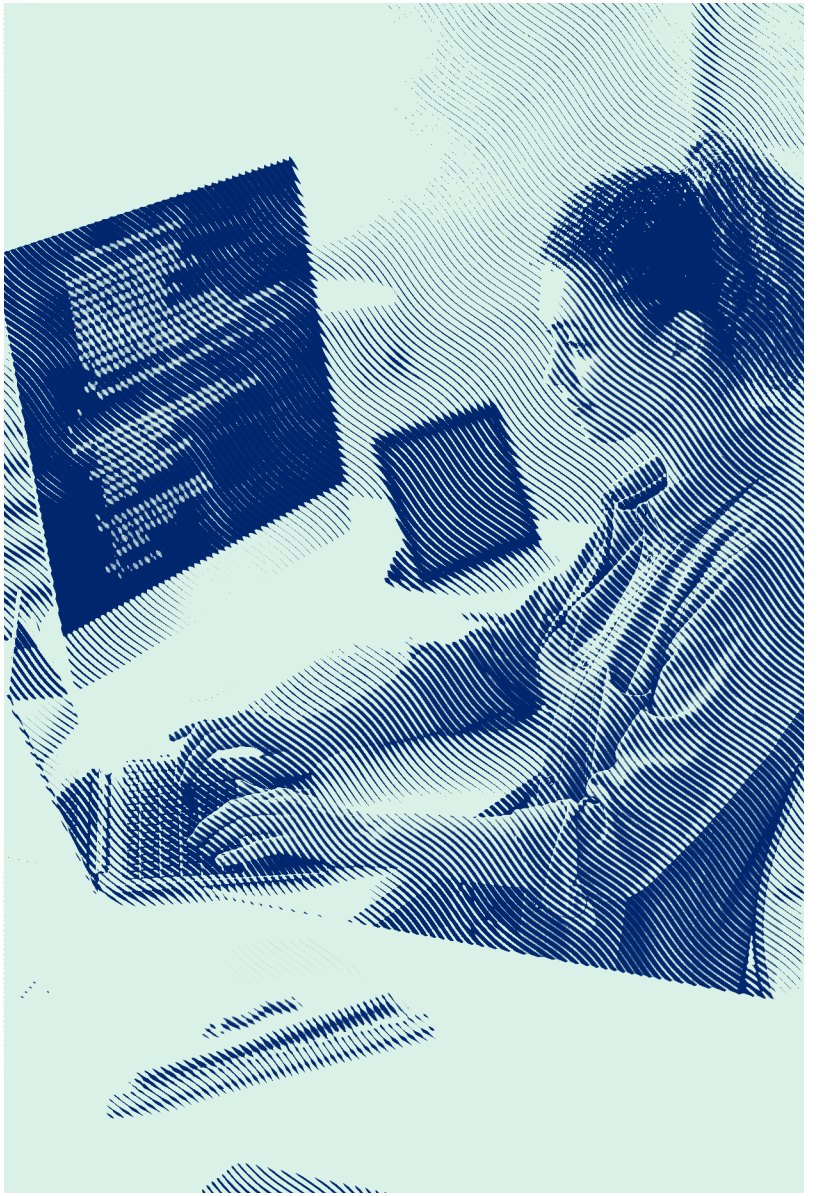
okta

Okta's Ransomware Prevention Checklist

Three practical steps to protect your organisation from ransomware attacks with an identity-centric zero trust approach to security

Enter



While ransomware is far from new, the rapid, global shift towards a new hybrid work culture that operates both inside and outside of the perimeter means organisations today are more vulnerable to attacks than ever before.

According to **The State of Ransomware 2021 report by Sophos**, 37% of organisations having already been hit by ransomware so far this year, while the average total cost of recovery from a ransomware attack has more than doubled from $761,106 in 2020 to $1.85 million in 2021. But what's driving this sudden upsurge?

Traditionally, good data backups and a rehearsed restoration procedure were a good investment against paying a ransom. Of course, examples of backups also becoming infected persist as grim war stories, but only as edge cases. Increasingly, ransomware crews have found innovative ways to circumvent security measures and ensure their efforts are rewarded.

SOPHOS
Cybersecurity evolved.

Data is now regularly stolen before encryption, allowing an attacker to threaten public release as additional motivation to pay. Once compromised, access to a network may be sold to other criminals via access brokers, leading to further attacks of varying motivations. If a supply chain is impacted by a ransomware event, attacks can seek to influence customers of a supplier to apply increased pressure on the victim to restore service quickly.

Knowledge of an attack can also be sold to financial brokers to short sell stock before the attack becomes widely known to the market. And now, far from requiring deep technical experience, ransomware-as-a-service is further enabling complex malicious technologies to a wider criminal audience, for a relatively small fee. This is an adaptive and agile criminal enterprise with many evolving avenues to making money from technical misery. So what's the solution?

While there's no silver bullet when it comes to protecting your organisation from ransomware attacks, this guide will explore how an identity-first security strategy centred around zero trust can help reduce the data breaches that fuel them.

Step 1

Neutralise ransomware attacks with strong, Adaptive Multi-factor Authentication

When it comes to exposing vulnerabilities within corporate IT networks, cybercriminals are usually spoilt for choice. Weak usernames and passwords are often easily compromised by credential stuffing, or password spraying, and act as quick entry points for ransomware attackers. Yet, strong usernames and passwords are also extremely vulnerable, especially when exposed to intelligent phishing attacks that fool victims into revealing their credentials unknowingly.

Fortunately, **Adaptive Multi-factor Authentication** is one of the most effective means of preventing account takeover. Adaptive MFA grants access based on contextual access policies to differentiate between normal and abnormal behaviours and between low-risk and high-risk user actions. These signals are often the first indicators of malicious activity.

While Adaptive MFA can help stop ransomware actors from gaining initial access, a holistic zero trust architecture protects the organisation from potential lateral movement of attackers within the network.

Euro Garages

Euro Garages* recently drafted a new strategy to simplify its IT processes and give its 4,000 employees and 1,000 external partners seamless, secure access to all the business applications they needed to do their jobs remotely. By leveraging Okta Single Sign-on and Adaptive MFA, the company was able to quickly implement a zero trust security model to protect its data at the individual level, while also providing employees with the flexibility to use whatever devices they wanted. As well as improving productivity and giving employees the freedom to work wherever works best, Okta's ability to enable best-in-class identity and access management practices also helped Euro Garages reduce its data breaches down to zero.

*Source

Step 2

Accelerate your identity-centric zero trust architecture

As many organisations begin their zero trust journeys with a variety of on-premises and cloud applications that are not integrated together, often IT is forced to manage disparate identities across many systems as well as the many applications and services used without IT awareness.

As a result, disparate access control issues create more fragmentation and vulnerabilities for ransomware attackers to take advantage of, and end users often require multiple (and, most likely, insecure) usernames and passwords that are easy to hack. Without visibility and ownership over these fragmented identities, IT and security teams are left with potentially large windows for attackers to exploit access into individual systems.

With identity as your company's new perimeter, however, IAM becomes the central control point across users, devices, data, and their networks. This "identity-first" security is what **Gartner** cites as one of the top security and risk trends of 2021 for its ability to provide greater visibility and control over which users have access to what resources. By adopting an identity-first security model, your organisation can minimise ransomware attacks through compromised credentials, incorrect provisioning, or incorrect authentication by implementing zero trust in the following stages:

At stage 1, your organisation should begin building a unified Identity Access Management (IAM) ecosystem and eliminating poor password hygiene by implementing **Single Sign-on (SSO)** and **Adaptive MFA** for employees to access key resources.

At stage 2, your businesses can adopt additional security best practices by extending access controls to other resources such as APIs and using rich context and diverse factors to better inform authentication decisions.

At stage 3, you will have successfully adopted a full risk-based authentication approach to zero trust, including passwordless and continuous access solutions.

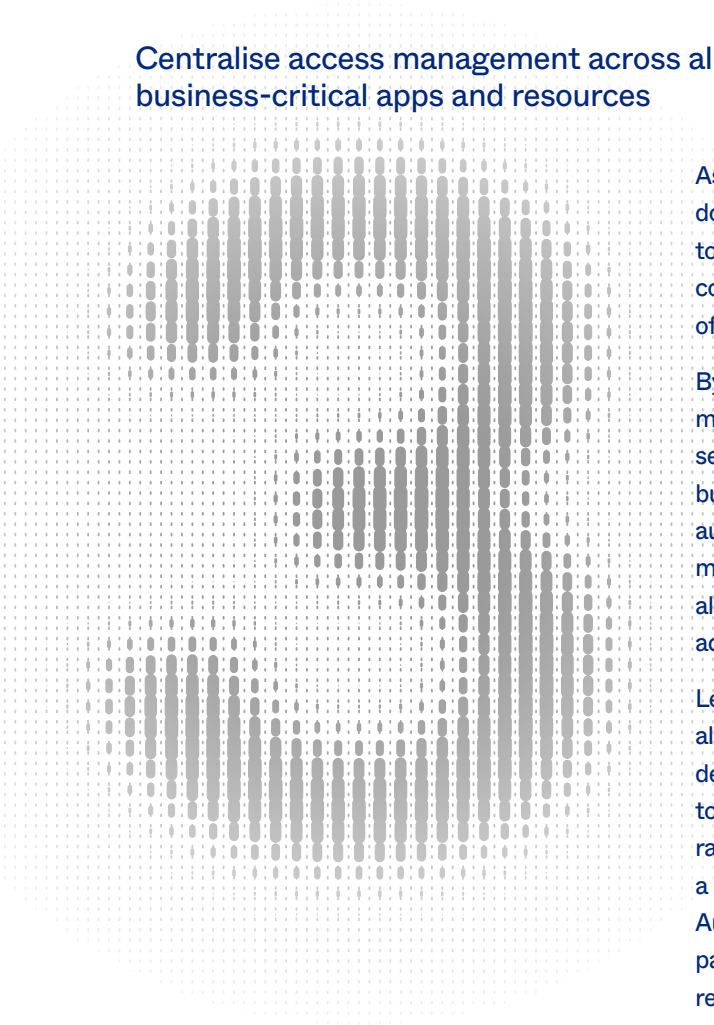
مطارات دبي
DUBAIRPORTS

Okta helped **Dubai Airports*** take its first steps towards a zero trust security strategy and reduced its attack surface by basing security decisions on individual users and the context of their access requests. This identity-first zero trust approach allowed Dubai Airports to protect data at the individual level, while also providing employees with the flexibility to use whatever devices they wanted. With Okta Adaptive MFA protecting both cloud and on-prem apps, Dubai Airports' 4,000 employees, as well as the 100,000 people working on the campus, can work securely without risk of exposing their data to outside threats.

*Source

Step 3

Centralise access management across all your business-critical apps and resources



As well as damaging the user experience and slowing down operations for both IT and Security managers, having to remember multiple passwords for multiple apps also complicates the authentication process and increases risk of exposure to third parties.

By implementing tools like SSO, your organisation can mitigate many ransomware threats by providing one secure, centralised Single Sign-on solution for every business app and platform. As a result, users can authenticate quickly, and your IT and security teams can manage user access much more efficiently and securely, allowing them to isolate and resolve any suspicious activities before they spread.

Leveraging **Okta Lifecycle Management** alongside can also play a huge role in bolstering your organisations defences against ransomware attackers. According to this **CRN report**, the infamous Colonial Pipeline ransomware attack happened when hackers infiltrated a dormant/inactive account that didn't use Multi-factor Authentication. While MFA would have prevented outside parties from accessing the account, LCM would have removed the account and/or its privileges entirely. By automating the provisioning process across every step of the joiner, mover, leaver cycle with LCM, users are only ever given the right access to the right apps at the right time, and dormant accounts can no longer be used by hackers to gain control over your IT network.

Alongside weak passwords and dormant accounts, ransomware attackers are also known for deliberately targeting organisations with visually complex, legacy architectures and poorly designed integrations. Reducing the attack surface of these large, complex networks, however, can be a huge problem for IT leaders, and creates many gaps for cybercriminals to exploit.

With the Okta Integration Network, your business can benefit from thousands of pre-built integrations, using modern protocols such as OpenID Connect that mitigate the risks of password sprawl and allow you to set consistent, dynamic, context-based access policies for all resources, all while making the experience better for your users.

Network Security and CASBs also use cloud traffic and application usage patterns to improve compliance, threat protection, and data loss prevention while security analytics expand your view across cloud, mobile, and on-prem systems to amplify correlation and enforcement opportunities.

As a result, your IT and security teams can easily adopt the latest apps, centralise your user management, and automate access workflows across cloud, on-prem, and mobile applications with minimal effort.

Vinted

To support its long-term growth plan, **Vinted*** needed a platform that could automate manual tasks and improve security without increasing friction for its users. By providing out-of-the-box SSO integration for 95% of Vinted's 394 apps, Okta allowed the company to quickly roll modern Identity out across its network in a fraction of the time and cost it would normally have required. Thanks to the ease of integrating with Okta, Vinted discovered a huge amount of shadow IT such as duplicate subscriptions and services, e.g., three or four apps doing the same thing. This led Vinted to create its own directory of users and applications using Okta's Universal Directory. For the first time, the company had a centralised, fully comprehensive list where it could see exactly who was using their applications and how they were using it.

*Source

okta

Why choose Okta?

Cybercrime never sleeps. That's why investing in an IDaaS provider who you can trust to protect your organisation around the clock is essential for staying ahead of the curve and keeping ransomware at bay.

As well as being **the world's #1 identity platform provider** that's consistently named a leader by major analyst firms and trusted by 13,000+ customers worldwide, Okta also has the broadest set of pre-built application integrations in the industry, with 6,500+ out-of-the-box cloud, on-prem, and mobile apps available in the Okta Integration Network.

Alongside our elite suite of cutting-edge identity products, Okta has built a global, scalable cloud architecture with an average of 99.99% uptime, making our identity platform one of **the most trustworthy and reliable solutions in the marketplace.**

Watch the MFA demo
Learn how to set up strong Multi-factor Authentication to increase network security and bolster your organisation's ransomware defences in this exclusive demo.

Watch demo

Ready to try Okta?
Start your free 30-day trial today.

Start trial