Datasheet
July 2021

How to protect against ransomware attacks with Okta

Ransomware attacks have been all over the news lately. Your organization needs to be prepared, as the average cost of rectifying a ransomware attack is $1.85 million.*

A variety of channels can be used to launch ransomware attacks, including:

- Email-based phishing
- Password abuse
- Unprotected remote desktop services
- Software vulnerability exploits

Once bad actors get hold of a victim's systems, they apply pressure to get the organization to pay up. There is no silver bullet to preventing ransomware attacks, but you can make your organization less vulnerable.

What can you do?

Good security hygiene and an identity-first security strategy are critical. As research firm Gartner noted in its Top Security and Risk Management Trends 2021 report, **"Identity-first security has reached critical mass."**

As a leader in identity and access management, Okta can help protect your organization against ransomware and other pressing threats.

Advance your Zero Trust architecture

Zero Trust ensures that only the right people have the right level of access, on the right device, to the right resource, in the right context.

Start your Zero Trust implementation with multi-factor authentication (MFA), one of the most effective means of preventing account takeover. Use Okta Adaptive MFA to implement contextual access policies that differentiate between normal and abnormal behaviors and between low-risk and high-risk user actions. These signals are often the first indicators of malicious activity.

Together, Adaptive MFA and Zero Trust can stop account takeovers. Adaptive MFA can help stop ransomware actors from gaining initial access, and a holistic Zero Trust architecture can prevent lateral movement if hackers do get in.

Secure access to all your critical resources, including cloud apps, on-prem apps, and infrastructure

Get the freedom to choose the best productivity and security tools for your business, and then make sure all your connections to those tools are secure.

Take advantage of Okta's independent, neutral platform to connect to everything you need. The Okta Integration Network (OIN) has 7,000+ pre-built integrations with all your most-used, best-of-breed apps. It uses modern protocols such as OIDC that mitigate the risks of password sprawl and allow you to set consistent, dynamic, context-based access policies for all resources.

Stay ahead of today's threats with strong, easy-to-use authentication controls

Implement easy-to-use authentication options to reduce the number of misconfigurations and remove the incentive for users to set up kludgy alternatives.

Striking the right balance between employees' user experience and security is key to ensuring productivity while protecting your organization. With Adaptive MFA, you prompt for MFA only during risky authentication attempts using device, location, and network signals—so low-risk users can get to what they need quickly.

Secure your organization with Okta

- 10,650+ global brands trust Okta to secure their digital interactions with employees and customers
- Architected for high resiliency and 99.99% uptime
- The most extensive and audited security controls
- Seamless scalability to meet your needs on demand

Learn more at **okta.com**

*Source: Sophos State of Ransomware Report 2021