Step-up your Essential 8 Maturity Level 3 with Okta

What is the Essential Eight?	2
Who needs the Essential Eight?	3
What is the Essential Eight Maturity Model?	3
Why Okta	4
Essential 8 Mitigation Strategies	4
Apply Multi-factor Authentication	5
Restrict Administrative Privileges	12
Patch applications	16
Patch operating systems	16
Implement Application control	17
User application hardening	17
Backup your data	18
Restrict Microsoft Office macros	18
Configuring your Okta org to meet Maturity 3 Requirements	18
Get Started Today	18
Appendix A: Essential Eight Requirements - November update	19
Appendix B: Okta Factor Matrix	20
Appendix C: Auth0 Factor Matrix	22

What is the Essential Eight?

The Essential Eight is a set of foundational security controls recommended by the Australian Signals Directorate (ASD) as top priorities for preventing and responding to the compromise of networked Microsoft Windows devices.

While the eight recommended controls were borne of ASD's experience responding to compromise of Microsoft Active Directory networks, seven of the eight are broadly applicable to any operating system. Over time, the Essential Eight has been elevated to a yardstick for strong cyber hygiene.

The Essential Eight mitigation strategies are:

1. Patch applications
2. Patch operating systems
3. Apply Multi-factor authentication
4. Restrict administrative privileges
5. Implement application control
6. Restrict Microsoft Office macros
7. Harden user applications
8. Backup your data.

Who needs the Essential Eight?

The Protective Security Policy Framework (PSPF) published by the Australian Government Department of Home Affairs has mandated that all Australian Government entities must be able to demonstrate compliance with **Maturity Level 2** for each of the eight essential mitigation strategies.

The Essential Eight are just as useful to non-Government entities. ASD recommends that all Australian organisations - from small to medium sized businesses through to large enterprises - implement the Essential Eight strategies to mitigate cyber threats.

What is the Essential Eight Maturity Model?

ASD developed the Essential Eight Maturity Model (E8MM) to allow organisations to target a specific level of control maturity during an uplift project before investing in the capabilities required to progress to the next level. This was made under the assumption that achieving a modest level of maturity across all eight controls provides a better security outcome than investing scarce resources in only a few of them.

This document maps the Okta technologies applicable to implementing the Essential Eight to the highest level of maturity, **Maturity Level 3**. In our view, the current threat environment necessitates stronger, phishing resistant multifactor authentication for all users, in order to limit exposure to

- Post-authentication attacks, in which adversaries steal and replay session tokens from the browsers of legitimate users after they sign-in to an online service,
- Adversary-in-the-Middle (AiTM) phishing attacks capable of accessing session tokens from legitimate users,
- Voice-based social engineering campaigns using phishing kits that extract and make use of user passwords and the OTP codes used for multifactor authentication within their period of validity, or that encourage users to approve push notifications.

Given the current rate of identity-based attacks, we also contend that all organisations need to invest in reducing the blast radius from any given account or device compromise. This environment necessitates least privilege access for standard user accounts and a transition to zero standing privileges for accounts with administrative permissions.

Maturity Level 3 of the Essential Eight provides a path toward these goals.

Why Okta

Okta is the world's largest independent, platform-neutral identity provider. Our mission is to safely connect users to any technology.

We view Identity as a fundamental pillar of security. Okta is well positioned to help customers meet all their multifactor authentication requirements, and to help customers take a modern approach to governance and privileged access.

This document also maps out where Okta's approach to identity can support our customers implementation of other Essential Eight strategies.

Essential 8 Mitigation Strategies

The table below presents the Essential 8 requirements where Okta can play a primary or supporting role in helping customers achieve **Maturity Level 3**.

As an organisation, Okta has been assessed against IRAP PROTECTED criteria to provide customers with the highest level of assurance about our own security.

Mitigation Strategy	Role of Okta	Okta Product
Apply Multi-factor authentication	Primary	Auth0 Okta Customer Identity Okta Workforce Identity Okta Privileged Access Okta Identity Security Posture Management Okta Access Gateway
Restrict administrative privileges	Primary	Auth0 Okta Customer Identity Okta Workforce Identity Okta Identity Governance Okta Privileged Access Okta Identity Security Posture

		Management
Patch applications	Supporting	Okta Workforce Identity
Patch operating systems	Supporting	Okta Workforce Identity
Harden user applications	Supporting	Okta's applications have undergone hardening and attestation, as confirmed by Okta's IRAP assessment.
Implement application control	Not applicable	Okta's applications have undergone hardening and attestation, as confirmed by Okta's IRAP assessment.
Restrict Microsoft Office macros	Not applicable	Not applicable
Backup your data	Not applicable	The resilience of Okta's services are attestation to and confirmed by Okta's IRAP assessment.

The eight strategies are sequenced below according to the role Okta can play to help customers meet these requirements.

Apply Multi-factor Authentication

Multifactor Authentication (MFA) is a vitally important tool for protecting user access to resources.

Okta products make it simple to apply MFA to workforce, customer and partner use cases. Users can be challenged at the point of authentication and as a "step-up" challenge to verify transactions or protect access to specific resources.

Collectively, Okta platforms offer the most configurable and extensible MFA use cases than any other platform.

Administrators using the Okta Platform can design authentication flows that apply MFA to an Okta single sign-on (SSO) session, as a "step-up" for access to specific applications, and in response to specific actions and risky behaviors.

Using the Auth0 Platform, web developers can design authentication flows that apply MFA to application access, or that trigger MFA for just about any event of their choosing - such as at the point of verifying a transaction.

Okta also offers the broadest available choice of MFA factors, from traditional methods like SMS and email to advanced options such as biometric authentication. These sign-in methods are available either built into the service or as simple third-party integrations.

Okta MFA controls relevant to required mitigation strategies for **Maturity Level 3** are presented below.

Mitigation Strategy Control Description	**Relevant Okta Services and Products**	**Available Okta Controls**
Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.	• Okta Workforce Identity • Okta Privileged Access • Okta Access Gateway	Okta Workforce Identity allows customers to easily administer MFA challenges to users for access to all a user's resources. This protects access to cloud services, web and mobile applications, devices, networks (via RADIUS integrations) and hybrid applications deployed on-premise (via Okta Access Gateway). Single Sign-On allows administrators to configure secure access to all the third-party resources a user needs via a single set of user credentials, and to protect access to these resources using MFA and other authentication policies.
Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.		
Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organisation's non-sensitive		

data.		
Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data.		
Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.		
Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.	• Auth0 • Okta Customer Identity	Auth0 and Okta Customer Identity each allow customers to easily require the use of MFA challenges at sign-in to a customer-facing application. MFA can also be dynamically applied to verify the identity of a user at critical moments of heightened risk: during transactions, modifications to a user profile, or when an Okta platform or third-party service identifies heightened user or session risk.
Multi-factor authentication is used to authenticate privileged users of systems.	• Okta Workforce Identity • Okta Privileged Access • Okta Device Access	By default, access to the Okta Admin Console and Auth0 Management Dashboard requires multifactor authentication. Okta also provides a range of additional MFA capabilities relevant to privileged users and accounts in downstream applications. This ranges from being able to create strong authentication policies for privileged users on a per-application basis using user attributes or group

		membership, through to dedicated solutions for identity governance and privileged access. Okta Privileged Access provides customers the ability to lock down access to servers, secrets, service and Active Directory accounts. Access to any privileged resource can be gated by multifactor authentication using security policy rules, and administrators can require the use of phishing-resistant factors in these policies. All roles and permissions granted using Okta Identity Governance, and all access secured using Okta Privileged Access, are recorded in the Okta System Log. Okta Device Access provides administrators an ability to enforce MFA for sign-in to user devices on either of the MacOS and Windows operating systems. Administrative access to on-premise servers running agents can be protected using Okta Privileged Access or Okta MFA for Windows Credential Provider.
Multi-factor authentication is used to authenticate unprivileged users of systems.	• Okta Workforce Identity • Okta Device Access	Okta Device Access provides administrators an ability to enforce MFA for sign-in to user devices on devices running MacOS and Windows operating systems.
Multi-factor authentication is used to authenticate users of data repositories.	• Okta Workforce Identity • Okta Privileged Access	Okta Workforce Identity allows administrators to apply MFA to control access to the applications that manage data repositories. Okta Privileged Access can be used to apply MFA challenges during server-level access to servers hosting data repositories and apply MFA to the checkout of credentials used for

		access to these repositories.
Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	• Okta Workforce Identity • Auth0	Okta supports over a dozen MFA factors out-of-the-box (see list in Appendix B). Customers can also choose to "bring their own" custom OTP factor. Auth0 supports multiple MFA factors out-of-the-box (see list in Appendix C).
Multi-factor authentication used for authenticating users of online services is phishing-resistant.	• Okta Workforce Identity	Okta Workforce administrators can configure authentication policies to require a user to sign-in using an MFA factor that meets the NIST definition of phishing resistance for access to any given resource. The range of MFA factors in the Workforce product that can enforce phishing resistance include Okta FastPass, FIDO2 WebAuthn (Passkeys or security keys) and PIV Smart Cards. Okta FastPass delivers a simple passwordless user experience, including zero or one-touch biometric authentication on all major operating system platforms. Okta secures this experience with device-bound, phishing-resistant authentication and device posture enforcement.
Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.	• Auth0 • Okta Customer Identity	Auth0 supports the use of FIDO2-compliant passkeys for access to web and mobile applications. Okta Customer Identity can be configured to require phishing resistant factors such as FIDO2-compliant passkeys or physical hardware keys.
Multi-factor authentication used for authenticating users of systems is phishing-resistant.	• Okta Workforce Identity • Okta Device Access	Okta Device Access provides administrators an ability to enforce the use of phishing resistant MFA for sign-in to user devices on either of the MacOS

		or Windows operating systems via support for FIDO2-compliant hardware keys.
Multi-factor authentication used for authenticating users of data repositories is phishing-resistant.	• Okta Workforce Identity	Okta Workforce administrators can configure authentication policies to require a user to sign-in using an MFA factor that meets the NIST definition of phishing resistance for access to any given resource. The range of MFA factors in the Workforce product that can enforce phishing resistance include Okta FastPass, FIDO2 WebAuthn (Passkeys or security keys) and PIV Smart Cards. Okta FastPass delivers a simple passwordless user experience, including zero or one-touch biometric authentication on all major operating system platforms. Okta secures this experience with device-bound, phishing-resistant authentication and device posture enforcement.
Successful and unsuccessful multi-factor authentication events are centrally logged.	• All Okta products	All Okta products provide customer-facing logs for administrators to troubleshoot access issues and for security teams to monitor for suspicious activity. At minimum, logged events include authentication and application access events, administrator and user actions, session context, and information on the source and target of an action.
Event logs are protected from unauthorised modification and deletion.	• All Okta products	Event logs in Okta products are immutable (unable to be modified).
Event logs from internet-facing servers are analysed in a timely	• All Okta products	Okta publishes APIs for programmatic access to event logs in the Workforce

manner to detect cyber security events.		Identity, Customer Identity Solution and Auth0. Event logs in these products can be streamed to security tools in near real-time. (Okta, Auth0)
Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.	• Okta Access Gateway	Okta Access Gateway provides administrators an ability to protect access to hybrid applications deployed in on-premise environments. Okta Access Gateway logs all user authentication, access, authorisation and administrative events relevant to these applications. Administrators can manage the type and verbosity of logged events. Events can be browsed or downloaded in the management console of the Okta Access Gateway. Administrators can configure log forwarders to push Okta Access Gateway logs to security tools.
Event logs from workstations are analysed in a timely manner to detect cyber security events.	• Okta Workforce Identity • Okta Device Access	All authentication events using Okta Device Access are recorded in System Log. Okta customers also have the option of evaluating device context in authentication policies - in which metadata about a device is evaluated at authentication and included as objects in the resulting event log.
Cyber security events are analysed in a timely manner to identify cyber security incidents.	• All Okta products	All Okta products provide mechanisms for security teams to monitor for suspicious activity. At minimum, logged events include authentication and application access events, administrator and user actions, session context, and information on the source and target of an action.

		Further, Okta emits specific log events when systems detect common security events, such as: • Suspected brute force, password spray or credential stuffing events (ThreatInsight in the Okta Platform and Bot Detection in Auth0) • The use of a known breached password (Breached Password Protection in the Auth0 and Okta Platforms) • Suspected targeting of users by an AiTM phishing proxy (FastPass in Okta Workforce Identity) • Suspected hijacking of an administrative session (location-based session binding, enabled by default in the Okta and Auth0 platforms. • Suspected hijacking of a user session (Okta Identity Threat Protection) • Suspected MFA Fatigue attack (Okta Identity Threat Protection)
Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.	• All Okta products	Okta customers are encouraged to register a "security contact" with Okta. This individual or group is notified in the case of a security incident at Okta or one of its subprocessors.
Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.		
Following the identification of a cyber security incident, the cyber security incident response plan is enacted.		

Restrict Administrative Privileges

Okta Workforce Identity provides customers a unified approach to access, governance and privilege management with the ultimate aim of enforcing least privilege access to all resources.

- Okta Identity Security Posture Management (ISPM) allows for the discovery of highly privileged and poorly protected accounts in cloud services and SaaS applications.
- Okta Identity Governance (OIG) provides the ability to gate requests for access to privileged resources behind customisable approval flows, as well as the ability to centralise entitlement management in downstream applications and perform rapid user access reviews (certification campaigns).
- Okta Privileged Access (OPA) provides customers the ability to lock down access to servers, secrets, service accounts and other administrative resources.
- Okta Workflows allows administrators to automate the remediation of identified issues.

These tightly integrated applications provide a single administration, management and audit point for all aspects of workforce identity.

Okta Privileged Access controls relevant to the required mitigation strategies for Maturity Level 3 are presented below.

Mitigation Strategy Control Description	**Relevant Okta Services**	**Available Okta Controls**
Requests for privileged access to systems, applications and data repositories are validated when first requested.	• Okta Workforce Identity • Okta Identity Governance • Okta Privileged Access	Requests for access to privileged administrative roles in Okta can be subject to customisable approval flows using the Govern Okta admin roles feature bundled into every Okta Workforce Identity tenant. Requests for access to privileged administrative roles in third-party applications can also be subject to customisable approval flows and re-certification campaigns using Okta Identity Governance. Requests for access to privileged systems can be subject to customisable approval flows built-in to Okta Privileged Access.

Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated. Privileged access to systems and applications is disabled after 45 days of inactivity.	• Okta Workforce Identity • Okta Identity Governance • Okta Privileged Access	Okta Privileged Access allows for time-bound access to the secrets required for access to privileged resources. Okta Identity Governance supports time-bound access to roles, as well as recurring certification campaigns that assess user access to any given resource. Administrators can configure campaigns to automatically disable access to a resource based on a defined criteria as one of several remediation options.
Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.	• Okta Workforce Identity	Okta Workforce products support the creation of dedicated accounts for administrative purposes. Authentication Policies can be used to restrict access to administrative resources to only these specific accounts.
Privileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties. Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.	• Okta Workforce Identity • Okta Identity Governance • Okta Privileged Access • Okta Identity Security Posture Management	Okta Identity Governance and Okta Privileged Access can be used to provide time-bound access to roles, systems, secrets and other resources that are subject to approval flows. Access Certification campaigns can also be used to review the use of standing privileges. Okta Identity Security Posture Management can identify unused administrative accounts or rarely used permissions within accounts in downstream cloud applications.
Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from	Not applicable	Application hardening on administrative workstations is best handled by partner solutions.

accessing the internet, email and web services.		
Secure Admin Workstations are used in the performance of administrative activities.	• Okta Workforce Identity	Enforcing separation of workstations for administrative and end user personas is best handled by partner solutions. Okta products can play a supporting role in enforcing separation between administrative and user accounts, given: • Support for restricting access by network zone (IP, IP range, ASN, IP Type) • Support for restricting access using device management and other device attributes • Support for federation of multiple Okta orgs (Okta tenants)
Privileged users use separate privileged and unprivileged operating environments.		
Privileged operating environments are not virtualised within unprivileged operating environments.		
Unprivileged user accounts cannot logon to privileged operating environments.		
Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.		
Just-in-time administration is used for administering systems and applications.	• Okta Workforce Identity • Okta Identity Governance • Okta Privileged Access	Okta Privileged Access provides just-in-time access to privileged resources.
Administrative activities are conducted through jump servers.	• Okta Privileged Access	Okta Privileged Access includes a component called 'Gateways' which can deliver additional infrastructure access controls including: • Support for policy-based access controls for user access to a server via SSH or RDP, including what access controls are required (approvals, MFA) and privilege elevation support for optional

		administrative access • Function as a protocol proxy to sit between end-users and infrastructure to optionally capture and record network activity • Provide bastion and jump host capabilities which allows infrastructure to be protected from direct internet connectivity • Implement Zero Trust use-cases which eliminates end-user devices from receiving unencrypted credentials which could be compromised and used for infrastructure access • Implement audit logging and session recording capabilities for additional visibility into activity
Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.	• Okta Workforce Identity • Okta Identity Governance • Okta Privileged Access • Identity Security Posture Management	Break Glass accounts can be managed by Okta Privileged Access and governed using Okta Identity Governance. Administrators can enforce minimum complexity requirements for any credentials stored in Okta Privileged Access or more broadly in Okta Workforce Identity. Okta Identity Security Posture Management can be used to detect when an account tagged for break glass use is used to access a cloud application.
Memory integrity functionality is enabled.	Not applicable	Memory integrity functions are best met with partner solutions.
Local Security Authority protection functionality is enabled. Credential Guard functionality is enabled.	• Okta Workforce Identity	OS credential dumping is a technique used by attackers that have compromised a host on a Windows network. These attack techniques arise from inherent weaknesses in local directories, necessitating these additional

Remote Credential Guard functionality is enabled.		configuration steps. Okta customers can use Okta-mastered user profiles in Universal Directory to reduce the blast radius from a compromised host.
Privileged access events are centrally logged	• Okta Privileged Access • Okta Identity Governance • Okta Workforce Identity	All privileged access events in Okta are logged in the same System Log as user and API events.
Privileged user account and security group management events are centrally logged.	Not applicable	Security Group Management is a Windows-specific feature and is best managed using partner solutions.
Event logs are protected from unauthorised modification and deletion.	See table above on Multifactor Authentication.	
Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.		
Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.		
Event logs from workstations are analysed in a timely manner to detect cyber security events.		
Cyber security events are analysed in a timely manner to identify cyber security incidents.		
Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon		

as possible after they occur or are discovered.	
Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.	
Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	

Patch applications

Okta Workforce Identity can play a supporting role in ensuring workforce applications, such as browsers, are kept up-to-date.

Okta Device Assurance features methods of constraining user access from Chrome browsers that have not been assessed to meet a minimum security posture. This evaluation relies on the device context gathered from the end-user device by a trusted agent.

Patch operating systems

Okta Workforce Identity can play a supporting role in ensuring workforce operating systems are kept up-to-date.

Okta Device Assurance features methods of constraining user access to resources from end-user device operating systems that meet a minimum version requirement, as well as other trust signals such as disk encryption and device authentication.

This evaluation relies on the device context gathered from the end-user device by a trusted agent. Okta customers can use signals on managed devices via endpoint security integrations with external services for device posture, or on unmanaged devices using Okta Verify.

These trust signals are propagated to Okta during authentication and other user interactions, and serve as metadata for evaluation of Authentication Policies. In doing so,

Okta provides the control required to deny access or to enforce phishing-resistant MFA if the evaluated device posture of the device does not meet their requirements.

Implement Application control

The Essential Eight Maturity Level 3 requires that application controls are implemented on workstations, servers, web browsers, email clients and system folders so as to prevent malicious code from executing in a manner that puts an organisation's data at risk of exposure or damage. These requirements are not met directly using Okta products and are best met with partner solutions.

Okta plays a supporting role in ensuring end users can safely access the resources (applications) entitled to them.

The Okta Workforce Identity provides administrators with control over *who* can access *what* resources using group-based or attribute-based application assignments. Group memberships can be seamlessly managed based on certain attribute based rules or via integration with established sources of trust, such as HRIS systems, enabling administrators to automate joiner, mover and leaver scenarios.

Okta provides reports on user app access, group membership and current assignments to give administrators a concise view of what users can access what applications, when they were granted access, and when they last accessed these applications.

Okta Identity Governance can be used to conduct periodic access certification campaigns to revalidate all application access at regular intervals.

User application hardening

The Essential Eight Maturity Level 3 requires that user tools and applications like web browsers, productivity tools like Microsoft Office and developer tools like Powershell are hardened and or certain features disabled where necessary.

These requirements are not met directly by Okta products and are best met with partner solutions.

Backup your data

The Essential Eight Maturity Level 3 requires regular backups of data and configurations, with a retention period enforced on the basis of business criticality and BCP (business continuity planning). Backups must be secured from unauthorised viewership and their integrity must be protected.

Under the shared responsibility model, Okta is accountable for service availability and has consistently met its 99.99% uptime goal for the Workforce Identity, Customer Identity Solution and for Auth0.

Customers are responsible for backing up their data and configurations. Okta offers customers API coverage for most configuration options, and a range of third party partner solutions are available for using this API access to backup Okta configurations.

Restrict Microsoft Office macros

The Essential Eight Maturity Level 3 requires that all untrusted Microsoft Office macros must be disabled for all users. An exception permitting the use of trusted macros be made for an identified set of business users on a need to use basis.

These requirements are not met directly by Okta products or capabilities and hence are not in scope for this document.

Okta provides the flexibility for organisations to choose the workforce productivity tools that best meet their business and security requirements.

Get Started Today

Given the current threat environment, Okta is the ideal choice for organisations seeking to meet Maturity Levels 2 and 3 for MFA requirements, and those organisations seeking a streamlined approach to meeting Privileged Access requirements.

We urge all organisations to embrace phishing-resistant authentication, which dramatically reduces exposure to most common identity-based attacks, and to invest in posture management solutions that identify gaps in MFA enforcement in downstream SaaS applications and cloud services.

We also believe it's time to accelerate the journey toward zero standing privileges for administrative roles and permissions.

Okta is ready to partner with Australian organisations to help them meet these goals.

Appendix A: Essential Eight Requirements - November update

In November 2023, the Australian Government updated the Essential Eight Maturity Model. The updates most relevant to Okta products concern the types and attributes of MFA factors required for different use cases.

The refreshed set of requirements are listed below.

Requirement	Maturity Level (ML1 / ML2 / ML3)	Previous Version (2017)	Implementation with Okta (Details covered in later sections)	Sample Policy
Composition of factors for MFA must include **knowledge** (something-you-know) and **possession** (something-you-have) factors.	ML1	Factor categories were not prescribed.	Okta Workforce Identity allows the definition of rich authentication policies that can be used to enforce the use of a certain composition of factor types.	Knowledge & Possession
Regular **non-privileged workforce users** of systems must be required to use a **phishing resistant form of MFA** for authenticating to their **devices**.	ML2	MFA was not required for regular non-privileged users. Phishing resistant authenticators were not required.	Okta Workforce Identity supports three forms of phishing resistant authenticators: namely Okta Fastpass, generic FIDO2 authenticators (Passkeys or security keys) and PIV Smart cards. In addition, Okta Device Access extends the same centralised identity engine and user directory used to protect online applications and data to also protect sign in to Windows and MacOS devices using phishing resistant MFA. This brings all identity and	Phishing Resistant

			access policies under a single point of control.	
Regular **non-privileged workforce users** of online services must be required to use a **phishing resistant form of MFA.**	ML2	MFA was not required for regular non-privileged users. Phishing resistant authenticators were not required.	Okta Workforce Identity supports three phishing resistant authenticators: namely Okta Fastpass, FIDO2 authenticators (Passkeys or security keys) and PIV Smart Cards. Phishing resistant authenticators can be enforced at the application level using authentication policies.	Phishing Resistant
Event logs must be available at a **centralised** location and their integrity and availability must be protected.	ML2	Local event logging was acceptable.	With Okta performing the role of a centralised authentication policy authoring and enforcement point, the Okta System Log becomes a centralised, immutable event log for interactive login and API transactions. Each log document is a collection of rich contextual information including the end user's IP address, geo location, device information and more. Okta Log Streaming can be easily configured to export the streaming of logs to an external SIEM for monitoring, analytics, dashboards and longer retention periods.	
Workforce users' access to **all data repositories** must be protected using MFA.	ML3	Only the critical data repositories were subject to MFA access.	Okta views all applications and data as resources for which authentication and authorisation policies can be applied.	Phishing Resistant

Appendix B: Okta Factor Matrix

Authenticator	Available Factors	Available Method Characteristics	Assurance
Email OTP or MagicLink	Possession	User verification	Low
FIDO2 WebAuthn Platform Authenticator	Possession Possession + Inherence (with biometrics)	Phishing resistant Device bound Hardware protected User verification User presence	High
FIDO2 WebAuthn Roaming Authenticator	Possession Possession + Inherence (with biometrics) Possession + Knowledge (with PIN)	Phishing resistant Device bound Hardware protected User verification User presence	High
Hardware Token (Time-bound OTP device)	Possession	User presence Hardware protected	Medium
Passkey (as a primary authenticator)	Possession Possession + Knowledge (with PIN) Possession + Inherence (with biometrics)	Phishing resistant Device bound User verification User presence	High
Okta Verify FastPass	Possession Possession + Inherence (with biometrics) Possession + Knowledge (with PIN)	Phishing resistant Device bound Hardware protected User verification User presence	High

Okta Verify Push	Possession Possession + Inherence (with Biometrics)	Device bound User verification User presence	High
Password	Knowledge	User verification	Low
PIV Smart Card	Possession Possession + Knowledge (with PIN)	Phishing resistant Device bound Hardware protected User verification User presence	High
Security Questions	Knowledge	User verification	Low
SMS, Voice OTP	Possession	User verification	Low
Soft Token (Time-bound OTP Apps)	Possession	User presence	Medium

See this factsheet for a complete breakdown Factor Types & Assurance Levels

Appendix C: Auth0 Factor Matrix

Authenticator	Factors	Available Method Characteristics	Assurance
Auth0 Guardian Push	Possession Possession + Knowledge (with PIN) Possession + Inherence (with biometrics)	Device bound User verification User presence	High
FIDO2 WebAuthn Platform Authenticator	Possession Possession + Knowledge (with PIN) Possession + Inherence (with biometrics)	Phishing resistant Device bound Hardware protected User verification User presence	High
FIDO2 WebAuthn Roaming Authenticator	Possession Possession + Knowledge (with PIN) Possession + Inherence (with biometrics)	Phishing resistant Device bound Hardware protected User verification User presence	High
Passkey (as a primary authenticator)	Possession Possession + Knowledge (with PIN) Possession + Inherence (with biometrics)	Phishing resistant Device bound User verification User presence	High
Password	Knowledge	User verification	Low
Recovery Codes	Knowledge	User verification	Low
SMS, Voice, Email OTP	Possession	User presence	Low
Soft Token (Time-bound OTP Apps)	Possession	User presence	Medium