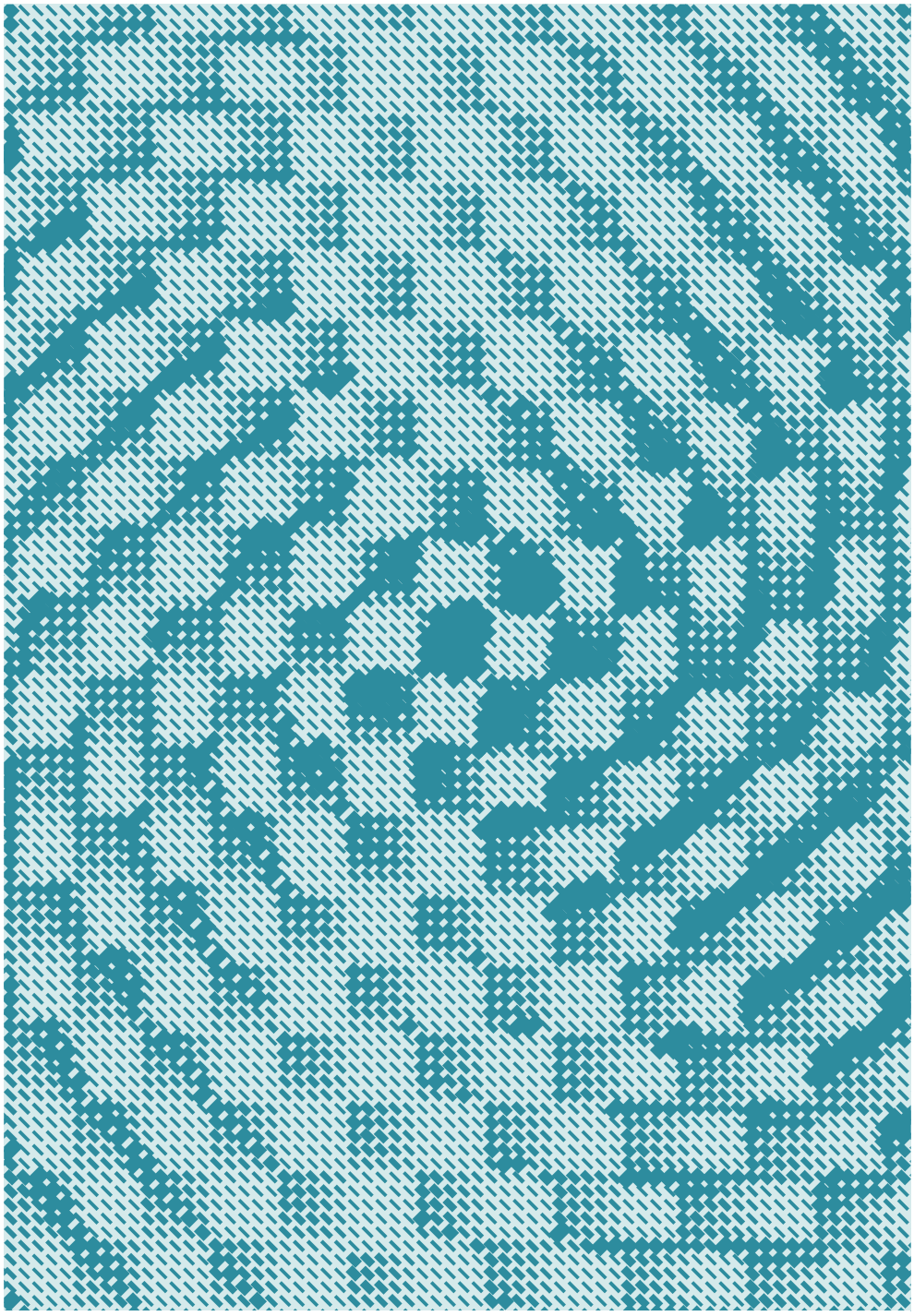
Whitepaper

February 2022

How to make your Essential Eight program a springboard to Zero Trust



Okta Australia Pty Ltd

80 Pacific Hwy, Level 13

North Sydney, NSW 2060

info_apac@okta.com

+61 2 8310 4484

okta

Contents

Executive Summary

Zero Trust – in which users and devices are continuously validated and verified before access to resources is granted – has emerged as the answer to contemporary security challenges posed by widespread uptake of mobile and cloud technologies.

Australian Government agencies, the primary audience for this whitepaper, are currently required to prioritise the implementation of baseline security controls under the Essential Eight program.

This paper sets out to explore approaches to complying with Essential Eight that best support the transition to a Zero Trust future. In particular, we consider potential approaches to implementing multi-factor authentication, given the foundational role of identity in the Zero Trust journey.

We posit that the choices an agency makes to meet today's compliance obligations can have a limiting or an empowering effect on future architecture.

When old models break down

The soaring adoption of mobile and cloud technologies has forced organisations to contend with an environment in which users and workloads spill freely over the boundaries of the corporate network. This penetration of the corporate "wall" is in fact increasingly by choice – cloud services deliver flexibility, rich functionality and cost-competitiveness, making them a necessary and desirable feature of corporate environments.

Many organisations have also leveraged cloud services to remain productive during the COVID-19 pandemic, allowing employees to access corporate applications and data from home. In many organisations, these arrangements look set to continue even in a post-COVID reality.

The implication here is the steady erosion of the network perimeter as a defensive mechanism. The paradigm of an "inside" and "outside", with trusted individuals in the former and untrusted individuals in the latter, cannot be sustained in this environment.

Two key security trends further undermine the perimeter security paradigm. First, the high prevalence of identity compromise reveals that malicious actors are regularly entering corporate networks with valid credentials. Stolen or compromised credentials account for a large proportion of cyber-attacks, according to prominent reports such as Verizon Data Breach Investigations Report.

Secondly, defensive postures can't always rely on the visibility of traffic on the internal network, due to the uptake of encryption standards such as TLS 1.3 and DNS-over-HTTPS.

A new direction is needed for security strategies. Enter Zero Trust.

To account for these trends, a significant rethink in security strategies is underway. IT and security teams have realised that the traditional corporate perimeter, and which side of it a user sits on, is no longer an arbiter or signal of the trust that can be placed in them.

Future security strategies accordingly need to evolve to become “perimeter-less”. Identity – of users and devices – is the new perimeter. Instead of relying exclusively on network location, decisions on whether to grant trust and access become the result of a dynamic assessment of user identity, device posture, the applications requested and the broader context of the request.

These are some of the core ideas of Zero Trust, a security framework first developed by Forrester Research. In a Zero Trust world, access decisions are made under the philosophy of “never trust, always verify”. All users, devices and sessions must be verified before access to a resource is granted and continuously verified for the life of that access.

Zero Trust is a set of principles, not a specific technology. The US National Institute of Standards and Technology (NIST) summarises the goals of Zero Trust as being “to prevent unauthorised access to data and services coupled with making the access control enforcement as granular as possible”[1]. It requires the interchange of trust signals between numerous technologies: operating systems, browsers, endpoint security software and networking devices among them. Ideally, these trust signals are managed using a control plane that independently assigns identity attributes to users, devices, apps and APIs.

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

How does my Essential Eight implementation fit with Zero Trust?

The ACSC's Essential Eight has long been held up as a simple and practical set of priority controls, and help organisations defend themselves against common attack tactics. It includes strategies such as application allowlisting, OS and application patching, blocking macros, user application hardening, restricting admin privileges multi-factor authentication and daily backups.

While it has long been recommended, the Essential Eight will soon be mandated for public sector entities as part of planned changes by the Government to the Protective Security Policy Framework (PSPF)[2].

The ACSC often qualifies that while the Essential Eight is highly regarded, it only sets out to solve a specific set of problems unique to Windows environments. It cannot account for all cyber security threats nor does it address many of the evolving security challenges outlined earlier in this paper. The Essential Eight remains relevant and pragmatic because for the most part, policymakers haven't dreamed any bigger.

The United States, by contrast, is actively seeking that government agencies put forward plans for adoption of cloud services and Zero Trust approach to access. A 2021 Executive Order on cybersecurity put forward by US President Joe Biden requires US government agencies to adopt multi-factor authentication, in the first instance, and Zero Trust architectures in the medium-term[3].

Australian public sector entities do not have to be constrained by the Essential Eight mandate. The Essential Eight model, while rooted in traditional network paradigms, is not mutually exclusive with Zero Trust principles. The decisions an agency makes today to climb the Essential Eight maturity ladder have some bearing on the journey to Zero Trust. Multiple Essential Eight controls directly support Zero Trust. For example, restricting admin privileges relates to a core Zero Trust principle of least privilege, where the lowest possible access is granted to each user or device.

Identity and access is arguably at the core of Zero Trust. This makes the deployment of multi-factor authentication – as required under the Essential Eight – both a logical place and foundational step for Australian organisations in their Zero Trust journey.

[2] https://www.itnews.com.au/news/govt-to-mandate-the-essential-eight-cyber-security-controls-565699

[3] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Identity and MFA – step one to Zero Trust

Given the foundational role played by identity in every access decision, MFA is a logical and compelling place to start the Zero Trust journey. Research also shows that companies where the security team owns identity and access functions are more likely to have a defined Zero Trust initiative in place[4].

Use of MFA has also been steadily gaining broad acceptance, even prior to the Essential Eight mandate. A fifth of global companies say they have now implemented MFA for employees, while 82 percent intend to accomplish that in the next 18 months[5]. Okta also saw a 184 percent increase in the use of its Okta Verify MFA product between February and October 2020.

Announcements by large digital services to mandate MFA are also poignant markers. In May 2021, Google announced it would be making MFA compulsory for all users accessing its services[6]. Salesforce will do the same for customers wishing to access its products from February 2022[7]. Finally, reports highlighting the lack of MFA as being a central factor in recent high profile Australian government cyber incidents (such as the breach of Service NSW in March 2020[8]) have also likely whet the appetite for MFA.

For organisations looking to use MFA as a springboard towards Zero Trust, the recently revised **Essential Eight maturity model**[9] lays out a useful roadmap.

An implementation of MFA should be made with a zero trust future in mind.

For instance, targeting Maturity Level One for MFA may be the most imminently achievable option. This makes a significant impact on an organisation's security - **Microsoft notes that MFA can block over 99.9 percent of account compromise attacks**[10]**.** Any MFA is clearly better than no MFA.

However, many of the Level One prescriptions don't align strongly to Zero Trust maturity. Agencies who pursue higher maturity levels under Essential Eight are far better positioned for a Zero Trust future.

For example, subsequent maturity levels require the combination of multiple factor types (ie. combinations of knowledge-based, possession-based and biometric factors) for access to certain applications). This model of authentication aligns more readily to Zero Trust, where users are presented with step-up authentication requests based on context or risk.

[4] https://www.okta.com/sites/default/files/2021-07/WPR-2021-ZeroTrust-070821.pdf
[5] https://www.okta.com/sites/default/files/2021-07/WPR-2021-ZeroTrust-070821.pdf
[6] https://www.blog.google/technology/safety-security/a-simpler-and-safer-future-without-passwords/
[7] https://help.salesforce.com/articleView?id=000356005&type=1&mode=1
[8] https://www.audit.nsw.gov.au/sites/default/files/documents/Final%20report%20-%20Service%20NSW%20s%20handling.pdf
[9] https://www.okta.com/au/resources/datasheet-australia-and-the-essential-eight-maturity-model/
[10] https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

Identity and MFA – step one to Zero Trust

In a similar vein, when assessing and implementing MFA, IT and security teams should consider the following markers of Zero Trust, and how well the Essential Eight maturity level they are pursuing supports them:

1. Context-based access policies: where signals about the user context, application context, device context, location and network are used to determine what's required to gain access
2. Availability of multiple factor types, including phishing-resistant factors. (Agnostic support for MFA providers may be important in the ability to support various factor types).
3. Continuous and adaptive assessment, where changes in context or risk trigger re- authentication.
4. Support for logging of MFA attempts and protection of logs against unauthorised modification and deletion.

Beyond the immediate security benefits, MFA implementations that align more closely to Zero Trust also minimise friction for users, by prompting for a second factor based on evaluations of heightened risk. As hybrid working arrangements become the new normal, enabling greater productivity through this kind of contextual access becomes a stronger imperative for IT teams.

The Zero Trust ecosystem

While MFA provides a solid starting point for Zero Trust, fulfilling the mantra of “never trust, always verify” goes behind access and authentication alone. Zero Trust also entails the ability to assess and verify device posture, clients, network characteristics, risk posture around detected behaviour and other signals. In short, it is unlikely any single provider can fully solve for Zero Trust – more realistically, an approach that supports and integrates best-of-breed technologies across these various domains will deliver true Zero Trust.

Using Okta for MFA not only applies Zero Trust principles to user authentication, but by supporting integrations with other security solutions, it also provides organisations a managed entry into the extended Zero Trust ecosystem. For example, Okta easily integrates with Endpoint Detection Response (EDR) providers Crowdstrike and Microsoft, as well as various Cloud Web Application Firewall (WAF) providers such as Fastly/Signal Sciences, F5/Shape, and Perimeter X.

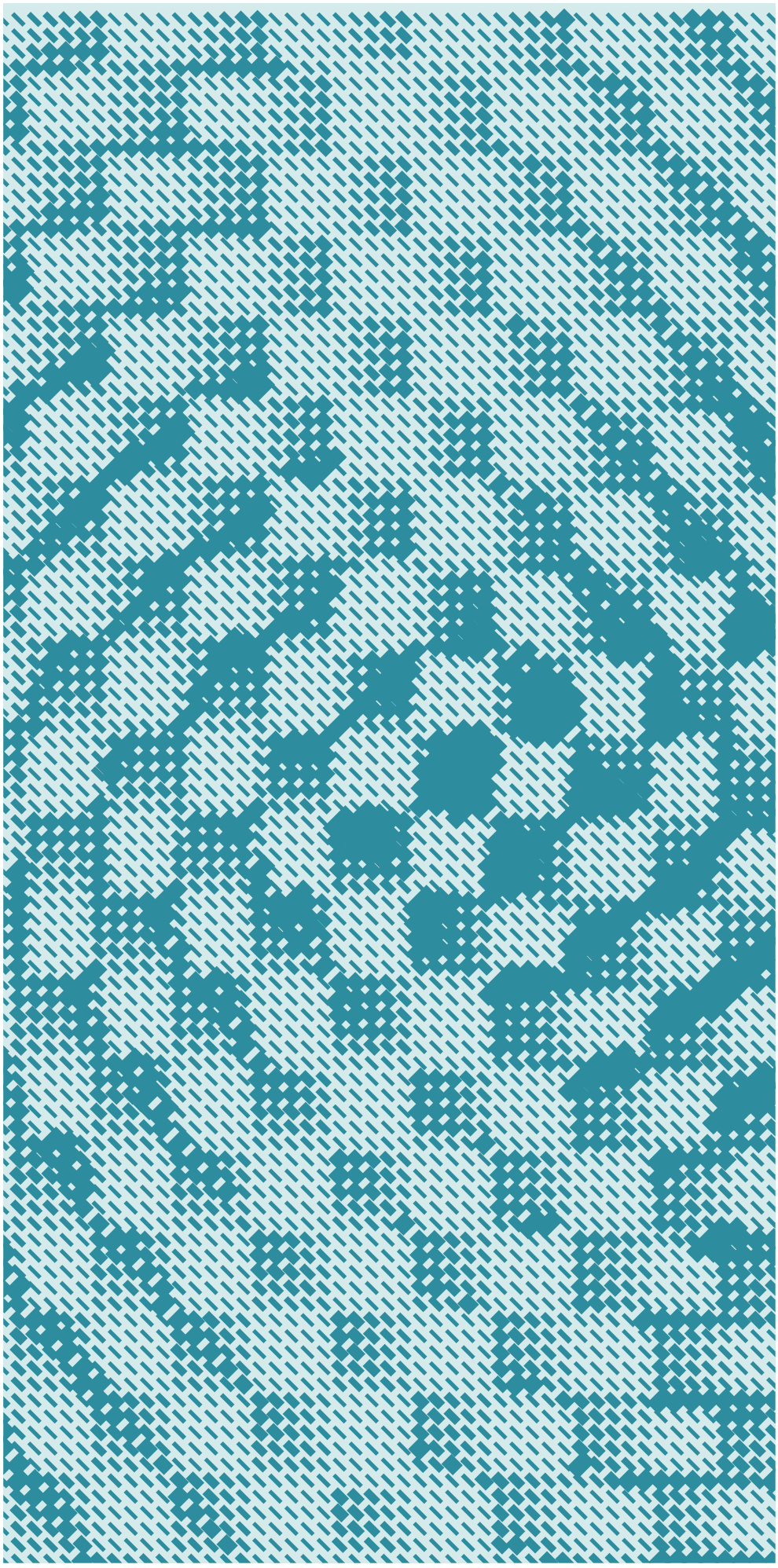
Conclusion

Here are our key questions to ask yourselves to ensure your MFA implementation delivers Essential Eight maturity while also springboarding your Zero Trust journey.

Does your MFA implementation support:

1. Context-based access, where signals about user context, application context, device context, location and network determine access?
2. Use of multiple factor types, including phishing-resistant factors?
3. Continuous and adaptive assessment, where access is continuously verified and changes in context or risk trigger re-prompting for authentication?
4. Logging and monitoring of MFA attempts, and the protection of these logs against unauthorised modification and deletion?

Identity is a logical area to start the Zero Trust journey, and Okta's Adaptive MFA supports both rapid deployment of MFA and the requirements of Zero Trust. For more information on how to get started, **contact us** today.



okta