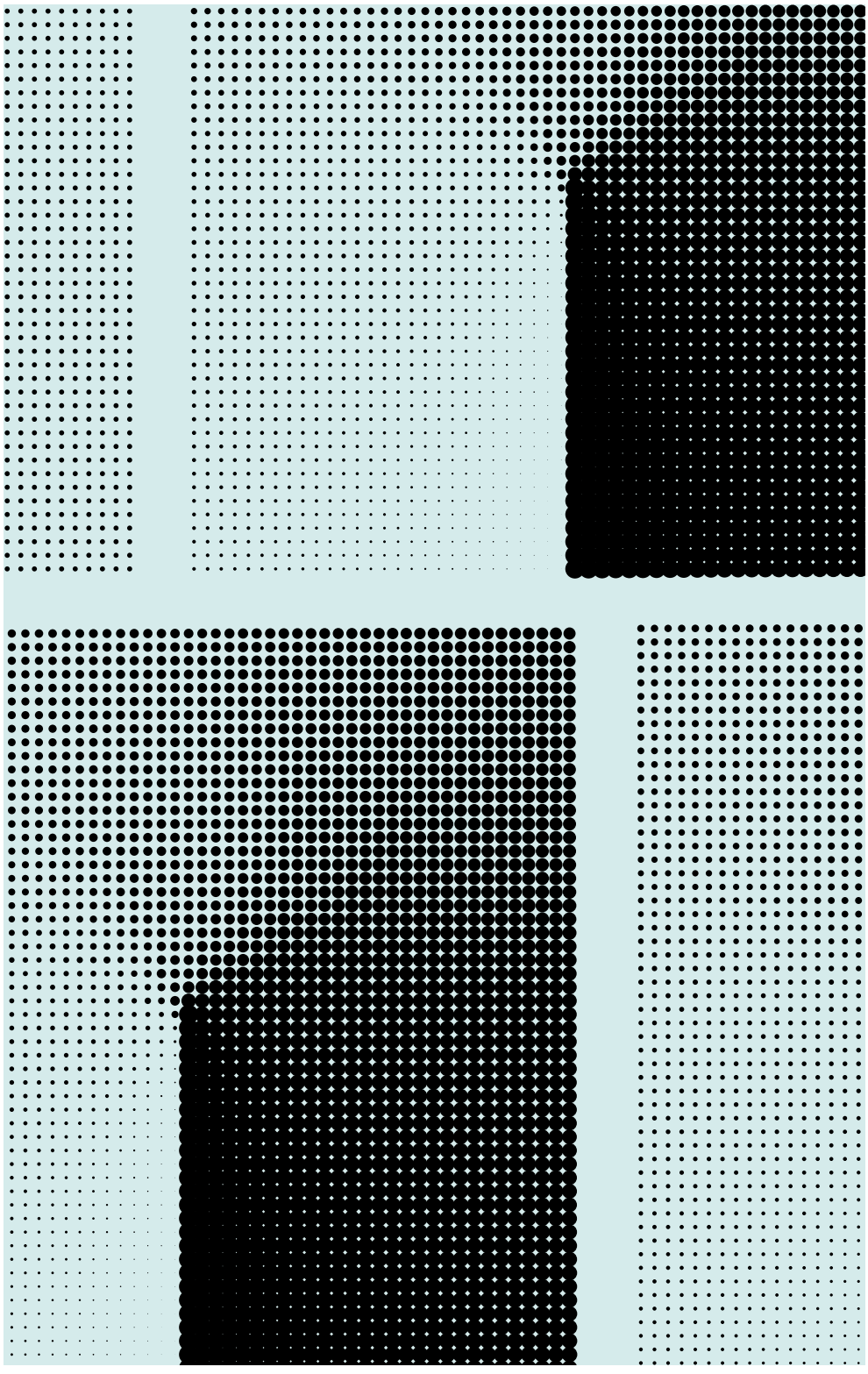
Whitepaper

November 2020

Getting Started with Zero Trust

Never trust, always verify

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871



okta

Contents

Executive Summary

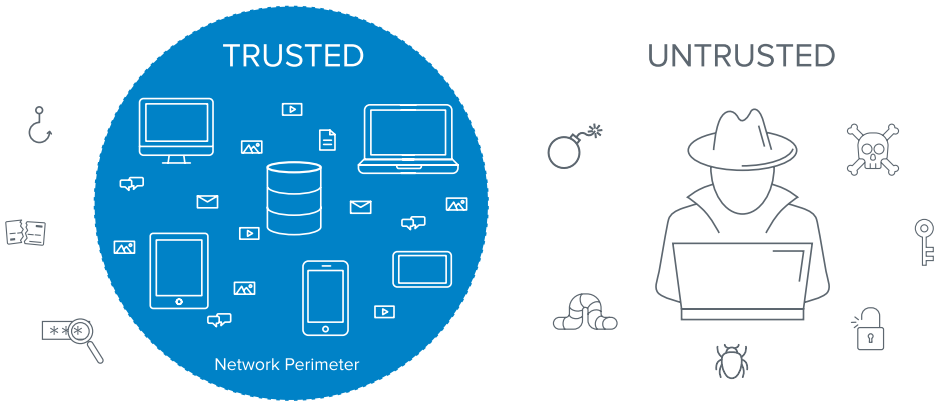
Zero Trust security throws away the idea that we should have a "trusted" internal network and an "untrusted" external network. The adoption of mobile and cloud means that we can no longer have a network perimeter-centric view of security; instead, we need to securely enable access for the various users (employees, partners, contractors, etc.) regardless of their location, device or network. There is no silver bullet when it comes to achieving a Zero Trust security architecture, but identity and access management is the core technology that organizations should start with on their Zero Trust journeys.

Here, we'll explore the shifts in the security landscape that led to the creation of Zero Trust, what the Zero Trust Extended Ecosystem (ZTX) framework looks like today, and how organizations can utilize Okta as the foundation for a successful Zero Trust program now, and in the future.

Challenge: When the Wall Protecting Your Data Vanishes

Traditional security architectures were built with two groups in mind: trusted individuals, able to access everything inside the organization, and untrusted individuals, kept on the outside. Security and IT teams invested in defensive systems that protected the barrier between them, focusing heavily on securing the network perimeter, often with firewalls. While they were successful in building a wall between potential threats and the safety of the corporate ecosystem, this full-trust model is problematic, because when that perimeter is breached, an attacker has relatively easy access to everything on a company's privileged intranet—not to mention the havoc a rogue insider could wreak without even breaching the perimeter.

The "Castle and Moat" Approach to Securing the Enterprise



With today's increased adoption of mobile and cloud technologies, where work is increasingly done outside the safety of a corporate network, the network perimeter becomes increasingly difficult to enforce. In this world, there is no longer a wall around a business' sensitive assets: employees, contractors, partners and suppliers all access data from across the traditional perimeter.

In a cloud and mobile world, more people access more resources and data from more devices and locations than ever before. It only takes one bad actor to cause damage across the entire ecosystem. As a result, organizations can no longer assume trust across any part of the IT stack.

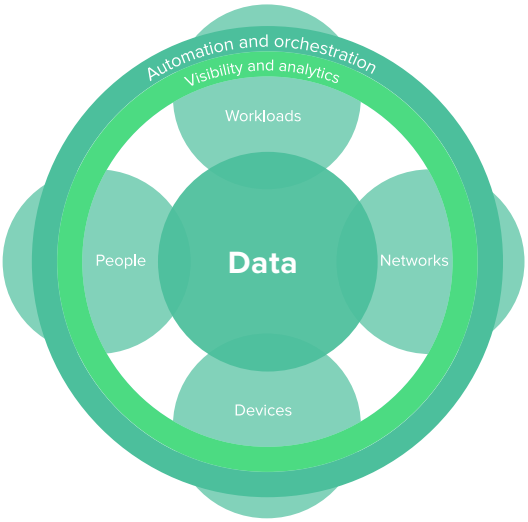
The Next Frontier: The Evolution of Zero Trust

This shift in the security landscape is what led to the birth of Zero Trust. Zero Trust is a security framework, developed by Forrester Research analyst Jon Kindervag in 2009, that throws away the idea of a trusted internal network and versus an untrusted external network; instead, he argued we should consider all network traffic untrusted. In this initial framework, Kindervag focused on revamping the network perimeter and recommended organizations inspect all network traffic in real time, which requires a network segmentation gateway. Specifically, the three principles that made up his Zero Trust include: 1) all resources must be accessed in a secure manner, regardless of location; 2) access control is on a need-to-know basis and is strictly enforced; and 3) organizations must inspect and log all traffic to verify users are doing the right thing.

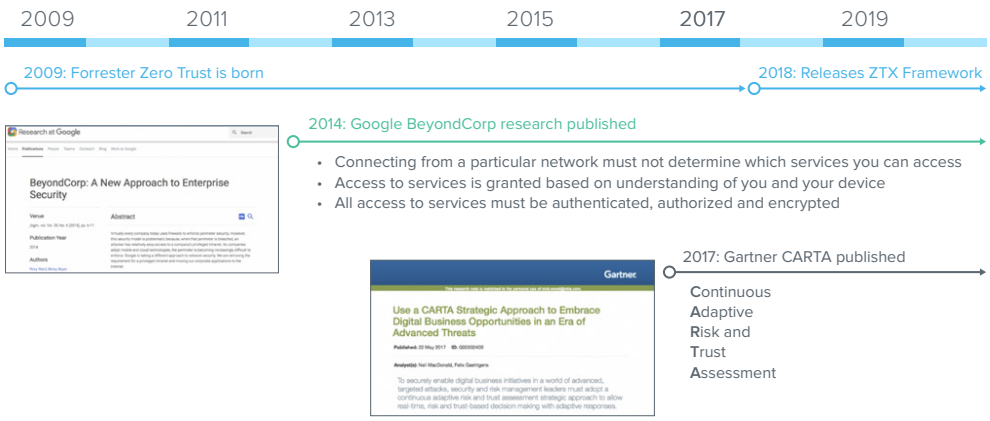
Since 2009, the rise of cloud and mobile has served as a catalyst for evolving Kindervag's original Zero Trust model. Gartner's 2017 CARTA framework[1] echoed Kindervag's Zero Trust framework with an added focus on not just authenticating and authorizing access at the front gate, but continuously throughout the user's experience through an adaptive, risk-based assessment to identify potential threats. Google's BeyondCorp research was published in 2014[2] and today serves as the marquee example of Zero Trust done right at massive scale.

Forrester's evolution of the Zero Trust framework—the Zero Trust Extended Ecosystem (ZTX), led by analyst Chase Cunningham—also emphasizes this shift beyond network segmentation. Cunningham's evolution moves Zero Trust beyond 'Next Generation Firewalls' to 'Next Generation Access,' elevating the people aspect of the model and making command and control over who has access to the network and data key to success. Forrester's team calls out capabilities such as Single Sign-On (SSO) as a critical feature, and notes that Multi-Factor Authentication (MFA) "reduces access threats exponentially."[3]

[1] Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats, Gartner, Inc., May 22, 2017
[2] BeyondCorp: A New Approach to Enterprise Security, Google, 2014
[3] The Zero Trust eXtended (ZTX) Ecosystem, Forrester Research, Inc., January 19, 2018



As the model has evolved, this core Zero Trust concept has stayed the same: in today's security landscape, it's no longer about the network—it's about the people who access your systems, and the access controls for those individuals. This is where identity—and Okta—comes in.



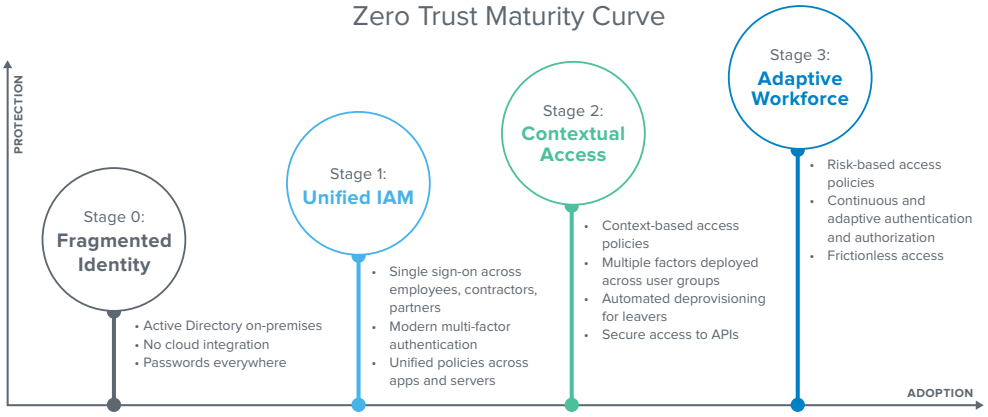
Forrester also recently published new Zero Trust research[4] that further emphasizes the importance of access, naming Okta a Strong Performer in the Zero Trust security market. The report, The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018, included a number of vendors; Okta scored the highest possible score in the evaluation criteria "people/workforce security," "ZTX vision and strategy," and "market approach." The firm writes: "As traditional notions of 'systems' and 'infrastructure' disappear, identity—in all its various forms—becomes ever more important." Due to the critical nature of identity, Forrester sees it as "a core pillar of Zero Trust."[5]

[4] Future-Proof Your Digital Business With Zero Trust Security, Forrester Research Inc., 28 March 2018

[5] The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018

Making Identity the Foundation for Zero Trust

Put simply, the core principle of Zero Trust is to "never trust, always verify." This ensures the right people have the right level of access, to the right resources, in the right context, and that access is assessed continuously—all without adding friction for the user. That Zero Trust nirvana doesn't happen overnight, and as organizations implement Zero Trust architectures, we've seen several stages of infrastructure maturity:



Stage 0: Fragmented Identity

Many organizations begin their Zero Trust journeys with a variety of on-premises and cloud applications that are not integrated together or with on-premises directories such as Active Directory. As a result, IT is forced to manage disparate identities across a number of systems as well as the many applications and services used without IT awareness. For the user, this also means numerous (and, most likely, insecure) passwords. 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.

Stage 1: Unified Identity and Access Management (IAM)

The first step to resolving the security gaps left open by many fragmented identities is consolidating under one IAM system, across on-premises and cloud. This Stage 1 consolidation, via single sign-on (SSO), is critical to managing access and shouldn't be limited to solely customers but instead any user that needs access to a service, including the full extended enterprise of employees, contractors and partners. Layering a second factor of authentication to that centralized, identity access point further helps to mitigate attacks targeting credentials. Additionally, unifying access policies across applications as well as servers, a critical part of IT infrastructure, is key to bringing IAM together into one secure, manageable place for IT.

Thousands of organizations use Okta SSO to unify their user identities. Often paired together are Okta Universal Directory and Okta SSO. Okta Universal Directory is a cloud-based directory service that can serve as a single source of truth for IT organizations, and it serves as an integration point to multiple ADs and other on-premises directory services. Okta SSO makes managing and securing the extended enterprise simpler for IT and eliminates the password proliferation that plagues users. With Okta Advanced Server Access, IT can extend the same access control to the server layer, bringing secure access management to the full breadth of on-premises and cloud resources IT needs to manage.

Stage 2: Contextual Access

Once IT has unified IAM, the next stage in Zero Trust security is layering in context-based access policies. This means gathering rich signals about the user's context (i.e. Who are they? Are they in a risky user group?), application context (i.e., which application the user is trying to access), device context, location and network, and applying access policies based on that information. For example, a policy could be set to allow seamless access to managed devices from the corporate network, but unmanaged devices logging in from new locations would be prompted for MFA. Organizations can also employ multiple factors across user groups to step up authentication based on an understanding of those authentication attempts. Examples might include low risk users without smartphones using one-time passcodes, or high value targets would be required to use hard tokens using a cryptographic handshake to securely authenticate to a service. Furthermore, if a user leaves or changes roles within an organization, automated provisioning ensures the user has access only to the tools s/he needs to do their work (or, in the case of a departure, automatically revokes all access, mitigating the risk of orphaned accounts or latent access after a departure). Finally, these rich access controls should be extended to all technologies used by the workforce, including secure access to APIs that are the building blocks of modern applications but can expose sensitive data to the web.

Many organizations today are already using Okta's contextual access management feature set with Okta Adaptive MFA. By processing a variety of contextual insights about a user, device, location, network and the application or browser a resource is accessed from, the Okta policy framework can serve up a contextual response. This response is based on an organization's risk tolerance, which acts as the first line of defense in keeping an organization secure. For example, if a user attempts to authenticate from their usual corporate laptop on the corporate network, an organization could set a policy that only requires that user to successfully enter a password. But, if the user attempts to authenticate from the corporate laptop in a foreign country on a public wifi network, the policies could require both a password and a second factor. This kind of contextual access benefits both the user and IT/security, only prompting for a second factor during risky authentication attempts, not every time.

Contextual Access Management

Stage 3: Adaptive Workforce

The final stage of Zero Trust implementation extends organizations' focus on authenticating and authorizing access. This means authentication no longer occurs just at the front gate, but continuously throughout the user's experience through an adaptive, risk-based assessment to identify potential threats. This first looks like adding an intelligent, risk-based engine to the contextual responses from Stage 2, going beyond the discrete policies set in the prior stage. IT can now set risk tolerance and allow the risk scoring based on those contextual signals to determine the riskiness of a particular authentication event, and prompt for a second factor based on that insight. That trust is also no longer absolute: this adaptive authentication is continuously monitored for a change in one of those signals, re-prompting for authentication and authorization verification should an aspect of that user's context change. Finally, while security is increased through these intelligent, risk-based access controls, the experience for the end user is ultimately be simplified—allowing for frictionless access and, in cases where IT has set a policy to allow for it, passwordless authentication.

Okta allows administrators to use policies to transform the end user authentication experience, and includes completely removing the password from the authentication flow. Replacing passwords with an alternate factor (such as Okta Verify or a YubiKey) as the primary factor for authentication gives IT administrators choices. They can set risk-based authentication policies that require step-up authentication based on risk tolerance around the varied signal inputs. If confidence is high that the user is who they say they are, that user is only prompted for that first, non-password factor.

And while Okta has a robust policy-driven approach that incorporates context-based signal data, we are continuing to evolve our policy engine intelligence to become much more behavioral in nature. Most organizations today are at ground zero of the Zero Trust maturity curve, but as they continue to adopt the never trust, always verify approach to their IT security, Okta continues to support additional features that enable stronger, simpler access management.

Extending Zero Trust across the Broader Security Ecosystem

Beyond delivering identity as the foundation for a zero trust, Okta also integrates deeply across security solutions to unify your approach to zero trust. Through the Okta Integration Network, Okta invests in and maintains deep integrations across all components of the extended Zero Trust ecosystem including:

netskope	McAfee Together is power.	For data security
paloalto	CISCO	For network security
vmware	Carbon Black.	For device security
CYBERARK	BOMGAR	For workload security
splunk>	IBM QRadar	For analytics
servicenow	splunk>	For orchestration

This expansive category of integrations supports a best-of-breed, vendor-neutral approach that is a signature of the Okta Identity Cloud.

And while intelligently controlling access to corporate resources is the foundation of behavioral monitoring, pinpointing the root cause of a compromise is difficult—especially when the problem is an issue of who, not what. With security analytics and SIEM integrations, Okta enables organizations to take advantage of Okta's rich identity context and user activity and enforce remediation actions against compromised accounts. Okta also integrates with CASBs like Netskope and McAfee, providing organizations with detailed visibility and alerting for continuous checks on risky events during the authenticated sessions. As with Okta's SIEM partners, Okta can provide valuable authentication data to better detect anomalies, allowing CASB services to issue a response back to Okta, which can then revoke access at the identity layer. These are just a couple examples of the ways the Okta Integration Network delivers zero trust for the enterprise.

Case Study: 21st Century Fox

Security has always been a major consideration at 21st Century Fox, the world's premier portfolio of cable, broadcast, film, pay TV, and satellite assets. Reaching more than 1.8 billion subscribers in approximately 50 languages every day, 21st Century Fox is home to a global portfolio of cable and broadcasting networks and properties, including film and television production studios. A few years ago, the attack of another major studio jump started the company's drive to strengthen their security objectives.

Stage 1: Getting started with Zero Trust

21st Century Fox had all the usual perimeter-based security pieces in place, from firewalls to antivirus software. One of the first projects CISO Melody Hildebrandt charged the IT team with was getting all internal Fox users into the same environment. This effort included strengthening authentication, making it easier to see which users are requesting access to which applications, and streamlining identity management processes. Once she had unified the core identity and access infrastructure, she looked to design a new, Zero Trust architecture. This served to counter the credential theft attempts and phishing attacks that are the cause of many of today's headline-driving data breaches. These changes were made without compromising the user experience of the employees, contractors and partners who support Fox network.

Stage 2: Adopting dynamic, contextual access across 21st Century Fox's extended enterprise

21st Century Fox used the Okta Identity Cloud to tackle this Zero Trust approach across their range of workers, with Okta's workforce identity products for their employees, and Okta API products for their partner and contractor ecosystem. The company was already using Okta SSO, Universal Directory, and Lifecycle Management and decided to add Adaptive MFA and API Access Management to the suite.

After getting the core infrastructure in place, moving to a dynamic access model was mandatory for Hildebrandt's team, which is why they implemented Okta Lifecycle Management and Universal Directory. As soon as a user's status changes in Workday, Fox's HR system, UD looks at their attributes, and sorts the user into the appropriate group. Then, Lifecycle Management provisions the tools and level of access the user needs to do their job.

Ultimately, this means users have everything they need on day one, and there's no risk that someone will accidentally access information they shouldn't have. Furthermore, if their credentials are ever compromised, there's less risk that someone else can access sensitive data or content. It also means that when a 21st Century Fox employee leaves the company, or a partner finishes their contract, those loose ends are tied up almost immediately. Access is revoked as soon as their account is deprovisioned in Universal Directory, with no "zombie accounts" remaining. With Adaptive MFA, the company is also able to make smart authentication decisions based on factors like who the user is, what kind of device they're using, where they're working, and which application they're requesting access to. That means the company can maintain high levels of security

> Okta was the foundation that could help us mature to a zero trust model. This was the identity plane where we could introduce so much of the control that we needed to have in order to assess who a person is. So it was actually a way to accelerate, our thinking around zero trust.
>
> Melody Hildebrandt,
> CISO, 21st Century Fox

without forcing employees to take unnecessary steps during the authentication process. As 21st Century Fox rolled out Adaptive MFA, it listened very carefully to its employees and partners, and provided as many factor options as it could, including Okta Verify, YubiKey, Okta Verify with Push, Voice, SMS, and U2F USB tokens.

21st Century Fox's Zero Trust Nirvana: Security + Ease of Use

21st Century Fox's ability to easily and securely provide consumers with content is the ultimate measure of success. One example involves Hot Star, a mobile application that the company offers to consumers in India, which recently surpassed over seven million concurrent live viewers. "That's a pretty amazing achievement for an app that has been around for less than two years, to deliver cricket to mobile users in India for the first time, in a way that's protected against DDoS or against potential credential stuffing attacks, which were significant threats," says Hildebrandt.

With Okta, 21st Century Fox employees and partners are able to focus on what they do best—delivering delightful content to the company's customers—without worrying about external threats. Essentially, they're able to close a large security gap while reducing complexity for users and IT. That means Fox viewers have a lot to be excited about, because the content's only going to get better from here.

What's Next with Okta and Zero Trust

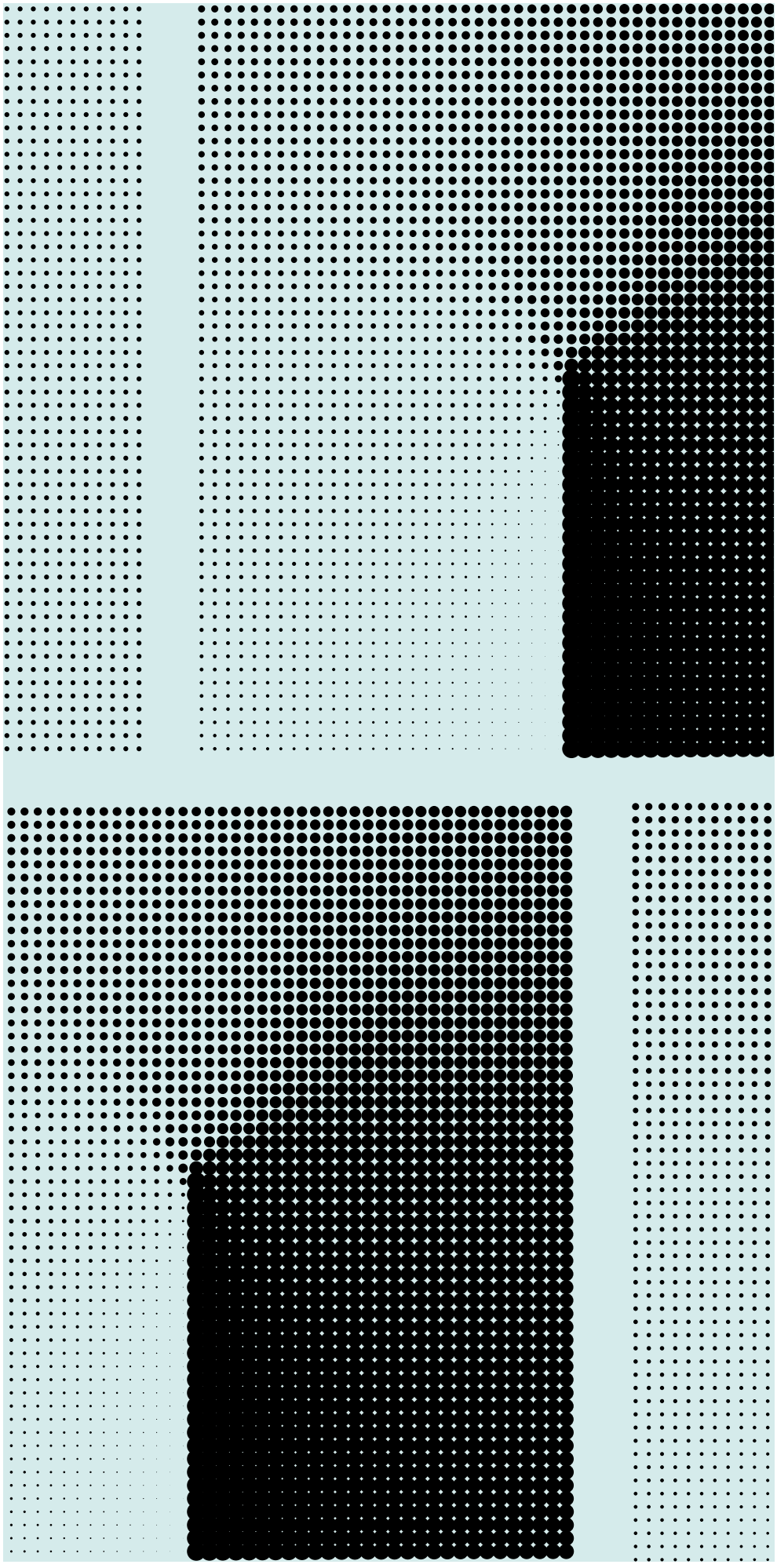
There's no silver bullet for Zero Trust. Some technology vendors will claim otherwise, but organizations want to embrace best-of-breed technologies that allow for greater flexibility and productivity. That's why organizations today look to identity and Okta as the start of their Zero Trust journeys, using the Okta Identity Cloud as the core of their next-generation access strategy—and ensuring that only the right people have access to the right information, at the right time. Never trust, always verify.

Modern Access Management

Okta continues to invest in helping organizations at all stages of this journey. Stay tuned to our corporate and Security blogs (**okta.com/blog** and **www.okta.com/security-blog/**) as additional updates are rolled out to our platform.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 application integrations, Okta customers can easily and securely use the best technologies for their business. To learn more, visit **okta.com**.



okta