



PUTTING TRUST IN ZERO TRUST:

Switching to a more modern security approach



THE WORKFORCE IS EVER EVOLVING

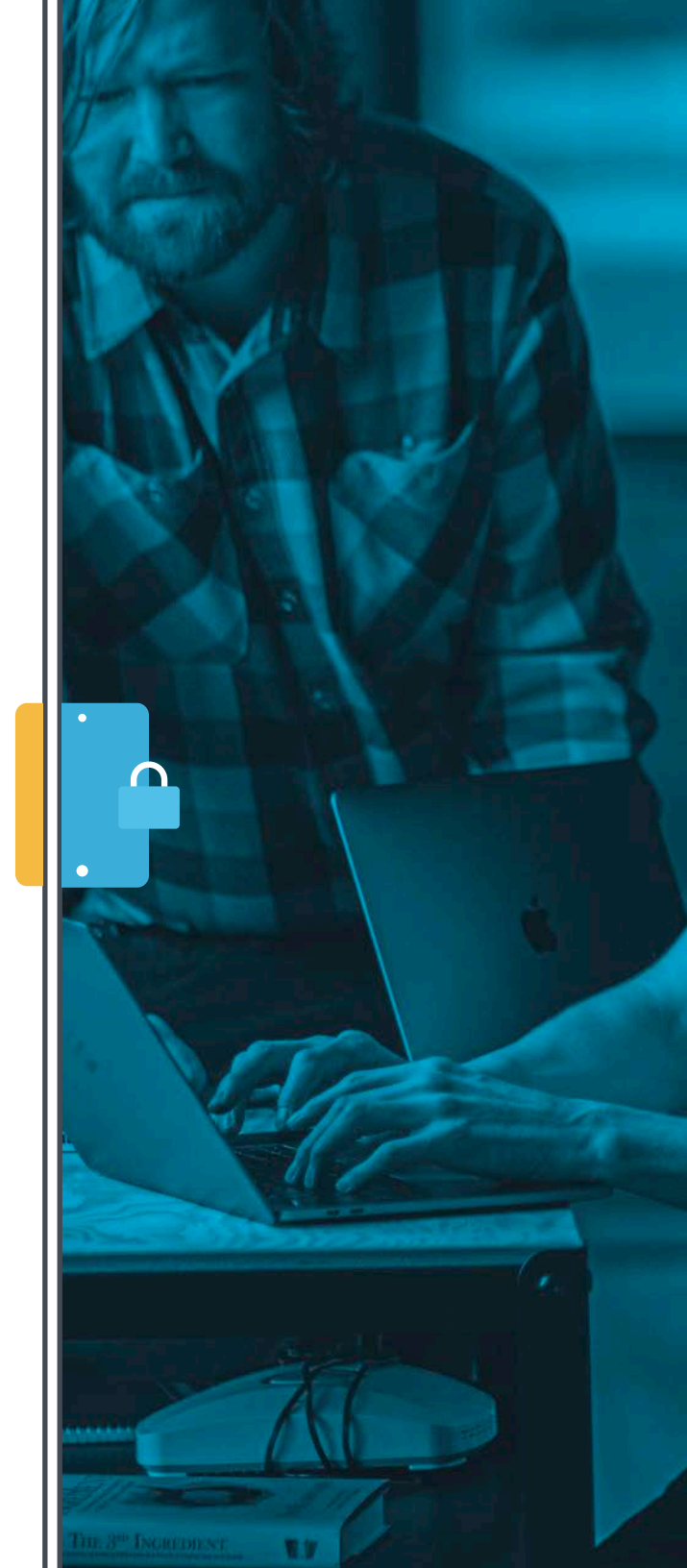
and seeking to combine efficiency and effectiveness in their work, with the global demands of modern business.

Alongside the workforce, technology is advancing to connect people and give them access to everything they need, from anywhere, from most any device. Together, the workforce and technology are allowing the working world to make leaps and bounds at a rate that has companies doing everything they can to keep up with their employees, wherever they are, and support them with their mobile, work needs.

This support demands that IT admins overcome and adjust to the added challenge of keeping data secure, while still allowing complete and frictionless freedom for employees to access everything they need, from anywhere, to stay productive.

Almost overnight, the concept of a corporate network was deemed insufficient in a modern, remote working world. It lacked flexibility for global workforces constantly on the move, led to added cost in the form of help desk tickets without IT available at the ready and increased security risks due to exposed data. With other aspects of technology making many strides forward to accommodate this shift, there had to be a better way for secure access, as well.

Enter Zero Trust, a model for more effective security with an identity-centric approach.



WHAT IS A ZERO TRUST SECURITY MODEL?

Zero Trust, at its core, is not a new concept. In fact, it has been over a decade since Forrester Researcher Jon Kindervag developed the Zero Trust origin concept that throws away trusted internal networks in place of an idea that considers all network traffic untrusted, inside or outside of its perimeters. His concept summarized in another way — **“NEVER TRUST, ALWAYS VERIFY.”**

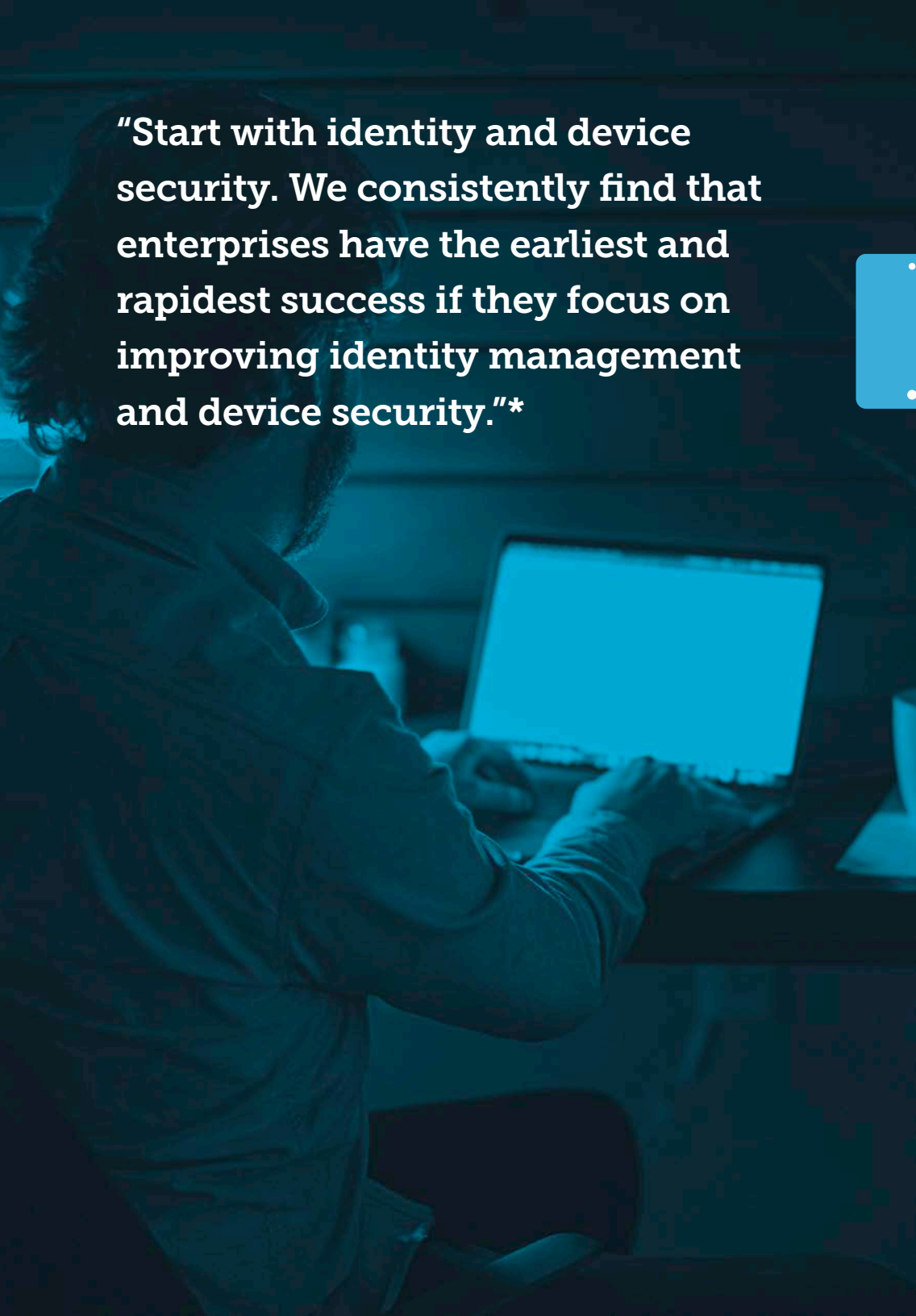
The Zero Trust concept comes with three guiding principles in addition to “never trust”:

- All resources must be accessed in a secure way, from a secure machine, regardless of location
- Access control is on a “need to know” basis correlated to a user’s identity and what that user is authorized to access
- Organizations must inspect and log all traffic to verify users are doing the right things




Over the decade since this initial concept was developed, it has been enhanced and revamped, including Chase Cunningham’s emphasis that the central focus of security should be the users. This notion was turned into an achievable reality with advances to cloud identity, device security, the rise of identity and access management and endpoint security solutions serving as the foundation for modern access control and security.





"Start with identity and device security. We consistently find that enterprises have the earliest and rapidest success if they focus on improving identity management and device security."*



By putting an emphasis on the “people” aspect of security, the focus shifts to who accesses your system, and the access controls they have. This is where a cloud identity provider — like Okta — comes into play and is very important. Leveraging cloud identity allows you to ensure the right people have the right level of access to resources. Those users have authorization to access what they need to be productive, wherever and whenever they need that access — without adding friction to the user.

This treatment of users which ensures confidence in the identity of the person requesting access along with the guiding principles can lead organizations to Zero Trust architecture and success but leveraging the right partners along the journey is crucial.



DELIVERING IMPROVED SECURITY WITH ZERO TRUST

Just as Zero Trust components put people as the focal point, organizations must consider their user's experience almost as much as the security itself. The priorities are no longer

"1. SECURITY 2. USER EXPERIENCE" BUT MORE

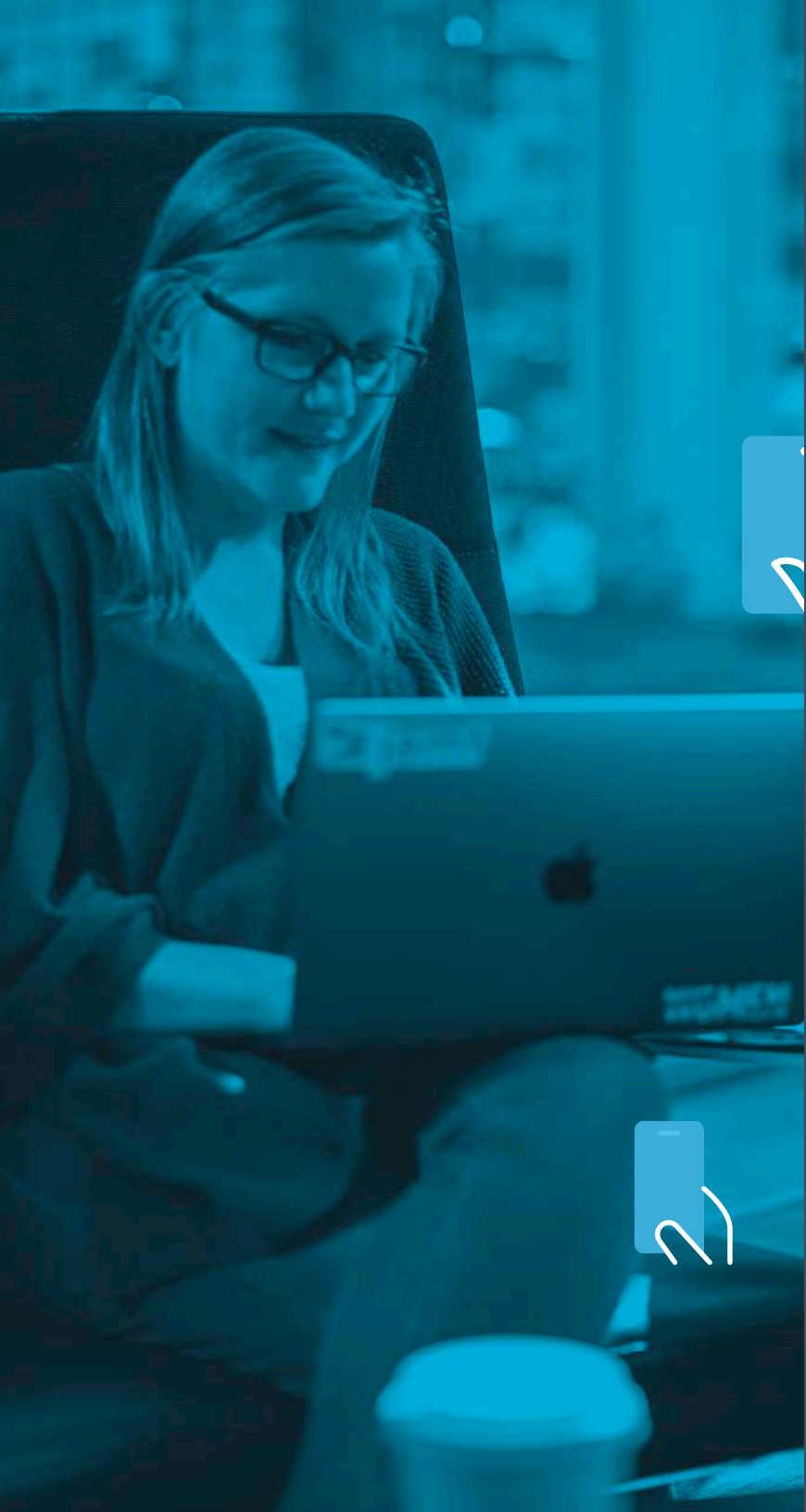
"1A. SECURITY 1B. USER EXPERIENCE".

Unfortunately, in the past, heightened security requirements often meant a heavy burden on employees, forcing them to go through extra steps to gain access - not anymore.

With Okta Identity Cloud and [Jamf Connect](#), organizations can ensure a high level of user trust by unifying identity across apps and devices through seamless single sign-on and offer the option for:

- Provisioning and authentication out of the box
- Keeping cloud-based credentials in sync
- Passwordless access to business-critical apps





Jamf Connect pairs with most mobile device management solutions

but when combined with [Jamf Pro](#) and Okta Device Trust, IT has the ability to prevent an unmanaged, untrustworthy Mac or user from accessing corporate apps and important information. Okta's Device Trust capabilities allow admins to require users to leverage only known and secure devices to access an organization's most important asset, its data. These three combined, means users log in, have their credentials verified and gain seamless, secure access in the form of a triple-layered, security fortress, wherever they set up to work. The office, home or on the road, a user's identity is verified, and they have what they need, and IT knows everything is secure.

Using an Identity Provider like Okta means you can centrally and remotely manage users, groups, passwords and access to resources in a secure manner with the cloud. Using Jamf Connect and Jamf Pro, allows your single sign-on (SSO) to span across all your user's programs, apps and resources which have been securely deployed. This means IT can know there is that high level of security regardless of where a user is accessing resources from. Giving workers flexibility in how they that allows IT to actually increase worker's efficiency and effectiveness while strengthening its security.

jamf | CONNECT

okta

JAMF CONNECT TRIAL

LEARN MORE ABOUT OKTA

EXTENDING TRUST BEYOND THE USER TO THE DEVICE



“**NEVER TRUST, ALWAYS VERIFY**” also includes verification of the device itself. Verifying the user’s identity is a major part of the security battle but verifying the machine from which a user is accessing resources adds an extra layer of armor. [Symantec’s 2019 Internet Security Threat Report](#) found that “one in 36 devices used in organizations were classified as high risk.” Especially with the popularity of BYOD. “The default deny” approach of ensuring a device’s secured status before granting access to critical resources is of utmost importance in a Zero Trust model.

As Venafi states, “[In Zero-Trust environments, each machine needs to have its own identity and there needs to be a way to verify that the machine identity is valid for every transaction.](#)”

Thankfully, Venafi’s Trust Protection Platform integration turns management of TLS-based trust certificates and machine identities into a streamlined, simple process through their new integration with Jamf Pro. With this integration, a multitude of certificates, from any number of certificate authorities, can be automatically issued or revoked for thousands of devices. Configuration profiles and flexible scoping allow stored certificate configurations to be applied to specific groups of alike devices. At the same, Venafi’s platform allows for special custom policies to be managed as well, enabling flexibility for unique certificate use cases. This allows either corporate owned or BYOD devices to all share the same secure baseline level of trust before they’re granted access to critical WiFi, VPN, or other organizational resources. The Venafi integration brings high speed, high scale identity security to your machines and devices, completing the full circle of your Zero Trust efforts.



VENAFI®

LEARN MORE ABOUT VENAFI

START MAKING THE SWITCH TODAY

In a mobile world, what was once achieved by the “corporate network” now has to be capable of being constantly on the move. For some, on-premise Microsoft Active Directory is all they have known. Active Directory (AD) offers identity and authentication, protecting against those outside the directory, but it’s restrictive and not adequate anymore because users have to be on the domain and inside the walls of an office, which no longer works because today’s users and devices interact entirely outside of those walls.

Removing the false sense of security behind a firewall or corporate perimeter allows IT and security teams to evaluate the security of their access controls, devices and resources more frequently. Knocking down the barrier of trust solely based upon being on a corporate network and adapting to modern technologies creates a stronger shield of protection around users and devices, while also enhancing workforce productivity. Examining the risk of access, devices and data opens up the confidence to empower remote employees with the tools they need to be productive. Frictionless, secure access in a streamlined intuitive fashion for users. Just how Apple intended.

Sources:

Forrester, A Practical Guide To A Zero Trust Implementation, Jan 2020
<https://reprints.forrester.com/#/assets/2/53/RES157736/reports>

Venafi, Why Zero Trust Requires Machine Identity Protection, May 2019
<https://www.venafi.com/blog/why-zero-trust-requires-machine-identity-protection>

BEGIN YOUR ZERO TRUST JOURNEY

jamf | CONNECT

JAMF CONNECT TRIAL