PERSISTENT AUTHENTICATION. ALWAYS ON GUARD.

The Ultimate Guide to Next-Gen Authentication

PROXIMIA®

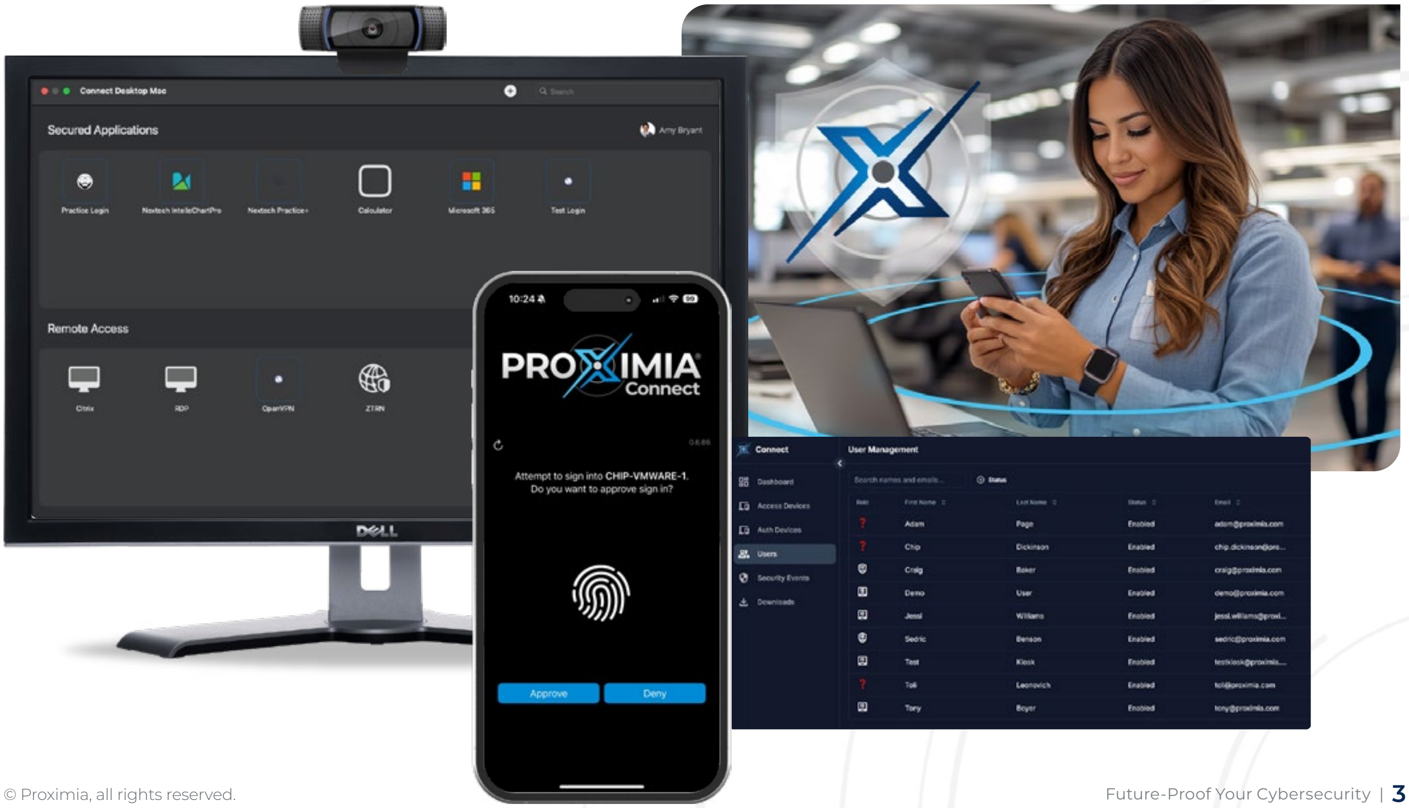
Table of Contents

Future-Proofing Authentication for the Next Generation

Virtually every login today relies on a username and password. It's not convenient, but we've accepted it as a necessary step to protect critical assets. Yet, with near-daily headlines about breaches—both in business and personal lives—it's clear this method is not working.

In 2016, a group of security experts asked a critical question: isn't there a more sophisticated, future-proof authentication paradigm that's easier for users and far more secure?

Proximia took on this challenge and redefined a solution that doesn't just guard a single point of entry with static logins or one-time multifactor authentication (MFA). The true solution required an invisible, persistent security shield that goes beyond traditional one-time logins MFA, is Zero-Trust adherent, and evolves with today's cybersecurity landscape. Proximia delivered on this idea with an innovative solution that continuously verifies who you are, where you are, and what you should have access to, transforming the way we should, and are now able to, protect critical assets and resources.

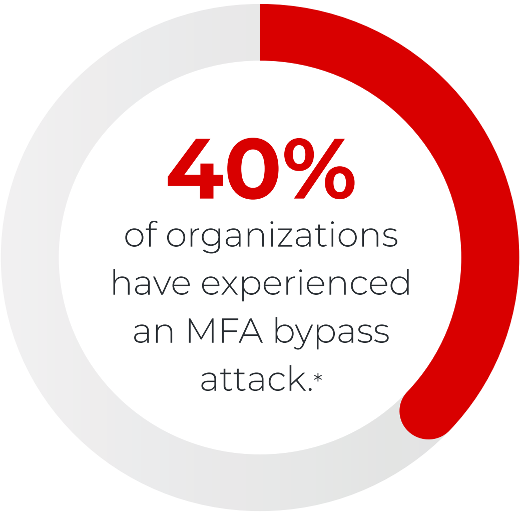


Attempt to sign into CHIP-VMWARE-1.
Do you want to approve sign in?

User Management

Role	First Name	Last Name	Status	Email
?	Adam	Page	Enabled	adam@proximia.com
?	Chip	Dickinson	Enabled	chip.dickinson@pro...
🛡	Craig	Baker	Enabled	craig@proximia.com
🖥	Demo	User	Enabled	demo@proximia.com
🖥	Jessi	Williams	Enabled	jessi.williams@proxi...
🛡	Sedric	Benson	Enabled	sedric@proximia.com
🖥	Test	Kiosk	Enabled	testkiosk@proximia....
?	Toli	Leonovich	Enabled	toli@proximia.com
🖥	Tony	Boyer	Enabled	tony@proximia.com

Why Passwords and MFA Are Not Future-Proof



Passwords shouldn't be easy to guess, yet they must be complex—making them hard to remember and often poorly managed. Whether stored in password vaults or on notepads, passwords are prone to mishandling and theft, creating significant security risks.

To add protection, many organizations turn to Multi-Factor Authentication (MFA), often incorporating one-time bio-authenticators like Face ID or fingerprint scans. While these static forms of MFA add a layer of security by verifying identity at login, they fall short of protecting an entire session. Once initial access is granted, there's no continuous verification, leaving an open door for potential security breaches if the session becomes compromised. Furthermore, traditional MFA processes can be cumbersome, slowing down user workflows and leading to frustration, which ultimately impacts adoption rates. Recognizing these gaps, Proximia developed a more persistent and adaptive security model that continuously verifies identity, securing each session from start to finish without added friction for users.

> ***"The problem in the market that really got me involved was my personal frustration with the proliferation of usernames and passwords. I use numerous websites and numerous applications, and each has their own credentials. And they all have different rules about how to change them."***
>
> \- Kevin Welch, Chairman

**2023 CyberArk Global Identity Security Threat Landscape Report*

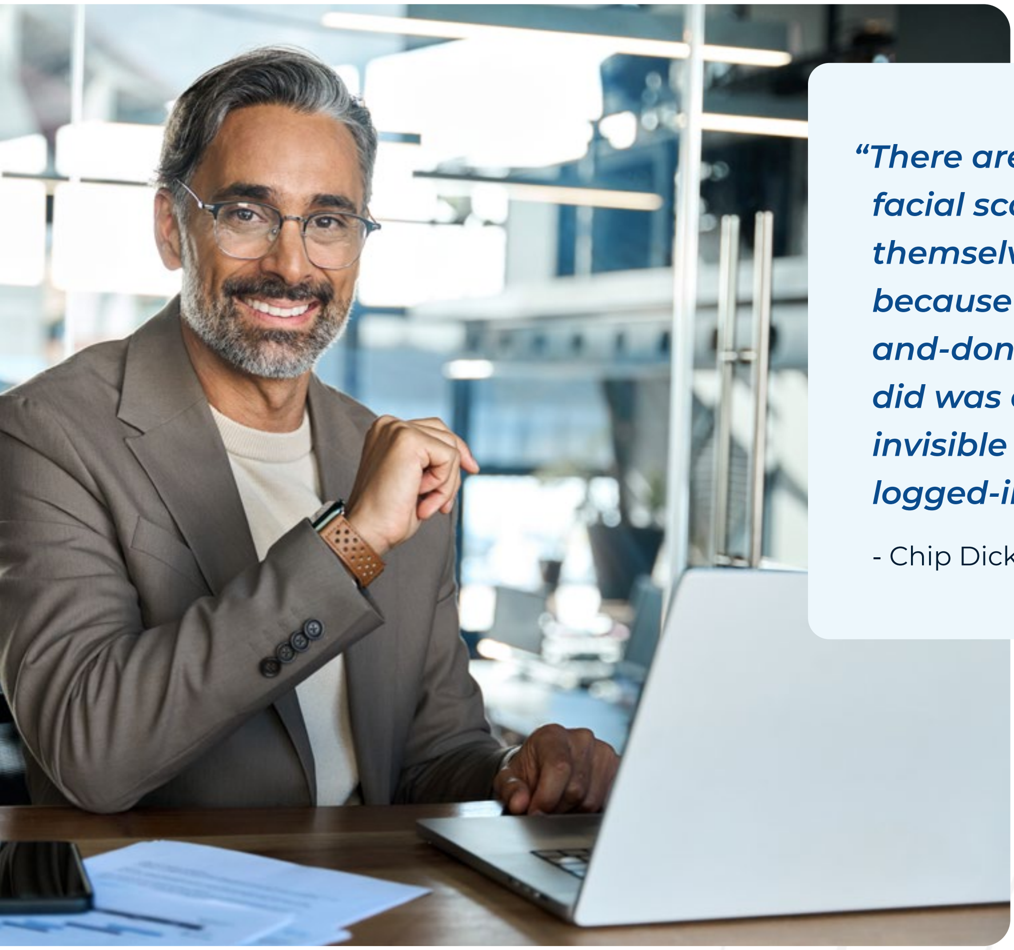
Revolutionizing Authentication for a Zero Trust Future

Security experts know that traditional models of protection no longer suffice. The U.S. government's 2022 Zero Trust mandate emphasized constant monitoring, not one-time verification, operating on "never trust, always verify." Today's solutions need to align with Zero Trust principles to create authentic and sustainable security solutions that go beyond standard MFA. With continuous validation throughout each session, Proximia brings the highest level of protection and user ease.

> ***"We don't trust anything. That's what the mutual trust aspect is – making sure that we constantly authenticate both sides, without user disruption. I know who you are, they know who I am. We believe that we have the only true zero trust solution out in the market."***
>
> - Chip Dickinson, Chief Technology Officer

Dynamic Biometric Triggers for Ongoing Security

Biometric data—such as a fingerprint or facial scan—is used once at login by most systems. Proximia takes it further by using biometric triggers as ongoing verification throughout the session, continually securing access without needing to store sensitive biometric data. Flexible and future-ready, Proximia is agnostic to the specific type of biometric used (e.g., face, fingerprint, or iris). If one biometric method becomes less secure in the future, Proximia can adapt and integrate another, providing flexibility and ensuring continued security.



> *"There are fingerprints, there are facial scans, but those in and of themselves don't fully protect data because they represent a one-and-done login solution. What we did was apply biometric triggers, invisible to the user, throughout the logged-in session."*
>
> - Chip Dickinson, Chief Technology Officer

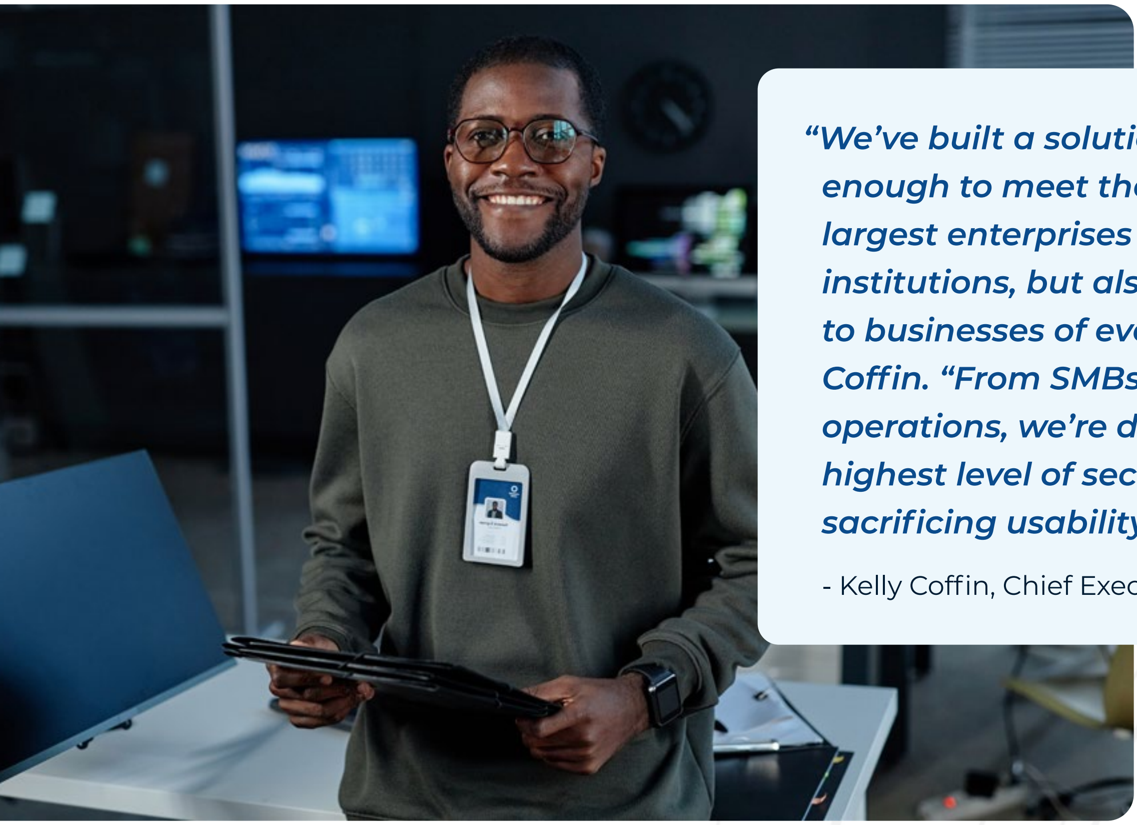
Persistent Security with Dynamic-Proximity and Mutual Trust

Proximia's dynamic-proximity feature continuously monitors whether the user is still near the device, ending sessions automatically if the user moves out of range. This adaptive security ensures that only those in proximity stay authenticated, making impersonation and remote attacks nearly impossible. Proximia authenticates both the user and device, creating a mutually trusted environment that remains secure, providing unmatched safety for modern business environments.

Integration and Accessibility

The Proximia platform can be integrated into existing systems without a total overhaul. Technology implementations are typically complex, requiring business downtime and the burdensome replacement of legacy systems. Replacing those systems with a new security system can be time-intensive – what Proximia CTO Chip Dickinson refers to as "forklift" projects to remove the existing security, install new software, and rewrite existing enterprise code to connect installed systems with the new security system.

Acting as an outer security wrapper, Proximia brings persistent, Zero Trust security to legacy systems without disrupting daily operations. Designed to work with current password databases, Proximia enables a secure transition to passwordless functionality without compromise.



> *"We've built a solution robust enough to meet the demands of the largest enterprises and government institutions, but also accessible to businesses of every size," says Coffin. "From SMBs to large-scale operations, we're delivering the highest level of security without sacrificing usability."*
>
> - Kelly Coffin, Chief Executive Officer

Adaptable to Modern Work Environments

Any modern authentication solution needs to meet the demands of today’s work, providing secure, uninterrupted access across devices—whether on-site or remote. With Proximia, this flexibility extends to both company-issued and personal devices, enabling seamless and secure access regardless of the user’s location. By integrating seamlessly with existing infrastructure, Proximia empowers remote and hybrid workforces with consistent, reliable security.

Key Questions to Ask Any Authentication Solution Provider

To ensure your cybersecurity investments truly protect your business long-term, here are essential questions to consider when evaluating any authentication solution provider:

How Do You Eliminate the Risk of Password Vulnerabilities?	Ask how the solution minimizes or eliminates passwords. Passwordless systems reduce reliance on static credentials, which are often the weakest security link.
Does the Solution Offer Persistent Verification?	Traditional MFA is often a one-time check. Seek out solutions that continuously verify users throughout their sessions to maintain security even after initial login.
Does the Solution Employ Key Security Checks Like Dynamic-Proximity and Mutual Trust for Real-Time Security?	Ask how it ensures that access is adjusted based on the user's location and verified by mutual trust between user and device, offering additional safeguards against impersonation or unauthorized use.
Is the Solution Aligned with Zero Trust Principles?	A future-proof solution should incorporate Zero Trust, which involves ongoing, adaptive verification of both user and device, safeguarding access at every point.
How Are Biometric Triggers Used Beyond Login?	Many solutions use biometrics at login but leave sessions vulnerable thereafter. Look for providers that employ ongoing biometric triggers for continuous security without storing sensitive data.
Can the Solution Support Complex, Mixed Environments with IoT, Legacy Systems, and Modern Applications?	With the increase in IoT devices, diverse on-prem and cloud applications, and legacy systems in many workplaces, ensure the solution integrates seamlessly across these to provide secure, unified access.
How Does the Solution Support Modern, Flexible Work Environments?	Ensure that the solution accommodates both remote and in-office work scenarios, extending its protections to your distributed workforce.

As you evaluate your options, these questions can help you identify an authentication solution that is not only secure today but is also adaptable to tomorrow's cybersecurity landscape. Consider providers that offer comprehensive answers to these points to keep your business ahead of emerging threats.

PROXIMIA®

Your Path to Future-Ready CYBERSECURITY

Emerging from the ever-evolving cybersecurity landscape, Proximia offers a best-in-class authentication solution built to tackle the next generation of security challenges. Their innovative approach is redefining authentication technology and software design across the waterfront and will set a new precedent in enabling organizations to secure and manage access to mission-critical digital assets with greater resilience.

888.795.1480 | proximia.com