Palo Alto Networks Prisma Access and Beyond Identity Secure Workforce

Stop Credential Breaches by Securing Users, Their Devices, Applications, and Data

Benefits of the Integration

- Stop credential-based attacks and the potential of breaches with passwordless, phishing-resistant MFA.
- Minimize the attack surface via continuous validation of device security.
- Protect the organization with continuous authentication disconnecting devices that are out of policy.
- Eliminate user friction often found with MFA with a seamless user experience for Prisma Access customers.

The Challenge

Organizations are challenged by the combination of securing complex network architectures and defending against phishing, ransomware, and credential theft, which includes the ability to bypass traditional forms of multi-factor authentication (MFA).

Modern work requires complex network architectures with on-premises, cloud, and hybrid segments and applications everywhere. Further, password attacks remain the most popular access route for bad actors. MFA bypass attacks are easily facilitated by open-source phishing kits. Phishing-as-a-service subscriptions eliminate the technical knowledge previously required to effectively execute these attacks. The ability to protect users and their many devices while delivering a frictionless user experience remains unsolved.

That begs the question: How do organizations secure applications and data, defend against attacks, and simultaneously delight users?

The Solution

To secure a dispersed and broad attack surface requires a combination of network-centric and identity-centric models with least-privilege security architecture. The integration delivers phishing-resistant, passwordless Zero Trust authentication for a Zero Trust Network Access (ZTNA) environment.

ZTNA secures connections and hides applications from the internet while providing easy access for authorized individuals from the office, home, and on the road.

Zero Trust authentication delivers continuous, risk-based multi-factor authentication that positively identifies users and ensures only devices with a validated security posture gain access with a phishing-resistant, passwordless user experience.

Beyond Identity Secure Workforce

Beyond Identity Secure Workforce prevents credential-based breaches by eliminating the largest sources of cyberattacks and ransomware—passwords and first-generation MFA bypass. By incorporating technology based on the principles of Zero Trust, it delivers robust multi-factor authentication that eliminates passwords, ensures continuous device integrity, and delivers secure and frictionless authentication for your extended workforce, contractors, consultants, agents, and suppliers.

Palo Alto Networks Prisma Access

Cloud adoption and work-from-anywhere mandates have rendered traditional security architectures obsolete. Palo Alto Networks Prisma Access transforms security with the industry's most complete cloud-delivered platform, allowing organizations to enable secure remote workforces. Legacy network security products require significant manual effort to deploy, manage, and maintain, do not scale, and leave gaps in coverage which impact productivity and increase risks. Prisma Access provides more security coverage than any other solution, protecting all application traffic to reduce the risk of data breaches while providing guaranteed performance with leading SLAs to provide an exceptional end-user experience.

Palo Alto Networks and Beyond Identity

Successful security teams deliver on two mandates: Protect the business and enable users. The integration of Palo Alto Networks Prisma Access and Beyond Identity Secure Workforce delivers on the dual mandate.

Secure Workforce's passwordless, phishing-resistant, multi-factor authentication delivers the secure, frictionless login experience users and security teams love. The Universal Passkey architecture delivers secure multi-factor authentication for Palo Alto Networks GlobalProtect cloud service client.

Prisma Access protects the hybrid workforce with the superior security of ZTNA 2.0 while providing exceptional user experiences from a simple, unified security product. Purpose-built in the cloud to secure at cloud scale, only Prisma Access protects all application traffic with best-in-class capabilities while securing both access and data to dramatically reduce the risk of a data breach.

The integration secures the initial authentication through the network to the application and data while providing a superior user experience.

Use Case: Passwordless, Phishing-Resistant Authentication Reduces Breaches and Delivers Frictionless Authentication

Challenge

Current authentication methods using passwords or first-generation MFA solutions no longer protect the organization's network, applications, or data. Proof points include recent basic attacks on passwords like phishing and MFA methods like MFA bypass and fatigue attacks. Stronger security is required.

Solution

Organizations seeking end-to-end security coverage for the extended workforce, including full-time employees, contractors, and suppliers, can provide least-privileged access and frictionless authentication. Starting at the point of initial authentication, Secure Workforce delivers passwordless, phishing-resistant authentication for GlobalProtect cloud service client.

Prisma Access protects all application traffic with best-in-class capabilities while securing both access and data. The result is a minimized risk of breaches.

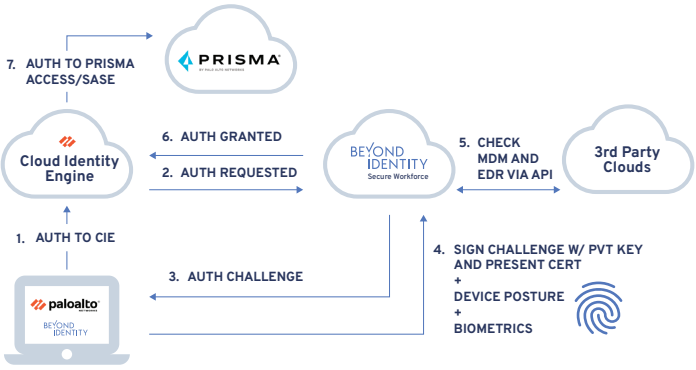

Figure 1: Prisma SASE and Beyond Identity authentication flow

About Beyond Identity

Beyond Identity is the technology innovator in FIDO2 certified multi-factor authentication, delivering a passwordless, phishing-resistant and frictionless user experience that prevents credential breaches and delights users. Companies like Snowflake, Unqork, and Roblox rely on Beyond Identity's cloud-native platform to advance their zero trust strategies. To learn more visit beyondidentity.com.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. For more information, visit www.paloaltonetworks.com.

paloalto NETWORKS | BEYOND IDENTITY

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

prisma_pb_beyond-identity-secure-workforce_031323