Palo Alto Networks Prisma Access and Thales SafeNet Trusted Access

Gain Simple Zero Trust Access to Remote Internal Resources with Palo Alto Networks and Thales

Benefits of the Integration

Palo Alto Networks and Thales offer a joint solution that:

- Prevents unauthorized access by providing the right method and level of complexity for each authentication journey
- Reduces login burden for end users and calls to the help desk with Smart SSO
- Speeds up deployment and reduces overhead with automated token life cycle management and unlimited software tokens
- Ensures compliance with security regulations and avoids penalties by complying with MFA mandates
- Enables Zero Trust with centrally managed user access and security policies across on-premises and multicloud environments
- Reduces the attack surface and stops threats with consistent security policies
- Provides greater visibility by eliminating remote access blind spots

The Challenge

All users and their authentication needs are not equal. Complicated authentication needs are increasing as regular users and privileged users access cloud-based apps and onsite resources from a variety of devices and locations. Phone-based authenticators seem like an easy fix until you encounter environments where a phone is not allowed, there is no connectivity, employees are unwilling to add a corporate app to their personal phone, the data is highly sensitive, or regulatory requirements require a more secure connection.

The reality is that today's users work remotely, access up to 27 apps each day, frequently access hybrid deployments, and they forget passwords. Forgotten passwords increase calls to the help desk, and weak or stolen passwords lead to the majority of data breaches. Passwords are no longer enough. Disparate IAM systems add complications when they operate as silos by increasing administrative costs and complexity and creating inconsistent user experiences.

Thales SafeNet Trusted Access for Complex Authentication Journeys

Thales SafeNet® Trusted Access (STA) is an authentication-centric AM solution that handles complex authentication journeys and plays well with others. STA simplifies the user experience by balancing risk and convenience, and supports multiple authentication journeys by supporting multiple work environments and devices. To accelerate user acceptance while maintaining security, STA can rigorously enforce access to sensitive applications and take a lighter approach with less-sensitive data. CISOs recognize that all users and their authentication needs are not equal. To support diverse BYOD and remote employee use cases, enterprises support multiple authentication journeys. No single technology can support all the journeys, so STA supports a range of technologies for authentication journeys ranging from simple to complex. STA overcomes IAM silos through integrations with existing IAM systems. Additionally, STA reduces help desk costs by providing end-user self-service and administrative management capabilities.

Palo Alto Networks Prisma Access

Prisma® Access by Palo Alto Networks is a secure access service edge (SASE) solution that provides network connectivity and consistent security for any device at any location. It simplifies networking and security, replacing conventional point products such as firewalls, proxies, secure web gateways, remote access VPNs, CASBs, DNS security solutions, and more. Prisma Access supports the Zero Trust model for network access, driving identity-based access controls to applications while maintaining full visibility and inspection of network traffic. Prisma Access Next-Generation CASB addresses your CASB needs and provides deep visibility into SaaS risks, data protection, leakage prevention, data governance, compliance assurance, advanced threat prevention, and more.

Palo Alto Networks Prisma Access and Thales

Enable your users to access cloud apps and onsite resources with a Zero Trust approach from Palo Alto Networks integrated with Thales user authentication that is contextual, adaptive, and convenient. Prisma Access provides network connectivity and security while STA enforces authentication at the access points. Regardless of their physical location and device, employees and third-party contractors can access internal cloud and legacy resources. Enterprises can effectively migrate securely to the cloud, prevent breaches, and simplify regulatory compliance by using the Prisma Access Zero Trust approach and STA policy-based conditional access, rigorous SSO, and a broad range of authentication methods. Additionally, STA lets enterprises centrally manage and secure access to enterprise IT, web- and cloud-based applications, and create an audit trail. By combining Prisma Access with STA, businesses can meet strict compliance requirements and be audit-ready.

Use Case 1: Security at the Access Point

Challenge

The rapid adoption of remote work, cloud services, and BYOD massively increases enterprises' exposure to phishing and other attacks.

Solution

STA protects businesses from unauthorized access and reduces the risk of a data breach at the access point. STA enforces access policies and the appropriate level of authentication to assess human users, applications, APIs, and connected devices attempting to connect to Prisma Access. Combine STA with Prisma Access to comply with MFA mandates and enable authorized users to securely access both cloud-based and on-premises applications and data.

Use Case 2: Maintaining a Positive User Experience with Remote Work

Challenge

CISOs are often met with the challenge of balancing security with user experience. This challenge, coupled with shadow IT and hybrid IT, makes the balance even harder to achieve. Organizations need a solution that helps them enforce the right level of security for the right user and use case.

Solution

In conjunction with the Zero Trust capabilities of Prisma Access, STA offers flexibility to the IT team to configure granular policies for different groups of users. A remote administrative worker, for example, can be configured to use an OTP token to gain access to a privileged application, whereas a remote sales executive could use a Thales FIDO2 token or a mobile authenticator like MobilePASS+ to gain access to a customer relationship management (CRM) application. This adaptive SSO capability can help IT create the right user experience for each use case and user group.

Palo Alto Networks and Thales Integrations

Product integrations between Palo Alto Networks and Thales include:

- Prisma Access and Thales SafeNet Trusted Access
- Cortex® XSOAR and Thales SafeNet Trusted Access
- NGFW and Thales SafeNet Trusted Access
- NGFW and Thales Luna Network

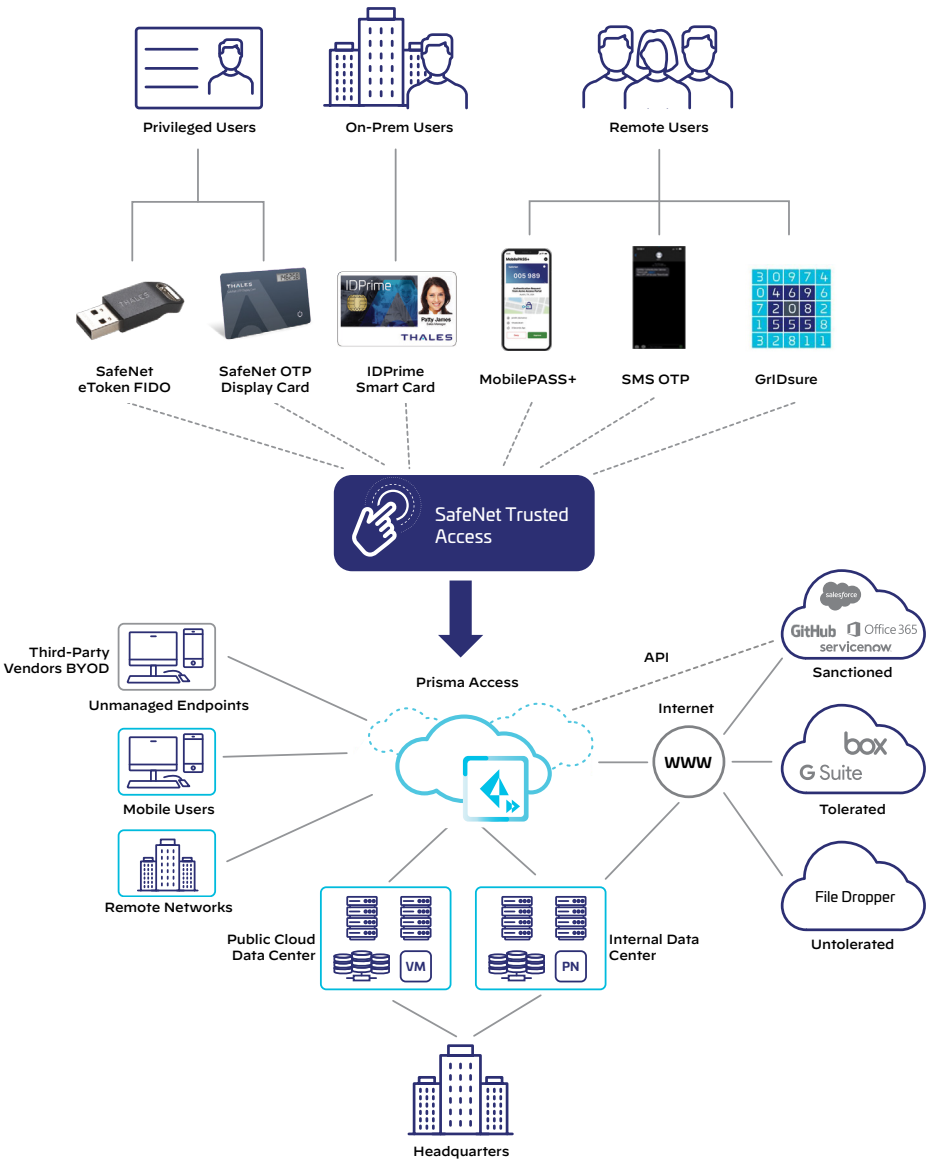

Figure 1: Palo Alto Networks and SafeNet Trusted Access integration—strong support for every authentication journey

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation. Decisive technology for decisive moments. For more information, visit https://cpl.thalesgroup.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 | THALES

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