PRISMA ACCESS
BY PALO ALTO NETWORKS

Secure the Cloud: Zero Trust Cloud Security

Overview

Access controls are the starting point for good security because unnecessary access is never a good thing. Excessive levels of access increase exposure to risk because a person (or bot) may stumble upon something he or she shouldn't see. In the worst-case scenario, excessive levels of access can provide just enough room to use an exploit or steal data. Even if someone with no ill intent obtains data he or she should not otherwise see, it might set off a data breach notification protocol due to access from an unauthorized party.

Limiting access also reduces the attack surface area, making it far more difficult for attackers to advance on their objectives. It also makes other protection more effective because organizations can reduce the number of possible attack vectors and focus on the things that matter. For example, data protection controls are more effective when all traffic to an application is inspected.

Unfortunately, with the cloud, all traffic is not inspected, and unnecessary levels of access are the norm. With the growing number of applications ported or moving to the cloud, one might expect that cloud teams have well-established access practices in place. However, given the rapid adoption of the cloud, diverse cloud applications and platforms, and different DevOps teams building applications, it's quite common to see fragmentation in cloud access. The problem gets worse as cloud adoption grows and the responsibility for security within cloud environments spreads across different functional groups.

Borrowing lessons learned from the excessive levels of trust found in enterprise networks, the principles of Zero Trust can help—but how does an organization implement Zero Trust in the cloud?

Challenges with Cloud Access Today

There is no shortage of systems that implement some type of access control today. The problem is that none of them are designed to handle the access problem across the wide variety of cloud architectures.

Access Control at the Network Edge

The conventional model for controlling access is to simply limit who can connect to a given network, as with remote access virtual private networks (VPNs). Although this is sensible for applications in private clouds (internal data centers), it is an inefficient network path to use for the public cloud and software as a service (SaaS). Therefore, most organizations use remote access VPN for temporary, ad hoc connectivity to internal resources while avoiding it altogether when private cloud access is not necessary.

Authentication at the Application

The other conventional approach is to modify/replace local authentication within an application itself with federation to centralized identity management. Federated authentication has also greatly simplified ease of use for applications enabled in this manner. The challenge, however, is that the not every application can be enabled to support the enterprise identity management platform. In addition, even when front-door access to the application is secure, other vectors—such as the application programming interfaces (APIs)—must still be protected against exploits and abuse from parties who do not have valid credentials.

CASB Proxy

Proxying cloud applications through a cloud access security broker (CASB) is another approach to gating access. Proxies establish network boundaries between users and applications, creating the foundational separation that limits access. However, CASB proxies are often used to support some web-based applications while other teams need to deploy software-defined perimeters (SDPs) and VPNs to handle the ones that are not supported.

Software-Defined Perimeter

In the wake of the limited uses for remote access VPN, some vendors are applying a mix of brokering and tunneling to cloud-based applications. The SDP market blends the principles of the proxy for network separation along with end-to-end tunnel for VPN. The market for SDP is fragmented between those that use a client to tunnel to the resource and those that are clientless with a browser-based proxy, both of which offers support for some applications while omitting others. To date, many SDP vendors focus on access control functionality with little to no threat or data protection, thus posing risk to both applications and users.

Zero Trust for the Cloud

Many existing technologies, as stated above, are based on sound ideas but only solve a slice of the problem space. If we take a lesson learned from the past, the principles of Zero Trust provide a good starting point for a more comprehensive approach.

By establishing Zero Trust in their cloud environments just as they would in their own networks, organizations can gain visibility, reduce the attack surface, prevent known attacks, and detect and prevent unknown attacks. An architecture based on Zero Trust maintains separation between users and all applications, establishing the identity of a user to enforce policy on who can access a given resource as well as stop threats and control the movement of data.

To achieve Zero Trust in the cloud, an organization must be able to:

- Separate users and applications
- Identify users and devices
- Enforce threat prevention and data protection

Prisma Access for Zero Trust in Cloud Environments

Prisma™ Access (formerly GlobalProtect™ cloud service) helps your organization deliver consistent security to your remote networks and mobile users. It's a generational step forward in cloud security, using a cloud-delivered architecture to connect all users to all applications.

All your users, whether at your headquarters, branch offices, or on the road, connect to Prisma Access to safely use cloud and data center applications as well as the internet. Prisma Access consistently inspects all traffic across all ports and provides bidirectional networking to enable and control branch-to-branch as well as branch-to-HQ traffic.

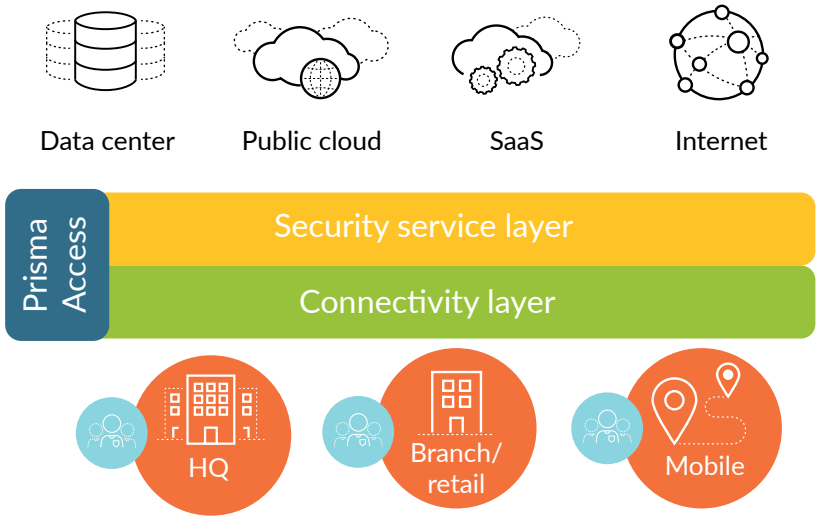

Figure 3: Prisma Access model

This architecture provides the correct model for implementing Zero Trust for the cloud:

- **Separate users and applications:** Instead of connecting directly to applications, users connect to Prisma Access. Hybrid cloud applications and private cloud environments are onboarded using IPsec tunnels to the connectivity layer.
- **Identify user and devices:** User-related attributes, such as identity and group information, along with endpoint criteria, such as the host and endpoint software configuration, are available for the evaluation of application security policy.
- **Prevent successful attacks:** To stop malicious content going to and from applications, and to control the movement of data, Prisma implements the enforcement of security and data protection capabilities that help organizations maintain safe and secure access.

Prisma implements these capabilities to enable safe access to the cloud:

- **Controlled access to all applications:** Unlike the point products on the market, Prisma Access provides connectivity and consistent security for applications in public clouds, private clouds/data centers, and SaaS, as well as on the internet.
- **Adaptive access to applications:** Your security team can establish the risk posture you want to take with a given application and use contextual controls to know who has access and the state of their devices.

- **Security visibility and analytics:** Maintain full visibility on the use of cloud applications. Take advantage of Cortex™ apps for security analytics and insights into risk factors.
- **Protection from compromised hosts:** Enforce policies based on an understanding of the endpoint to keep misconfigured and compromised devices from reaching your data.
- **Protection from unauthorized movement:** Use data protections to control the movement of data and files. Use App-ID™ technology policies to enable access to applications while blocking potentially risky functionality.

As a whole, these capabilities with Prisma Access are foundational for building your cloud application strategy. Unlike approaches that only address access to a handful of applications, Prisma Access lets you go one step further to protect all applications with a combination of Zero Trust capabilities, threat prevention, and data security.

Built for the Future

No matter where you are on your journey to the cloud, Prisma can help:

- Cloud-enabled mobile workforce
- Cloud-connected branch
- Zero Trust cloud security
- Cloud governance and compliance
- Cloud data protection
- Cloud threat protection
- Continuous security for DevOps

About Copper River Technologies

Copper River Technologies, a Federally recognized, Alaskan Tribal-Owned, 8(a) Certified Entity delivers high-performance IT solutions and services to enable private sector, enterprise organizations and SLED customers alike. Leveraging our unique advantage of holding elite-level partnerships with today's most innovative technology manufacturers, Copper River Tech delivers complete, end-to-end integrated solutions by combining these impressive product portfolios with our extraordinary engineering, design and professional services capabilities. Some of the innovative IT solutions and services we offer enable Cybersecurity, Data Center & Cloud Architectures, Enterprise Networks, and Mobility. Learn more 703.234.9000 or CopperRiverTech.com/Palo-Alto-Networks.

Contact

4501 Singer Court Suite 310 Chantilly, VA 20151 Main: 703.234.9000 CopperRiverTech.com