Secure the Cloud - Prisma

Application development methodologies are moving away from the traditional "waterfall" model toward more agile continuous integration/continuous delivery (CI/CD) processes with end-to-end automation. This new approach brings a multitude of benefits, such as shorter time to market and faster delivery, but it also introduces security challenges because traditional security methodologies weren't designed to address these modern application workflows. As developer teams embrace cloud-native technologies, security teams find themselves scrambling to keep up. Limited prevention controls, poor visibility, and tools that lack automation yield incomplete security analytics – all of these things increase the risk of compromise and the likelihood of successful breaches in cloud environments. Meanwhile, the demand for an entirely new approach to security emerges. Enter cloud-native security platforms (CNSPs).

The term "cloud native" refers to an approach to building and running applications that takes full advantage of a cloud computing delivery model instead of an on-premises data center. This approach takes the best of what cloud has to offer – scalability, deployability, manageability, and limitless on-demand compute power – and applies these principles to software development, combined with CI/CD automation, to radically increase productivity, business agility, and cost savings.

Cloud-native architectures consist of cloud services, such as containers, serverless security, platform as a service (PaaS), and microservices. These services are loosely coupled, meaning they are not hardwired to any infrastructure components, allowing developers to make changes frequently without affecting other pieces of the application or other team members' projects – all across technology boundaries, such as public, private, and multicloud deployments.

In short, "cloud native" refers to a methodology of software development that is essentially designed for cloud delivery and exemplifies all the benefits of the cloud by nature.

As more organizations have embraced DevOps and developer teams have begun to update their application development pipelines, security teams quickly realized their tools were ill-suited for the developer-driven, API-centric, infrastructure-agnostic patterns of cloud-native security. As a result, cloud-native security point products began to hit the market. These products were each engineered to address one part of the problem or one segment of the software stack, but on their own they could not collect enough information to accurately understand or report on the risks across cloud-native environments. This situation forced security teams to juggle multiple tools and vendors, which increased cost, complexity, and risk in addition to creating blind spots where the tools overlapped but didn't integrate.

Solving this problem requires a unified platform approach that can envelop the entire CI/CD lifecycle and integrate with the DevOps workflow. Just as cloud-native approaches have fundamentally changed the how cloud is used, CNSPs are fundamentally restructuring how the cloud is secured.

CNSPs share context about infrastructure, PaaS, users, development platforms, data, and application workloads across platform components to enhance security. They also:

- Provide unified visibility for SecOps and DevOps teams
- Deliver an integrated set of capabilities to respond to threats and protect cloud-native applications
- Automate the remediation of vulnerabilities and misconfigurations consistently across the entire build-deploy-run lifecycle

In the past, organizations that wanted to embrace new compute options were stifled by the need to buy more security products to support those options. Stitching together disparate solutions in an attempt to enforce consistent policies across technology boundaries became more of a problem than a solution. CNSPs, however, provide coverage across the continuum of compute options, multicloud, and the application development lifecycle. This coverage allows organizations to choose the right compute options for any given workload, granting them freedom without worry over how to integrate solutions for security. CNSPs epitomize the benefits of a cloud-native strategy, enabling agility, flexibility, and digital transformation.

The Palo Alto Networks CNSP includes the following solutions to secure the cloud: Prisma Cloud, Prisma Access, and Prisma SaaS.

Cloud application security (Prisma Cloud)

Prisma Cloud is the most comprehensive cloud-native security platform, designed to protect all aspects of cloud usage with the industry's leading technology. Prisma Cloud provides broad security and compliance coverage for the entire cloud-native technology stack, as well as applications and data throughout the entire application lifecycle, across multicloud and hybrid cloud environments. Prisma Cloud takes an integrated approach that enables SecOps and DevOps teams to accelerate cloud-native application deployment by implementing security early in the development cycle.

Prisma Cloud rests on four pillars:

- **Visibility, governance, and compliance.** Gain deep visibility into the security posture of multicloud environments. Keep track of everything that gets deployed with an automated asset inventory, and maintain compliance with out-of-the-box governance policies that enforce good behavior across your environments.
- **Compute security.** Secure hosts, containers, and serverless workloads throughout the application lifecycle. Detect and prevent risks by integrating vulnerability intelligence into your *integrated development environment* (IDE), *software configuration management* (SCM), and CI/CD workflows. Enforce machine learning-based runtime protection to protect applications and workloads in real time.
- **Network protection.** Continuously monitor network activity for anomalous behavior, enforce microservice-aware micro-segmentation, and implement industry-leading firewall protection. Protect the network perimeter as well as the connectivity between containers and hosts.

- **Identity security.** Monitor and leverage *user and entity behavior analytics (UEBA)* across your environments to detect and block malicious actions. Gain visibility into and enforce governance policies on user activities, and manage the permissions of both users and workloads.

Key Terms

An *integrated development environment* (IDE) is a software application that provides comprehensive tools – such as a source code editor, build automation tools, and a debugger – for application developers.

Software configuration management (SCM) is the task of tracking and controlling changes in software.

User and entity behavior analytics (UEBA) is a type of cybersecurity solution or feature that discovers threats by identifying activity that deviates from a baseline.

Cloud governance and compliance

Ensuring that your cloud resources and SaaS applications are correctly configured and adhere to your organization's security standards from day one is essential to prevent successful attacks. Additionally, making sure that these applications, as well as the data they collect and store, are properly protected and compliant is critical to avoid costly fines, a tarnished image, and loss of customer trust. Meeting security standards and maintaining compliant environments at scale, and across SaaS applications, is the new expectation for security teams.

Despite the availability of numerous tools, most organizations struggle to effectively control their data exposure and enforce security policies across ever-changing cloud environments and SaaS applications. Furthermore, ensuring compliance where data is stored across distributed environments puts a significant burden on your already constrained security teams.

Ensuring governance and compliance across multicloud environments and SaaS applications requires:

- **Real-time discovery and classification** of resources and data across dynamic SaaS, PaaS, and IaaS environments
- **Configuration governance** ensuring that application and resource configurations match your security best practices as soon as they are deployed, and preventing configuration drift
- **Access governance** using granular policy definitions to govern access to SaaS applications and resources in the public cloud as well as to apply network segmentation
- **Compliance auditing** leveraging automation and built-in compliance frameworks, to ensure compliance at any time and generate audit-ready reports on demand
- **Seamless user experience** that doesn't force additional steps or introduce significant latency in the use of applications as you add new security tools

Compute security

The cloud-native landscape is constantly evolving with new technologies and levels of abstraction. Hosts, containers, and serverless workloads provide unique benefits and have different security requirements. Prisma Cloud provides best-in-class solutions for securing any type of cloud-native workload, throughout the development lifecycle.

Prisma Cloud provides cloud-native compute security from build to run, including:

- **Vulnerability management.** Detect and prevent vulnerabilities and misconfigurations throughout the entire development process. Prioritize vulnerabilities based on your unique environment and prevent vulnerable code from ever reaching production.
- **Runtime security.** Prevent threats and anomalies across your hosts, containers, serverless functions, and orchestrators. Build automated, machine learning-driven models that define known good behaviors across process, network, file system, and system call sensors. Models are correlated to image IDs, so every time you build your app, you get a model uniquely calculated and tailored for that specific build.
- **Application security.** Protect applications and APIs through a powerful combination of web traffic inspection and *runtime application self-protection* (RASP). Embrace an "explicit allow" model where only the specific activities and capabilities required by your application are allowed – and everything else is treated as anomalous and is therefore prevented.
- **DevSecOps enabled.** Integrate security into your IDE, SCM, and CI workflows to detect and prevent issues as early as possible. Powerful plugins allow developers to inspect images, IaC templates, and functions as well as see vulnerability status every time they run a build. Security teams can prevent compromised assets from ever progressing down the pipeline.

Key Terms

Runtime application self-protection (RASP) detects attacks against an application in real time. RASP continuously monitors an app's behavior and the context of behavior to immediately identify and prevent malicious activity.

Network protection

Network protection must be adapted for cloud-native environments while still enforcing consistent policies across hybrid environments. Prisma Cloud detects and prevents network anomalies by enforcing container-level micro-segmentation, inspecting traffic flow logs, and leveraging advanced Layer 7 threat protection.

Prisma Cloud network protection capabilities include:

- **Network visibility and anomaly detection.** Ingest network traffic flow logs from multiple sources, and gain deep visibility into network behavior to detect and prevent anomalies.
- **Identity-based micro-segmentation.** Enforce cloud-native micro-segmentation at the container and host levels with Layer 4 and Layer 7 distributed firewalls. Segment cloud networks and deploy policies based on logical workload and application identities, rather than dynamic IP addresses.
- **Cloud-native firewalling.** Automatically model traffic flows between microservices, and dynamically create filters that allow valid connections and drop suspicious ones. Protect networks with Layer 4 and Layer 7 security capabilities, such as DNS security and URL filtering.

Identity security

Managing a large number of privileged users with access to an ever-expanding set of sensitive resources can be challenging. On top of that, cloud resources themselves have permission sets that need to be managed. Prisma Cloud helps you leverage the identity of cloud resources to enforce security policies and ensure secure user behavior across your cloud environments.

Key capabilities include:

Identity and access management (IAM) security. Secure and manage the relationships between users and cloud resources. Enforce governance policies to ensure that users and resources behave only as intended and do not introduce risk to the environment.

Access management. Ensure least-privileged access to cloud resources and infrastructure, and decouple user permissions from workload permissions.

Machine identity. Decouple workload identity from IP addresses. Leverage tags and metadata to assign a logical identity to applications and workloads, and then use it to enforce ID-based micro-segmentation and security policies that adapt to your dynamic environments.

UEBA. Continuously analyze the behavior of users and resources in your cloud to detect and prevent anomalous behavior, such as an admin logging in from an unknown location or a container accessing a file it should not be able to access.

Key Terms

A *secure web gateway* (SWG) is a security platform or service that is designed to maintain visibility in web traffic. Additional functionality may include web content filtering.

A *cloud access security broker* (CASB) is software that monitors activity and enforces security policies on traffic between an organization's users and cloud-based applications and services.

Secure Access Service Edge (Prisma Access)

With increasing numbers of mobile users, branch offices, data, and services located outside the protections of traditional network security appliances, organizations are struggling to keep pace and ensure the security, privacy, and integrity of their networks and their customers' data.

Today, many of the technologies on the market are built upon architectures that were not designed to handle all types of traffic and security threats. This forces organizations to adopt multiple point products to handle different requirements, such as secure web gateways, firewalls, secure VPN remote access, and SD-WAN. For every product, there is an architecture to deploy, a set of policies to configure, and an interface to manage, each with its own set of logs. This situation creates an administrative burden that introduces cost, complexity, and gaps in security posture.

To address these challenges, Secure Access Service Edge (SASE) has emerged. SASE (pronounced "sassy") is designed to help organizations embrace cloud and mobility by providing network and network security services from a common cloud-delivered architecture. A SASE solution must provide consistent security services and access to all types of cloud applications (public cloud, private cloud, and SaaS) delivered through a common framework. By removing multiple point products and adopting a single cloud-delivered SASE solution, organizations can reduce complexity while saving significant technical, human, and financial resources.

A SASE solution converges networking and security services into one unified, cloud-delivered solution (see Figure 3-12) that includes the following:

Networking:

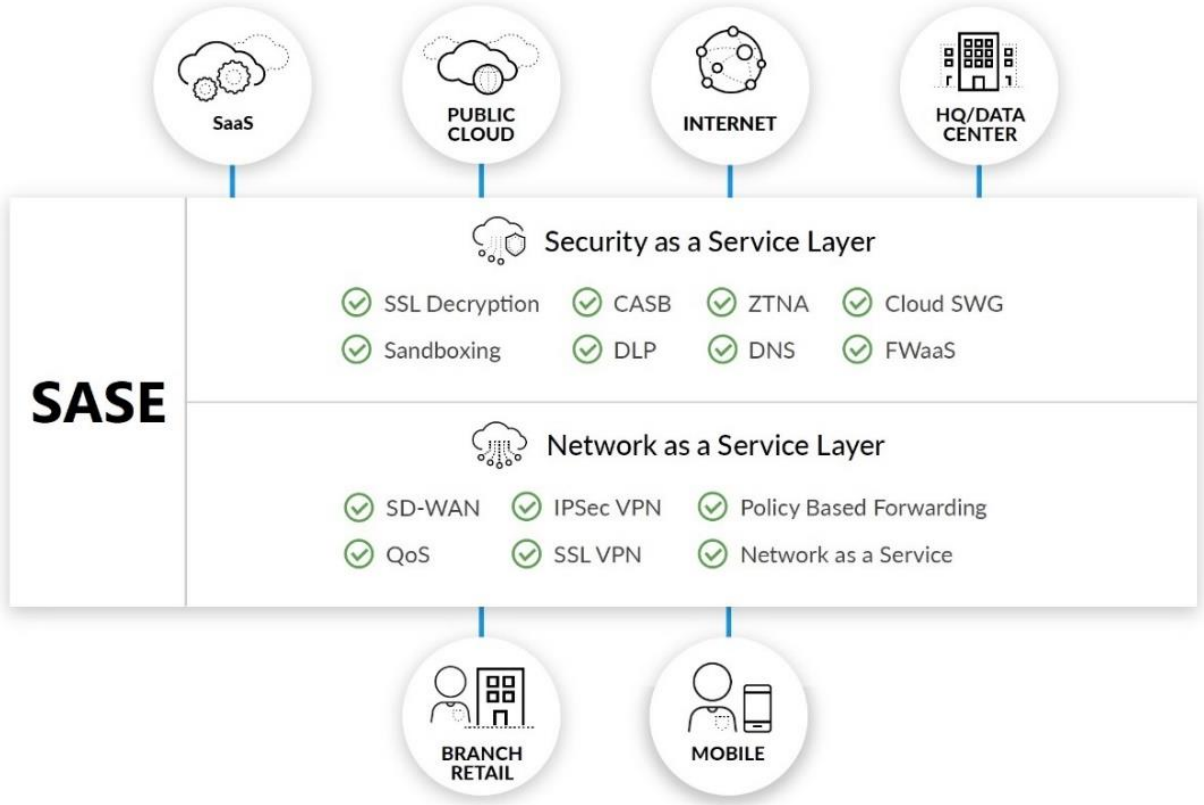
- Software-defined wide-area networks (SD-WANs)
- Virtual private networks (VPNs)
- Zero Trust network access (ZTNA)
- Quality of service (QoS)

Security:

- Firewall as a service (FWaaS)
- Domain Name System (DNS) security
- Threat prevention
- *Secure web gateway* (SWG)
- Data loss prevention (DLP)
- *Cloud access security broker* (CASB)

Figure 3-12

SASE delivers advanced network and security capabilities in a converged, cloud-delivered solution.



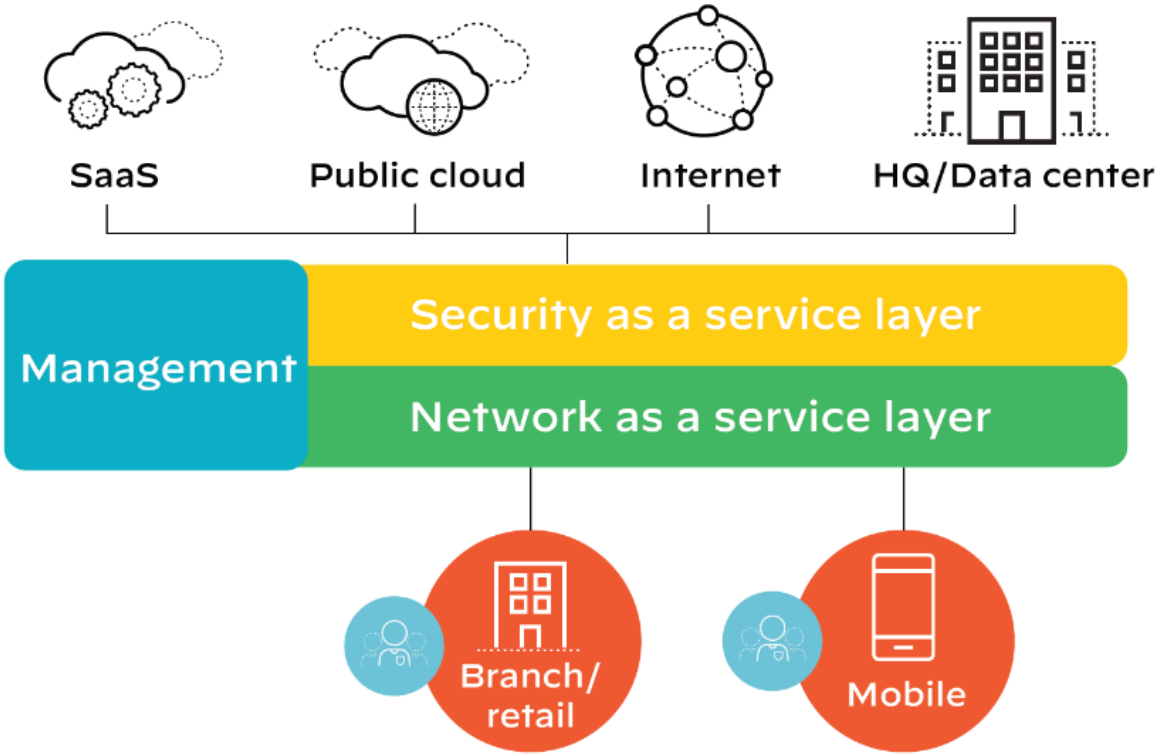
Prisma Access delivers globally distributed networking and security to all your users and applications. Whether at branch offices or on the go, your users connect to Prisma Access to safely access cloud and data center applications as well as the internet.

Prisma Access consistently protects all traffic, on all ports and from all applications, enabling your organization to:

- **Prevent successful cyberattacks** with proven security philosophies and threat intelligence for deep visibility and precise control that extends across your organization
- **Fully inspect all application traffic** bidirectionally – including SSL/TLS-encrypted traffic – on all ports, whether communicating with the internet, with the cloud, or between branches
- **Benefit from comprehensive threat intelligence** powered by automated threat data from Palo Alto Networks and hundreds of third-party feeds

The Prisma Access SASE architecture consists of a network-as-a-service layer, a security-as-a-service layer, and a common management platform to secure branch/retail and mobile users across SaaS, public cloud, internet, and headquarters/data center environments (see Figure 3-13).

Figure 3-13 *The Prisma Access architecture*



Network-as-a-service layer

The network-as-a-service layer in Prisma Access delivers key SASE capabilities, including:

- Software-defined wide-area network (SD-WAN)
- Virtual private network (VPN)
- Zero Trust network access (ZTNA)
- Quality of service (QoS)

SD-WAN

Companies are embracing software-defined wide-area network (SD-WAN) to connect branch offices to the corporate network and provide local internet breakout as an alternative to costly multiprotocol label switching (MPLS) connections. The challenge with SD-WAN, however, is how to combine security with the SD-WAN fabric, which leads to the need for multiple overlays.

In a SASE solution, SD-WAN edge devices can be connected to a cloud-based infrastructure, rather than to physical SD-WAN hubs located in data center or collocation facilities. This approach enables the interconnectivity between branch offices without the complexity of deploying and managing physical SD-WAN hubs.

SD-WAN should be something you are already considering or have already adopted into your organization's network infrastructure as a way to securely connect and control access to branch offices and remote employees. SASE creates a unified framework for SD-WAN services and other solutions to connect to, providing a single point of view and simplified management solution to protect your network.

Prisma Access connects branch offices over a standard IPsec VPN tunnel using common IPsec-compatible devices, such as your existing branch router, SD-WAN edge device, or a third-party firewall. It uses Border Gateway Protocol (BGP) or static routes for routing from the branch and equal-cost multi-path (ECMP) routing for faster performance and better redundancy across multiple links.

Virtual private network

Organizations rely on virtual private networks (VPNs) to provide a secure encrypted connection for mobile users and branch offices to access corporate data, applications, and internet access. There are many types of VPN services – from IPsec VPN to SSL VPN, clientless VPN, and remote access VPN – all of which require a connection to a VPN gateway. VPNs are not optimized for access to the cloud, resulting in no security or access control when users disconnect to reach cloud apps or services.

A SASE solution encompasses VPN services and enhances the capabilities to operate in a cloud-based infrastructure in order to securely route traffic to the public cloud, SaaS, internet, or private-cloud apps. In an IPsec VPN example, you can create a site-to-site connection to a cloud-based infrastructure from any IPsec-compatible device located at a branch or retail location via a branch router, wireless access point, SD-WAN edge device, or firewall. Mobile users employ an always-on IPsec or SSL VPN connection between their endpoint or mobile device, and a SASE solution ensures consistent traffic encryption and threat prevention.

No matter which type of VPN service you use in your organization, a SASE solution provides a unified cloud infrastructure to connect to, instead of backhauling to a VPN gateway at corporate headquarters. This solution dramatically simplifies the management and policy control needed to enforce least-privileged access rules.

Prisma Access (formerly GlobalProtect cloud service) provides cloud-delivered security infrastructure that makes it possible for your organization to connect users to a nearby cloud gateway, enable secure access to all applications, and maintain full visibility and inspection of traffic across all ports and protocols.

For managed mobile devices:

- Users with managed devices have the GlobalProtect app installed on their laptop, mobile phone, or tablet. The GlobalProtect app connects to Prisma Access automatically whenever internet access is available, without requiring any user interaction.

- Users can access all of their applications, whether in the cloud or the data center. The connectivity layer connects applications in different locations, making it possible to establish secure access (based on App-ID and User-ID policies) to public cloud, SaaS, and data center applications.
- Prisma Access delivers protection through the security service layer, such as protections against known and unknown malware, exploits, C2 traffic, and credential-based attacks.

For unmanaged/BYOD devices:

- Your organization can deploy Prisma Access in conjunction with mobile device management (MDM) integration to support bring-your-own-device (BYOD) policies. The integration enables capabilities such as per-app VPN.
- Users with unmanaged devices, such as contractors and employees with BYOD devices, can access applications without an app installed by using Prisma Access with Clientless VPN.
- Clientless VPN also enables secure access to SaaS applications from unmanaged devices with inline protections by using Security Assertion Markup Language (SAML) proxy integration. This functionality works in conjunction with Prisma SaaS.

Zero Trust network access

Zero Trust network access (ZTNA) is a key part of the Zero Trust philosophy of “never trust, always verify,” developed by Forrester to identify the need to protect data. ZTNA requires users who want to connect to the cloud to authenticate through a gateway before gaining access to the applications they need. This requirement provides an IT admin the ability to identify users and create policies to restrict access, minimize data loss, and quickly mitigate any issues or threats that may arise.

Many ZTNA products are based on software-defined perimeter (SDP) architectures, which do not provide content inspection, thus creating a discrepancy in the types of protection available for each application. In terms of consistent protection, the organization must build additional controls on top of the ZTNA model and establish inspection for all traffic across all applications.

SASE builds on the ZTNA key principles and applies them across all the other services within a SASE solution. By identifying users, devices, and applications, no matter where they are connecting from, policy creation and management are simplified. SASE removes the complexity of connecting to a gateway, by incorporating the networking services into a single unified cloud infrastructure.

A SASE solution should incorporate ZTNA concepts for protecting applications as well as apply other security services for the consistent enforcement of DLP and threat prevention policies. Access controls, in and of themselves, are useful for establishing who a person is, but other security controls are also necessary to make sure that their behaviors and actions are not harmful to the organization. And it is necessary to apply the same controls across access to all applications.

Quality of service

As organizations transition from MPLS to SD-WAN using broadband services, they are finding that the service quality varies. Quality of service (QoS) establishes bandwidth allocation assigned to particular apps and services. Businesses rely on QoS to ensure that their critical apps and services perform adequately (for example, medical equipment or credit card processing services). If these systems were to get bogged down due to lack of bandwidth, business operations and sales would be severely impacted. QoS prioritizes business-critical apps, based on a ranking system, so that you can choose which apps and services take precedence over others.

QoS is an important step when you begin migrating from MPLS. A SASE solution incorporates QoS services in the cloud, allowing you to easily mark sensitive applications (such as VoIP) as higher priority than general internet browsing and entertainment apps.

QoS is immensely important for businesses of any size. Managing the QoS traffic and allocation doesn't need to be difficult. SASE enables you to dynamically shape traffic based on the policies that prioritize critical application requirements. Make sure that your SASE solution contains QoS capabilities.

Security-as-a-service layer

The security-as-a-service layer in Prisma Access delivers key SASE capabilities, including:

- DNS security
- Firewall as a service (FWaaS)
- Threat prevention
- Secure web gateway (SWG)
- Data loss prevention (DLP)
- Cloud access security broker (CASB)

DNS security

Every organization uses DNS to translate a domain name into an IP address. DNS is an open service, and by default it does not have a way to detect DNS-based threats. As a result, malicious activity within DNS can be used to propagate an attack.

DNS security protects your users by predicting and blocking malicious domains while neutralizing threats. A SASE solution embraces DNS security features by providing consistent security across the network and users, no matter their location.

Your SASE solution should contain DNS protections, delivered within the cloud environment as part of the network access. DNS security should be built-in, rather than bolted-on, to the solution your branch offices and mobile users use to connect to the internet. The DNS security provided in your SASE solution should leverage a combination of predictive analytics, machine learning, and automation to combat threats in DNS traffic.

Prisma Access delivers the Palo Alto Networks DNS Security service, which provides a combination of predictive analytics, machine learning, and automation to combat threats in DNS traffic. Organizations can block known malicious domains, predict new malicious domains, and stop DNS tunneling.

Firewall as a service

Firewall as a service (FWaaS) is a deployment method for delivering a firewall as a cloud-based service. FWaaS has the same features as a next-generation firewall, but it is implemented in the cloud. By moving the firewall to the cloud, organizations can benefit from cost savings by eliminating the need to install or maintain security hardware at branch and retail locations.

A SASE solution incorporates FWaaS into its unified platform. By encompassing the FWaaS service model within a SASE framework, organizations can easily manage their deployments from a single platform.

A SASE solution should enable FWaaS capabilities in order to provide the protection of a next-generation firewall by implementing Network Security policy in the cloud. It is important to ensure that your SASE solution does not provide only basic port blocking or minimal firewall protections. You need the same features that a next-generation firewall embodies as well as the features that cloud-based security offers, such as threat prevention services and DNS security.

Prisma Access provides FWaaS, which protects branch offices from threats while also providing the security services expected from a next-generation firewall. The full spectrum of FWaaS includes threat prevention, URL filtering, sandboxing, and more.

Threat prevention

In today's world of small- and large-scale breaches, where ransomware attacks occur on a daily basis, threat prevention is key to protecting your organization's data and employees. A variety of threat prevention tools are available, from anti-malware and intrusion prevention to SSL decryption and file blocking, providing organizations ways to block threats. However, these point products require separate solutions, making management and integration difficult.

Within a SASE solution, all these point products and services are now integrated into a single cloud platform. This integration provides simplified management and oversight of all threats and vulnerabilities across your network and cloud environments.

Stopping exploits and malware by using the latest threat intelligence is crucial to protecting your employees and data. Your SASE solution should incorporate threat prevention tools into its framework so that you can react quickly and swiftly to remediate threats. Be sure to check the quality of threat intelligence that is being provided by the vendor. The vendor should be gathering and sharing data from various sources, including customers, other vendors, and other related thought leaders, to provide continuous protection from unknown threats.

Using Prisma Access for threat prevention combines the proven technologies in the Palo Alto Networks platform, together with global sources of threat intelligence and automation, to stop previously known or unknown attacks.

Secure web gateway

Organizations rely on secure web gateway (SWG) to protect employees and devices from accessing malicious websites. SWG can be used to block inappropriate content (such as pornography and gambling) or websites that businesses simply don't want users accessing while at work, such as streaming services like Netflix. Additionally, SWG can be used to enforce an acceptable use policy (AUP) before internet access is granted.

SWG is just one of the many security services that a SASE solution must provide. As organizations grow and add ever greater numbers of remote users, coverage and protection become more difficult. A SASE solution moves SWG into the cloud, providing protection in the cloud through a unified platform for complete visibility and control over the entire network.

A SASE solution includes the same security services in a SWG, allowing organizations to control access to the web and enforce security policies that protect users from hostile websites. It is important to remember that SWG is just one service of the SASE solution. Other security services – such as FWaaS, DNS security, threat prevention, DLP, and CASB – should also be included.

Prisma Access for SWG functionality is designed to maintain visibility into all types of traffic while stopping evasions that can mask threats. The Palo Alto Networks web filtering capabilities also drive its credential theft prevention technology, which can stop corporate credentials from being sent to previously unknown sites.

Data loss prevention

Data loss prevention (DLP) tools protect sensitive data and ensure that it is not lost, stolen, or misused. DLP is a composite solution that monitors data within the environments where it is deployed (such as networks, endpoints, and clouds) and through their egress points. It also alerts key stakeholders when policies are violated. Due to compliance requirements – such as the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), and others – DLP is a crucial solution needed for data security and compliance. Legacy DLPs rely on old core technology initially designed for on-premises perimeters and subsequently extended and adapted to cloud applications. Loaded with features, disjointed policies, configurations, and workarounds, DLPs have become very complex, difficult to deploy at scale, and too expensive. Digital transformation and new data usage models demand a fresh approach to data protection.

Through the SASE approach, DLP becomes one cloud-delivered solution centered around the data itself, everywhere. The same policies are consistently applied to sensitive data, whether at rest, in motion, and in use, and regardless of its location. In the SASE architecture, DLP is not a standalone solution anymore but is embedded in the organization's existing control points, thus eliminating the need to deploy and maintain multiple tools. With SASE, organizations can finally enable a comprehensive data protection solution that relies on a scalable and simple architecture and allows effective machine learning by leveraging access to global traffic.

DLP is a necessary tool to protect sensitive data and ensure compliance throughout the organizations. To this end, the SASE solution must include this core capability. With SASE, DLP is an embedded, cloud-delivered service used to accurately and consistently identify, monitor, and protect sensitive data everywhere across networks, clouds, and users.

Prisma Access combines integration with DLP controls that are API-driven (through Prisma SaaS) as well as inline (through Prisma Access). These DLP policies allow organizations to categorize data and establish policies that prevent data loss.

Cloud access security broker

Many organizations depend on cloud access security brokers (CASBs) to provide visibility into SaaS application usage, understand where their sensitive data resides, enforce company policies for user access, and protect their data from hackers. CASBs are cloud-based security policy enforcement points that provide a gateway for your SaaS provider and your employees.

CASB should be another security feature that is part of your SASE solution, creating a single platform for stakeholders to manage security controls. A SASE solution helps you understand which SaaS apps are being used and where data is going, no matter where users are located.

Your SASE solution should incorporate both inline and API-based SaaS controls for governance, access controls, and data protection. Also called a multimode CASB, the combination of inline and API-based CASB capabilities provides superior visibility, management, security, and zero-day protection against emerging threats.

Prisma Access and Prisma SaaS implement security controls that combine inline security API security and contextual controls, acting as a CASB to determine access to sensitive information. These controls are implemented in an integrated manner and applied throughout all cloud application policies.

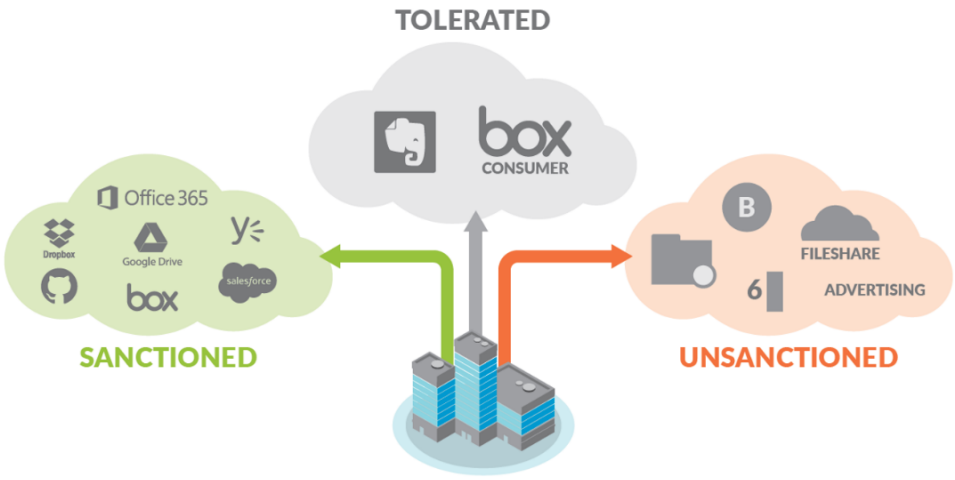
Prisma SaaS

To safely enable SaaS usage in your organization, start by clearly defining the SaaS applications that should be used and which behaviors within those applications are allowed. This step requires a clear definition of which applications are:

- **Sanctioned** (allowed and provided by IT)
- **Tolerated** (allowed because of a legitimate business need, with restrictions, but not provided by IT)
- **Unsanctioned** (not allowed), then prevent their usage with granular policies

Sanctioned SaaS applications provide business benefits and are fast to deploy, require minimal cost, and are infinitely scalable. Tolerated SaaS applications fulfill a legitimate business need, but certain usage restrictions may be necessary to reduce risk. Unsanctioned SaaS applications either clearly provide no business benefits or the security risks of the application outweigh the business benefits. For example, an unsanctioned SaaS application may violate regulatory compliance mandates, create an unacceptable risk of loss of corporate intellectual property or other sensitive data, or enable malware distribution (see Figure 3-14).

Figure 3-14 *Impacts of sanctioned and unsanctioned SaaS applications*



To control sanctioned SaaS usage, an enterprise security solution must provide the following:

- **Threat prevention.** SaaS applications introduce new threat risks that need to be understood and controlled. Many SaaS applications automatically sync files with users, and users often share data in SaaS applications with third parties that are out of an organization's control. These two aspects of SaaS environments create a new insertion point for malware that not only can get in from external shares but can also automatically sync those infected files across the organization without any user intervention. To address SaaS-based malware threats, a security solution must be able to prevent known and unknown malware from residing in sanctioned SaaS applications, regardless of the source.
- **Visibility and data exposure control.** After sanctioned SaaS usage is defined and controlled with a granular policy, data residing in those SaaS applications is no longer visible to the organization's perimeter firewalls. This loss of visibility creates a blind spot for IT. Additional data exposure controls are needed to specifically address the unique risks associated with SaaS environments, with a focus on data protection. Visibility of data stored and used in SaaS applications is critical to ensuring a deep understanding of users, the data they have shared, and how they have shared it.

- **Risk prevention, not just risk response.** An organization's users commonly use certain SaaS applications long before the organization officially sanctions those applications. Even after a SaaS application is sanctioned, data is often shared with third parties that don't necessarily have next-generation security solutions to effectively safeguard SaaS data from malware threats and data exposure risks. Threat prevention and data exposure control in a SaaS-based environment require visibility and control not just from the time that a SaaS application is sanctioned going forward. You need visibility and control of *all* your data, including data that was being stored – and shared – before the SaaS application was sanctioned.

Data residing within enterprise-enabled SaaS applications is not visible to an organization's network perimeter. Prisma SaaS connects directly to sanctioned SaaS applications to provide data classification, sharing/permission visibility, and threat detection within the application. This capability yields unparalleled visibility, which allows organizations to inspect content for data exposure violations and control access to shared data via a contextual policy.

Prisma SaaS builds on the existing SaaS visibility and granular control capabilities of the Security Operating Platform provided through App-ID, with detailed SaaS-based reporting and granular control of SaaS usage. Figure 3-15 shows an example of the granular controls for SaaS applications supported by App-ID.

Figure 3-15 *Example of granular controls supported by App-ID*

Application	Control	Feature
Box	Box – Personal	App-ID
	Box – Corporate	App-ID
	Upload control	File Blocking
	Download control	File Blocking
	Malware detection	WildFire & protection profile
	User-based control	User-ID

Prisma SaaS is a completely cloud-based, end-to-end security solution that provides visibility and control within SaaS applications, without the need for any proxies, agents, software, additional hardware, or network changes. Prisma SaaS isn't an inline service, so it doesn't impact latency, bandwidth, or end-user experience. Prisma SaaS communicates directly with the SaaS applications themselves and looks at data from any source, regardless of the device or location from which the data was sent.

SaaS threat prevention

WildFire threat cloud integration with Prisma SaaS provides cyberthreat prevention to block known malware and to identify and block unknown malware. This integration extends the existing integration of WildFire to prevent threats from spreading through the sanctioned SaaS applications, which prevents a new insertion point for malware. When new malware is discovered by Prisma SaaS, the threat information is shared with the rest of the Security Operating Platform, even if it is not deployed inline with the SaaS applications.

Data exposure visibility

Prisma SaaS provides complete visibility across all user, folder, and file activity, which provides detailed analysis that helps you transition from a position of speculation to one of knowing exactly what is occurring in the SaaS environment at any given point in time. Because you can view deep analytics into day-to-day usage, you can quickly determine if there are any data risk or compliance-related policy violations. This detailed analysis of user and data activity allows for granular data governance and forensics.

Prisma SaaS connects directly to the applications themselves, so it provides continuous silent monitoring of the risks within the sanctioned SaaS applications, with detailed visibility that is not possible with traditional security solutions.

Contextual data exposure control

Prisma SaaS enables you to define granular, context-aware policy control that provides you with the ability to drive enforcement and quarantine users and data as soon as a violation occurs. This control enables you to quickly and easily satisfy data risk compliance requirements such as PCI and PII while still maintaining the benefits of cloud-based applications.

Prisma SaaS prevents data exposure in unstructured (hosted files) and structured (application entries such as Salesforce.com) data. Both data types are common sources of improper data shares.

Advanced document classification

Prisma SaaS inspects documents for common sensitive data strings (such as credit card numbers, SSH keys, and Social Security numbers) and flags them as risks if they are improperly shared. Unique to Prisma SaaS is the ability to identify documents by type, through advanced document classification regardless of the data that is contained in the document itself. Prisma SaaS has been designed to automatically identify sensitive documents, such as those related to medical, tax, and legal issues.

Retroactive policy

A traditional network security solution can see only inline data and apply security policies to data that is accessed inline, after the policy is created. This approach doesn't effectively prevent SaaS data exposure, however, because SaaS data may have been shared long before the policy was created. This data may not be accessed inline for many months or years, potentially leaving sensitive data exposed indefinitely to malware infection and unauthorized access.

Prisma SaaS retroactively applies security policies to all users and data from the beginning of the SaaS account's creation, rather than the policy's creation, to identify any potential vulnerabilities or policy violations. Prisma SaaS does not wait for someone to access the data inline to apply policies and resolve any vulnerabilities or violations; SaaS data and shares are proactively discovered, protected, and resolved, no matter when they were created.

Policies are context-driven to allow for granular definitions of data exposure risks. This granularity is necessary to enable SaaS use by users while still preventing accidental data exposure. Policies take several factors in context to create an overall data exposure risk profile. One or two factors may not provide enough insight into the potential risk of the share. The overall risk of exposure is determined only after the full context of the share is understood.

Risks are calculated by user type, document type, sensitive data contained, how the data is shared, and whether malware is present. This capability provides the ability to control the exposure at a granular level based on several important factors.

For example, a financial team may be able to share financial data with other people on their team, but not beyond that. Even though the original share is allowed, they cannot share data that is infected with malware. The financial team may, however, be allowed to share non-sensitive data company-wide or, in some cases, with external vendors. The key to enabling this level of granularity is the ability to look at the share in the context of all the factors.

Prisma Cloud Security Posture Management (CSPM)

Effective cloud security requires complete visibility into every deployed resource as well as absolute confidence in their configuration and compliance status. As enterprises further adopt cloud-native methodologies and gain the flexibility of multicloud architectures, stitching together security data from disparate legacy tools becomes a considerable obstacle. DevOps and security teams need a single, integrated solution like Prisma Cloud.

Prisma Cloud takes a unique approach to cloud security posture management, going beyond mere compliance or configuration management. Vulnerability intelligence from more than 30 data sources provides immediate clarity on critical security issues, while controls across the development pipeline prevent insecure configurations from ever reaching production. Prisma Cloud Security Posture Management (CSPM) modules include:

- **Visibility, Compliance, and Governance**
    - *Cloud Asset Inventory*. Prisma Cloud delivers comprehensive visibility and control over the security posture of every deployed resource. While some solutions simply aggregate asset data, Prisma Cloud analyzes and normalizes disparate data sources to provide unmatched risk clarity.
    - *Compliance Monitoring and Reporting*. Prisma Cloud continuously monitors cloud compliance posture and supports one-click reporting from a single console. Numerous compliance frameworks are included out of the box, and you can build additional custom frameworks.

- *Infrastructure-as-code (IaC) Scanning*. Prisma Cloud enables users to scan IaC templates for vulnerabilities and build cloud-agnostic policies for the build and runtime development phases.

- **Threat Detection**

  - *User and Entity Behavior Analytics (UEBA)*. Prisma Cloud analyzes millions of audit events and then uses machine learning to detect anomalous activities that could signal account compromises, insider threats, stolen access keys, and other potentially malicious user activities.

  - *Network Anomaly Detection*. Prisma Cloud monitors cloud environments for unusual network behavior and can detect unusual server port or protocol activity, including port scan and port sweep activities that probe a server or host for open ports.

  - *Automated Investigation and Response*. Prisma Cloud provides automated remediation, detailed forensics, and correlation capabilities. Insights combined from workloads, networks, user activity, data, and configurations accelerate incident investigation and response.

- **Data Security**

  - *Data Visibility and Classification*. Prisma Cloud provides complete visibility into all Amazon Web Services Simple Storage Service (AWS S3) buckets and objects, including contents by region, owner, and exposure level. You can fine-tune data identifiers—such as driver's license, Social Security number, credit card number, or other patterns—to identify and monitor sensitive content.

  - *Data Governance*. Prisma Cloud includes specific data policies to quickly determine your risk profile based on data classification and exposure/file types. Enable or disable data compliance assessment profiles—for example, Payment Card Industry Data Security Standards (PCI DSS), General Data Protection Regulation (GDPR), System and Organization Controls Type 2 (SOC 2), and Health Insurance Portability and Accountability Act (HIPAA)—based on needs and generate audit-ready reports with a single click.

  - *Malware Detection*. Prisma Cloud helps users identify and protect against known and unknown file-based threats that have infiltrated S3 buckets, leveraging the WildFire malware prevention service to flag any objects that contain malware.

  - *Alerting and Remediation*. Prisma Cloud automatically generates alerts for each object based on data classification, data exposure, and file types. Analysts can take action on alerts to quickly remediate exposure, tag individual DevOps teams for violations, and delete any objects that contain malware.