proofpoint.

SOLUTION BRIEF

Zero Trust: How to Secure Your Network in the Age of Cloud and Worker Mobility

PRODUCTS

- Proofpoint Web Security
- Proofpoint Meta Secure Enterprise Access

KEY BENEFITS

- Deliver secure remote access to your employees and contractors
- Ensure zero-trust security through adaptive controls and granular access
- Enable a people-centric, software-defined perimeter
- Accelerate cloud migration through a cloud-native network
- Internet protection with dynamic access controls, advanced threat protection, and data loss prevention policies

Many enterprises heartily embrace cloud computing by putting their own applications in the cloud. They subscribe to ready-to-use SaaS applications and support an expanding remote and mobile workforce. However, these practices strain the capabilities of legacy networks built around site-centric connectivity and security stacks. Some well-known shortcomings of relying on data-center-based firewalls and VPNs include the large network attack surface, unreliable user experience and administrative headaches.

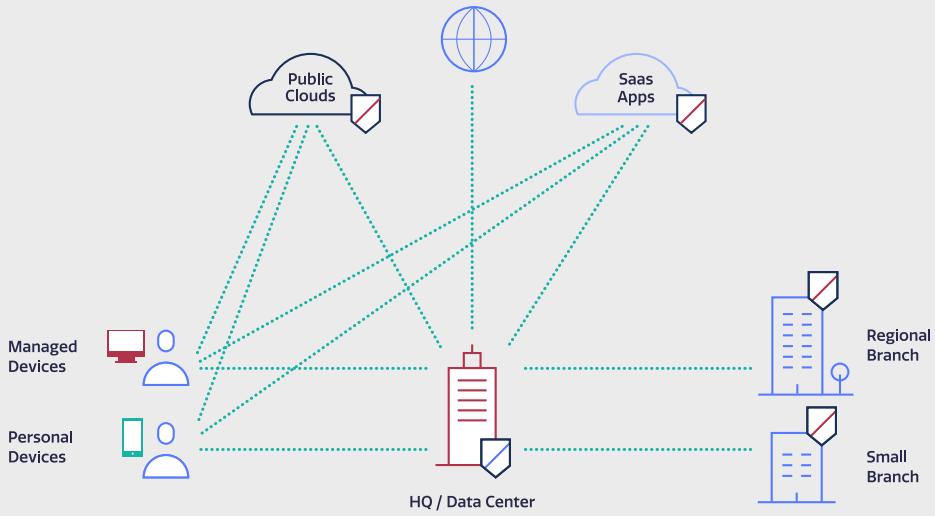
Proofpoint Meta offers an evolutionary step in networking—the first software-defined enterprise network-as-a-service that can securely connect your users to data centers, public and private clouds, SaaS applications and offices. And it provides you with the agility and performance that today's enterprises need. Web Security protects organizations from all types of internet-based threats by applying dynamic access controls, advanced threat protection and data loss prevention policies.

Networking and security for a bygone era

Most enterprises still have legacy networking and network security infrastructures that are site-specific and centered around a major location like a data center or company headquarters. Your security devices—firewalls, secure web gateways, IDS/IPS appliances and so on—are located on-premises with the networking infrastructure. And they seemingly create a secure perimeter around the network, the applications and the data contained within your site.

The assumption is that your employees work at this site during specific hours, log in to the network via wired or wireless connections, and access their routine business applications. Your remote employees use a company-specific VPN to come back into the home network even if they want to access web-based applications or the internet. Branch offices use a WAN, often with dedicated MPLS lines, to access your company applications and resources. Regardless of where it originates, traffic is backhauled to this site-specific central network and put through the security perimeter before being routed out to whatever destination it ultimately has.

This network architecture works just fine—if the year is 2005. But it isn't.



Cloud migration and a mobile workforce: Different network security needs

Today's way of work barely resembles that scenario. These days, many enterprise applications, workloads and storage are in the cloud as companies adopt a "cloud first" strategy to get out of the business of owning and managing infrastructure. They are migrating their own custom applications to the cloud to run on platforms like Amazon AWS or Microsoft Azure, as well as subscribing to enterprise SaaS applications like Microsoft 365, Salesforce, Workday, ServiceNow and countless other productivity applications.

The idea of people always working in the same office location during specific work hours seems quaint these days. The workday doesn't end at 5 p.m. Many people work extra hours at home in the evening and on weekends, and they need remote access to their office computer. People are mobile and they work from home or wherever they happen to be. In fact, some people may never even go to a company site—especially if they aren't actual employees of the company. An organization's workforce is very likely to include contractors, partners and consultants who need varying levels of access to applications, data and other company resources. What's more, workers may use non-corporate-owned, unmanaged devices as they access the network and applications.

With people and computing resources scattered about, unknown devices connecting from near and far and cloud-based applications now essential to business operations, the traditional site-centric perimeter of network security is long gone. Nevertheless, strong security is needed now more than ever. Threats are growing more pervasive and damaging. And reports of cyber breaches and attacks surface regularly.

Mission impossible: Securing the perimeter with overly permissive VPN

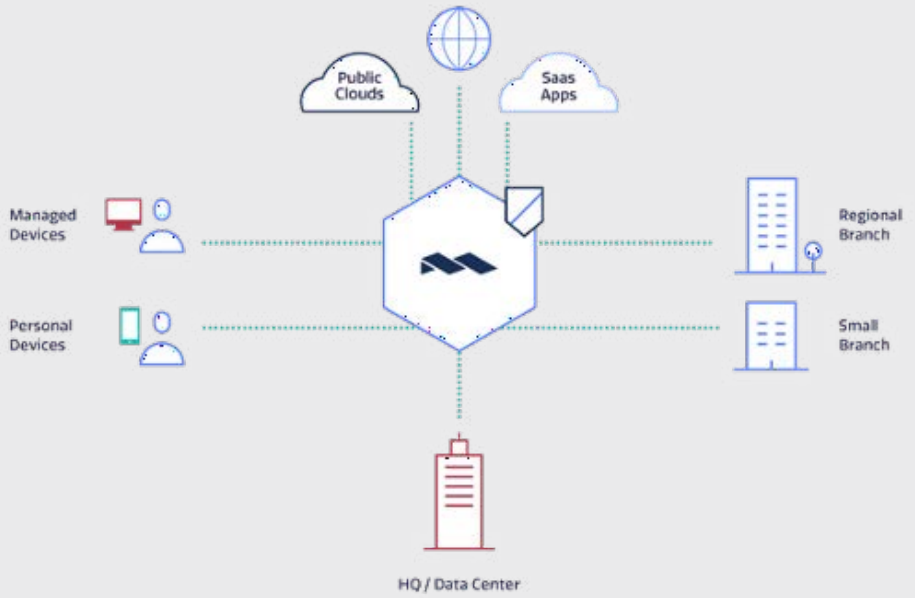
In terms of networking, people have to connect to something regardless of where they work. Most organizations do that today by connecting workers to the network in the corporate data center or headquarters.

For your employees in an office, it's typically a simple LAN or WAN connection; those outside the office (such as mobile or remote workers) usually connect via a VPN. The security paradigm for either method of connectivity is flawed because once authenticated users access the enterprise network, they are considered "trusted" and have overly broad access to the network. VPNs have their own problems because the user experience can be bad, and from the IT perspective, VPNs can be difficult to manage.

What is a Software-Defined Perimeter?

A software-defined perimeter (SDP) defines a logical set of disparate, network-connected participants within a secure computing enclave. The resources are typically hidden from public discover, and access is restricted via a trust broker to the specified participants of the enclave. This removes the asset from public visibility and reduces the surface area for attack.

Neil MacDonald, Gartner analyst



The connectivity and security challenges escalate when your organization uses cloud applications. For branch or mobile workers, the enterprise can either bring all traffic back to the headquarters network hub and then send it out to the cloud or allow the traffic to go straight to the cloud from wherever the user is. Backhauling all remote traffic to a central facility isn't practical. Companies do it to enforce the on-premises security stack, but this practice puts a strain on network and application performance and degrades the user experience. What's more, mobile users lose "locality," meaning that someone who is traveling quite far from the home network—perhaps out of the country—still has their traffic backhauled to the network hub. This results in latency and throughput issues.

Allowing your user traffic to go straight to the cloud or the internet is too risky. This practice circumvents corporate security infrastructure and policy and doesn't allow all traffic to be logged for audit and security purposes. Companies compensate by installing one after another security solutions—CASBs for SaaS applications, and VPNs for IaaS/PaaS, which becomes more complex and expensive with the growing number of instances.

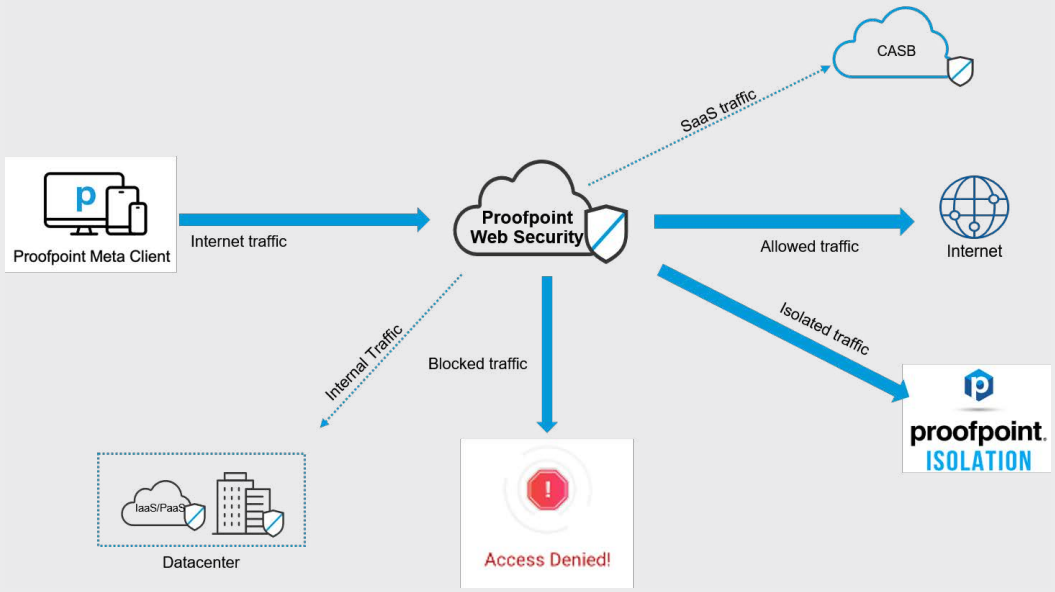
It's simply not practical or cost effective to deploy so many security solutions, especially for cloud applications. It forces your IT department to become systems integrators to make a lot of disparate solutions work together for the sake of trying to hold onto a porous security perimeter.

A new paradigm for networking and network security

As computing paradigms go, many enterprises are still in the early stages of grappling with these networking and security challenges. And it will only get more complicated as mobility grows, applications in the cloud and multiple clouds increase and traditional "sites" for computing hubs disappear.

The current site-centric networking and network security architecture can't meet today's needs, much less tomorrow's. You need a new, user-centric approach to networking and security. What does this mean?

- Instead of connecting your users to specific sites, they connect to a global network through a worldwide arrangement of local points-of-presence (PoPs) for "always on" secure connectivity.
- Instead of treating clouds as silos, clouds connect to Proofpoint Meta, and from there to your datacenter, offices or another cloud. Multi-vendor, cross-cloud networking is easily enabled.
- Instead of securing your network perimeter, there is a software-defined perimeter (SDP) for each user, giving your workers micro-segmented access to only the applications and network resources they need.
- Instead of turning your IT department into systems integrators, there is a best-of-breed network security stack in the cloud, and you can chain together the security services you need. Security is pervasive at every point in the network.



Cloud-based internet protection

Organizations are struggling to make sure their users have secure internet access regardless of when or where they connect from. With remote work becoming more common, it has become critical to make sure traffic is secured and that it doesn't become a point of data loss for an organization. With Proofpoint Web Security, organizations now have a scalable and easy to deploy way to protect their users while they browse the internet. Web Security can provide access to users and take action on their browsing such as allowing, blocking or sending to an isolated session. With best of breed Advanced Threat Protection, Web Security can protect users from advanced threats—both known and unknown. Finally, organizations can ensure their critical data does not become compromised by using the built-in advanced DLP capabilities that are part of Web Security. Together these capabilities ensure that organizations can have more confidence in their users' internet traffic and it won't lead to malware infections or data loss.

Zero trust network-as-a-service

Proofpoint Meta is building the fabric that delivers user-centric computing to enterprises. It is a global overlay network that is worldwide and multi-tenant. But it functions like a private enterprise-wide area network for each customer organization. All the infrastructure of this network is provided by Meta in the cloud, so there is no hardware for you to deploy.

Proofpoint Meta

Meta has a dense network of PoPs all around the world. Your users, legacy data centers, branch offices and clouds all connect to Meta via the nearest local PoP. There are two ways for users to connect. One is an always-on VPN-based connection, which is recommended for managed corporate devices. The other is browser-based secure remote access, which is most appropriate for personal devices and non-employees such as contractors, partners and consultants.

All user traffic—WAN, LAN and internet—flows through this network, where it is secured and audited. Internet traffic breaks out at the local PoP. From a technology perspective, this network is like a very big distributed identity-based router that Meta deploys in the cloud. Policies abstract the physical topology and deal with users and resources.

Because all traffic flows through this network, you can have a holistic approach to security—one that encompasses access to corporate applications and data, as well as internet access. This is essential to ensure a device isn't breached when it's disconnected from the enterprise network. With Meta, you can enforce an "always-on" security model to your employees if you wish, whereas many other software-defined perimeter solutions ignore the internet. That means you need to find another solution for internet traffic or leave the device vulnerable.

Meta has a zero-trust architecture where each user is bound by a software-defined perimeter. Each of your users has a unique, fixed identity no matter where they connect from to this network. The SDP security framework allows one-to-one network connections that are dynamically created on demand between the user and the specific resources he needs to access. Everything else is invisible to the user. No access is possible unless it is explicitly granted, and it's continuously verified at the packet level. This model effectively provides you with dynamically provisioned secure network segmentation.

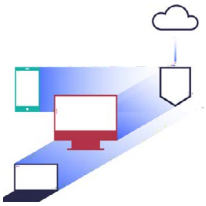
The process also ensures that all endpoints attempting to join the network are authenticated and authorized before gaining access any resource on the network, as well as throughout the session. This not only applies the principle of least privilege to the network, but it also reduces your attack surface area by hiding network resources from unauthorized or unauthenticated users.

In addition to the user-centric SDP, a wide range of more traditional security services are available as network functions. You can choose your preferred, best-of-breed services and "chain" them so that traffic passes through all the appropriate security points in succession. Meta has built-in security services, while many others come from a variety of partners that specialize in security. For example, Meta has built-in DNS and IP layer security, and partners provide services for solutions such as secure web gateway (SWG), network access control (NAC), and cloud access security broker (CASB). Through our technology partnerships, you can have a customized security stack consisting of your choice of best-of-breed products rather than a limited choice of vertically integrated products.

Integration happens in the cloud rather than on office appliances or your users' devices, which saves you time and labor. It means nearly zero-touch, policy-based provisioning of those products.

Key features of Proofpoint Meta

Here are some of the key characteristics of Meta network-as-a-service:

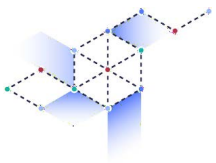


Cloud native

Meta leverages a secure cloud overlay over a worldwide backbone of PoPs. The density of the PoPs makes sure the last mile between the user and the network is always short, and therefore enables low latency and stable VPN connections. The traffic leaves the optimized network as close to its destination as possible, further reducing latency (sometimes close to zero, if they are hosted in the same cloud internet exchange). You can avoid backhaul to private data centers when accessing cloud and internet services.

User-centric

This network is built around your users, not around specific sites or offices. All connections are essentially "always on." People can connect from anywhere, with any device. The network has native client support for Windows, macOS, iOS, Android and Linux devices. Centralized policies of the software-defined perimeter control what resources users can access. The user experience is exceptional. The scaled-out, completely software-defined network assures low latency and is designed to support millions of concurrent users.



Scalable

We built Meta to support millions of concurrent IPSec tunnels that connect your users and applications to the Meta infrastructure. The network is built to scale and support any growing amount of traffic that is sent to it. The density of PoPs and their close location to users and resources provides you with excellent performance, regardless of the number of users connected.

Zero-trust access

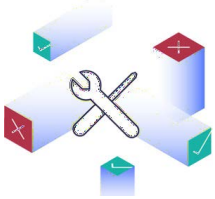
The software-defined perimeter means the network has micro-segmentation powered by strong identity from end-to-end. You have complete visibility into all network access, verified and enforced at the packet level and auditable at the user/device level. And there's no need to correlate data from different sources and services to deliver per-device audit and traffic detailed information.

An open security stack

You can choose the security services you prefer to use. We partner with the world's leading security vendors to integrate their solutions as services on the network. The services can be chained such that traffic passes through multiple security solutions before traversing the network, either for enterprise assets or for internet-bound traffic.

Comprehensive, non-repudiable audit logs

Meta captures complete logs for all traffic, all the time, regardless of where a user device connects from. Logs are always accessible and available to whatever services need to consume those logs. For example, these audit logs can be available to analytics tools, such as user behavior analytics to detect anomalies, or to forensic tools to determine what has happened surrounding an event or activity. The audit trails also support regulatory compliance requirements.



Easy deployment

There is no equipment to install. You do not need to buy, maintain or manage any RAS or VPN concentrators. It's simple to set up and tear down compared to an enterprise operating its own network. And it saves the time and unnecessary risk of creating segregated DMZs, introducing external users to Active Directory, and configuring complex firewalls. It's easy to onboard your people and bring applications and data onto the network. And cloud-delivered security further reduces security services onboarding, switching and maintaining. Once the topology is abstracted, all network management is policy-based, centrally managed and instantly enforced globally.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.