proofpoint.

WHITE PAPER

Why Choose Zero Trust for Contractor Remote Access

Software-defined perimeters: The zero-trust approach to secure remote access for your contractors, partners and customers

Connectivity for Contractors

The increased connectivity of the modern workforce is driving constant growth in contract workers. Nearly two-thirds (63 percent) of companies today have remote workers.[1] At Google, for example, contract workers outnumbered direct employees for the first time in 2018.[2]

Remote contract work is prevalent at companies of any size, including those that are not intentionally remote-friendly. "To gain an advantage in this increasingly competitive talent climate, companies must think outside their offices or city limits and embrace a flexible, remote workforce," says Stephane Kasriel, CEO of Upwork, the largest freelancing website.[3]

And yet, the majority of companies lack the policies and technological infrastructure to support efficient and secure remote work. This exposes them to security risks. And it hinders the effectiveness of their contractors, freelancers, partners or remote employees.

This paper examines software defined perimeter (SDP) solutions, which provide a more secure and manageable alternative to legacy VPNs for remote contractor work.

Using Forrester's terminology, SDP solutions adopt the Zero Trust eXtended (ZTX) approach, which is "a conceptual and architectural model for how security teams should strengthen data security using obfuscation techniques, limit the risks associated with excessive user privileges and access, and dramatically improve security detection and response with analytics and automation."[4]

1 Inc.com. "63 Percent of Companies Have Remote Workers—Yet More Than Half Do Not Have a Remote Work Policy." June 2018.
2 The New York Times. "Google's Shadow Work Force: Temps Who Outnumber Full-Time Employees." May 2019.
3 https://www.upwork.com/press/2018/02/
4 Forrester. The Zero Trust eXtended (ZTX) Ecosystem. July 2019.

Table of Contents

The Fall of the VPN

Network access of remote contractors is a high-risk use case that traditional VPNs were not designed to address. Primarily, VPNs provide excessive trust. Once a remote user is authenticated by a VPN, he/she is considered trusted and is granted access to more of the network than is required. Consequently, network resources are unnecessarily visible, overly vulnerable, and open to attack.

Another VPN drawback is management and administration complexity. Quite often, remote contractors must be provided access to dozens, and sometimes hundreds, of multiple cloud provider instances. This means deploying, configuring and maintaining VPNs for every instance. In addition, IT administrators find themselves investing precious time configuring and troubleshooting VPN clients.

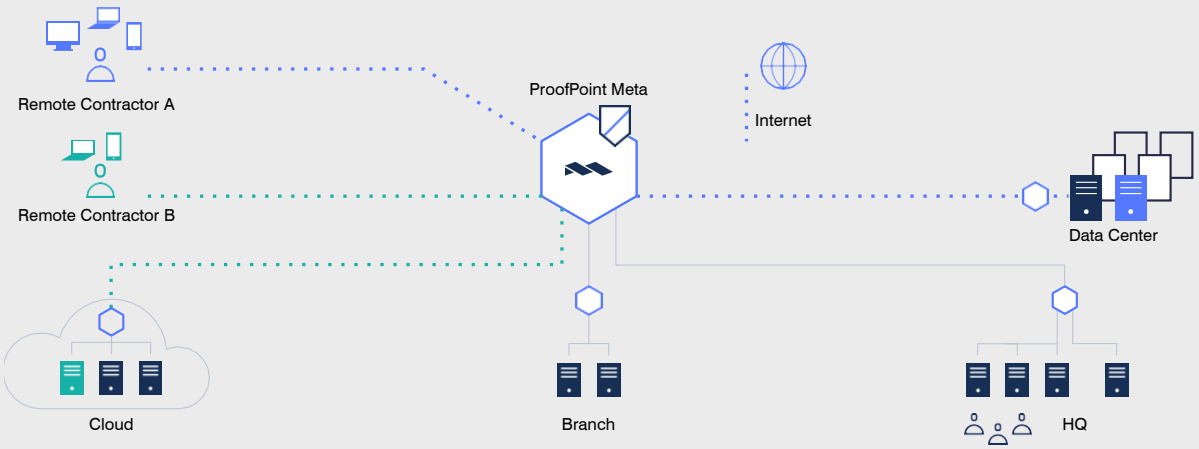
Introducing Software-Defined Perimeters (SDP)

SDP solutions, which implement zero-trust network access, provide a more secure and flexible alternative to VPN for remote users. They enable precise access to applications located on-premises and in the cloud.

In Gartner's words, "Zero Trust Network Access (ZTNA), which is also known as a software-defined perimeter (SDP), creates an identity- and context-based, logical-access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities. The broker verifies the identity, context and policy adherence of the specified participants before allowing access. This removes the application assets from public visibility and significantly reduces the surface area for attack."[5]

In the context of remote contract workers, an SDP solution can enforce a customized policy for each remote contractor's device. Any resource on the network that is unauthorized to a specific user is invisible to that individual. This significantly reduces the potential surface for attackers.

5 Gartner." Market Guide for Zero Trust Network Access." April 2019.



The zero-trust architecture restricts access for Remote Contractor A to one application in the data center and one in the cloud, whereas Remote Contractor B can only access one application at HQ.

Four Reasons to Make the Switch from VPN to SDP

"We are centrally managing a zero-trust network that covers all our applications and data, and our employees, contractors and customers. We're growing quickly and the solution is robust and flexible enough to grow with us—it's easy to onboard new customers and assure the granular security that we need."

Amir Mehler, Cross-tech TL, Via

"With the new system, each user is only exposed to the specific applications he or she needs, regardless of which data center it's located in."

Moshe Magal, IT team Leader, MyHeritage

"The Proofpoint Meta SDP solution was very easy to deploy and is far easier to manage than our former VPN solution. And just as important—our employees are happy to use it."

Amir Adar, CIO, Snowball

The zero-trust approach provides specific benefits for secure remote access of contractors and freelancers.

1. Reduced risk.

The zero-trust mandate to "never trust and always verify" is nowhere more relevant than in the case of contractors. Identity-based access, which is strongly authenticated, verified, logged and audited, combined with isolating and hiding unpermitted assets, significantly reduces your risk of providing contractors access to enterprise resources. Adaptive controls enable policies to be applied as a result of device posture checks, geolocation, and user behavior. So if, for example, a contractor's device suddenly tried to connect from Russia, or the anti-virus is not up to date, access may be restricted.

2. Application-specific access.

By defining granular security policies, you can associate contractors with specific applications and services, rather than providing access to entire network segments.

3. Efficient management.

A central, cloud-based management console enables you to set dynamic permissions for large user groups, roles and individuals, without the need for appliance configuration or synchronization. This makes onboarding new remote contractors much simpler compared to VPN. An administrator assigns the security policies for a new user based on his/her role, and can then send the user a link to access applications from his/her browser, or to install an SDP client.

4. Consistent end-user experience, no client required.

Provide all types of contractors with a superior user experience—whether using an SDP client, or a browser with no plug-in or agent. Using an SDP client, a remote contractor can maintain concurrent connections to multiple applications, regardless of their location. Temporary contractors can use their own, unmanaged devices to securely access designated applications.

Five Steps to Your SDP

Setting up an SDP solution to replace an existing remote access VPN involves five key steps, which are discussed very briefly below. For details, please refer to our paper, "From VPN to SDP: Implementation Guide."

The setup process begins with analyzing the access requirements of your organization (steps 1 and 2). It then proceeds with implementing these policies within the SDP admin console and onboarding users and resources (steps 3-5).

1. Designate Target Applications

If up until now, while using VPNs, your practice was to provide network access to a VLAN or to a range of IPs, with SDP your goal is to provide fine-grained access based on user needs. The first step, therefore, is to create a list of the specific enterprise applications and services you want to make selectively available to each user group. Begin by identifying the list of applications to expose using a fully qualified domain name (FQDN), a local domain name, or IP address and port.

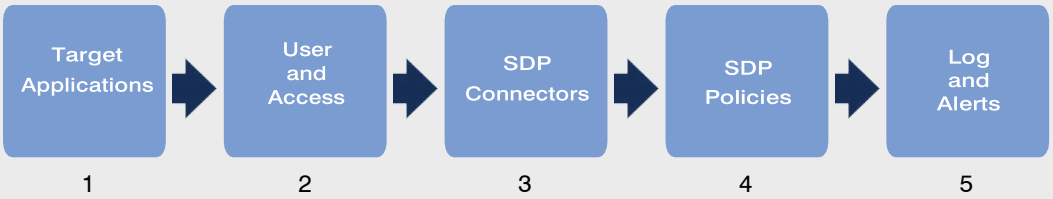
2. Onboard users and define access

Define the remote contractors that will access each of the applications/resources, including the required connectivity and authentication methods. You classify users into groups based on the access requirements (for example, contractors working with R&D can access Jira, but cannot access the Sales/Marketing file server).

Also define the required access type for each of the services and applications (for example, agent-based access or clientless) for access via the browser. Then define the authentication method you would like to enforce for user devices (such as username/password, 2FA, or single sign-on using an IdP).

3. Configure SDP connectors

Lightweight connectors provide a secure authenticated interface between your existing servers and the SDP cloud. Once configured, connectors enable users to access your applications via the SDP. Note that SDP connectors don't require any changes to your existing topology, such as changes to your local DMZ or AWS security groups.



The five key steps for setting up an SDP solution to replace an existing remote access VPN.

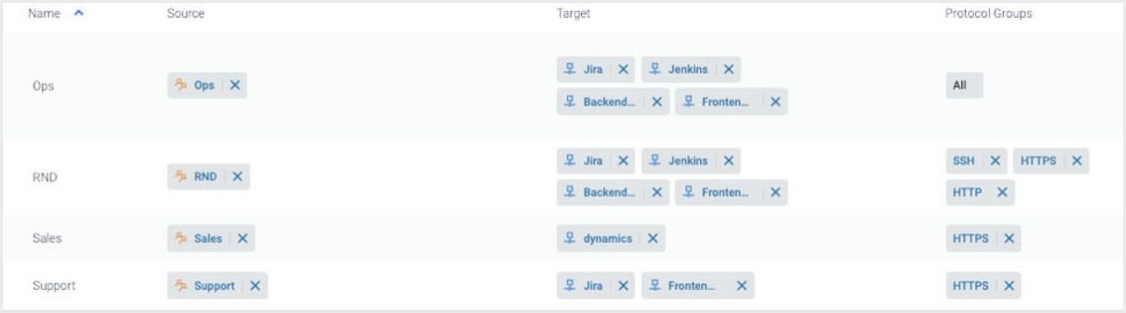
4. Set SDP policies

During this stage, implement the access policies you planned in the previous steps using the SDP admin console. Below, we see an example of the Proofpoint Meta admin console, where administrators define access policies using groups and user identity rather than IPv4 MAC addresses. All access is whitelisted, requiring that a policy is explicitly defined for an enterprise resource, including the specific protocol.

5. Define alerts and audit procedures

Finally, as a CISO, CIO or other IT/security manager, you want to be able to easily track and audit remote user activities. An SDP provides a single pane of glass for tracking access and network activity across systems.

Built-in access logs and alerts let you monitor data including network traffic and activities taken within the SDP system, or various security events like password resets and missing certificates.



An illustration of step 4, setting SDP policies.

Goodbye, VPN. Hello, SDP.

Software-Defined Perimeter solutions and zero-trust network access help meet the challenges of remote contractor work and efficiently address various logistical issues including data classification, segregation of duties, communication, job changes, event identification and risk reduction.

Gartner's recommendation is to "phase out legacy VPN-based access for high-risk use cases and begin phasing in ZTNA (Zero Trust Network Access). This reduces the ongoing need to support widely deployed VPN clients and introduces clientless identity- and device-aware access."[5]

5 Gartner. "Market Guide for Zero Trust Network Access." April 2019.

LEARN MORE

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