WHITE PAPER

Understanding Zero Trust Access (ZTA) in MetaAccess

OPSWAT®

Introduction

The Internet is a marvelous achievement. Its ability to share information instantaneously across the globe has fundamentally transformed businesses and enhanced our quality of life. Ironically, it is that same openness and collaborative nature of the Internet that now represents its most challenging impediment to continued growth and sustainability – Security.

The foundation of modern networks is built on a communication access protocol (TCP/IP) that allows every IP addressable device on the Internet to effectively "see" every other device, which does make it vulnerable to attack. Secure access to applications and data is based on an outdated "trust and verify" approach, which has become a treasure-trove of opportunity for malicious activity and hackers. The security industry has valiantly focused on implementing countless layers of security to guard against the never-ending deluge of cybersecurity attacks and threats. Unfortunately, it is not a matter of if, but when the next security event or data breach will occur. The security industry has now resorted to focusing on how quickly it can identify and remediate an exploitation to limit the organization's risk exposure.

On top of this, the trend towards remote access to applications and data has been increasing for years as more organizations undergo full digital transformations. Recent events have put this trend into overdrive given the quick shift by so many organizations to working from home or needing to provide remote access to third-parties to provide digital services from a distance.

The challenge is that organizations have effectively been exposing their critical computing resources to the world in the same way for over 30 years (since the invention of the firewall), and no matter how many layers of security are added, hackers are able to infiltrate cybersecurity defense services or bring down services using Advanced Persistent Threats (APTs) and Distributed Denial of Service (DDoS) attacks.

For most of those 30 years, Virtual Private Networks (VPNs) have been the go-to approach to secure remote access. They have served us well; however, VPNs are open to attack on the public internet, and when connected, open the network too broadly. VPNs are also not easy to deploy or integrate with the rest of the infrastructure if one tries to provide the required level of security on top of a VPN. Security tradeoffs with VPNs are discussed more below. ovide the required level of security on top of a VPN. Security tradeoffs with VPNs are discussed more below.

Four of the most targeted vulnerabilities in 2020 affected remote work, VPNs, or cloud-based technologies. Many VPN gateway devices remained unpatched during 2020, with the growth of remote work options challenging the ability of organizations to conduct rigorous patch management. [1]

Meanwhile, the need to stay compliant with standards like PCI, GDPR, and HIPAA, just to name a few, is more critical than ever as fines for not being compliant continue to grow. As such, ensuring that users and their devices are compliant is necessary—especially if the users may need to use personal or third-party provided devices to connect. How do you know the device is compliant before it gets access to data, or better yet before it can even see the network port? For example, are you able to ensure the drives are encrypted, antivirus is running and up to date, and not infected by malware?

All of this begs the question: isn't there a better way, a way to not have to simply trust the device is secure? That no hacker will exploit access to a network port or application endpoint they should not even know exists? And to do so in an easier to deploy and manage fashion?

Published October, 2021

Zero Trust Access (ZTA) - A Fundamentally Different and Better Way

Zero trust networking flips the traditional approach of securing access to network resources on its head. Instead of connecting, then authenticating and authorizing; the client is required to first authenticate, authorize, be checked for compliance. Only then is it allowed access. The concepts and term were first articulated by a Forrester[2] analyst in 2010. At about the same time, Google, in response to state level attacks from China[3] formulated their BeyondCorp[4] zero trust approach, Meanwhile the US Department of Defense, as part of its "Global Information Grid" (GIG) vision[5], painted a picture of zero trust based on end-to-end encryption, labeling it a "black core network", and inspiring the "black cloud" terminology often used for network level zero trust approaches.

Zero Trust Network Access (ZTNA) has now quickly progressed through the Gartner hype cycle, and by now many of you have already no doubt read about how this architecture relies on a "verity first, then trust" principle. According to Microsoft, 90% of IT decision makers are familiar with Zero Trust and 76% are In the process of implementation. [6]

For those that need a refresher, here are the core tenets of a zero trust network architecture:

> **Every network should be untrusted**
> Whether it is a corporate-owned network, or one maintained by a third-party (e.g. airport guest Wi-Fi), do not trust it. Just because an administrator calls part of a network secure, or it is inside the "security perimeter", does not make it secure — calling it secure just increases the false sense of security.

> **Every user and device should be untrusted**
> Visibility and access should be permitted on a least-privilege, just-in-time, need-to-use basis. A device or user should not even be able to tell a network resource or application exists unless they are already both authenticated and authorized.

> **Require all access to flow through the zero-trust mechanism**
> The only way to consistently provide zero trust is to force all access to go through the zero trust mechanism. For example, exceptions should not be made for direct access when on-premise while remote access goes through the zero trust mechanism—all potential access is to be untrusted.

> **Assess risk and security both before and during the session**
> Even before the resource is visible for attack and while the resource is in use, continue to reassess risk and trust. The zero trust mechanism must ensure potential connections are from secure and compliant devices before exposing the application or network resource to potential attack and then continue to reassess. If the device is found to be compromised during the session or the user no longer is authorized, the session should be terminated, the user informed as to the reason and provided remediation details.

While tenets and theory on how to achieve better security are great, the real world needs practical tools, and as alluded to above, DISA, based on these tenets, conceived of the Software Defined Perimeter (SDP), the technology behind MetaAccess Zero Trust Access. SDP offsets the weaknesses of TCP/ IP mentioned above, thereby making it safe to expose applications across the public internet, as well as protecting them from the threats that are inside the traditional firewall. Adhering strongly to the tenets of zero-trust, DISA's approach drew the attention of the Cloud Security Alliance which further developed SDP, defining specifications [7] that have now gone through multiple iterations. The CSA SDP design authorizes both the device and user first then checks for compliance before providing network-level visibility to the resources involved, whether it is an application, API endpoint, or network segment.

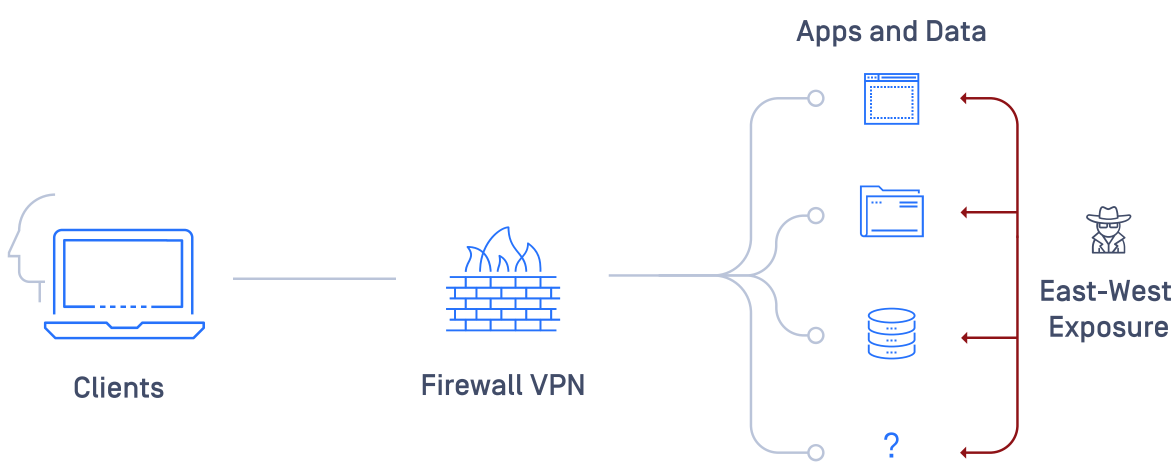
MetaAccess Zero Trust Access (ZTA) borrows much from the CSA's specification. The next section of this document explains this SDP architecture in detail, how it works, and how it offsets the weaknesses of TCP/IP mentioned above—helping prevent the most common network-based cyber-attacks such as DDoS, Man-in-the-Middle (MITM), Server Query (OWASP 10), and lateral impacts of Advanced Persistent Threats. Each year, threats such as these top the Verizon DBIR's list of reported incidents [8] and are reported as the source of the majority of breaches. For example, one takeaway from the recent DBIR is that 61% or more of breaches were caused by credential theft. And according to Digital Shadows, RDP and VPN access credentials have become the most common and valuable listings on cybercrime forums. [9]

Stopping lateral movement through network segmentation and the application of least-privilege, as SDP does, helps not only block lateral movement of system access, but also to contain ransomware attacks. According to the Ransomware Task Force, ransomware payments increased 311% in 2020, at a cost of more than $350 million.[10]

Understanding Zero Trust Access (ZTA) in MetaAccess | Section 2

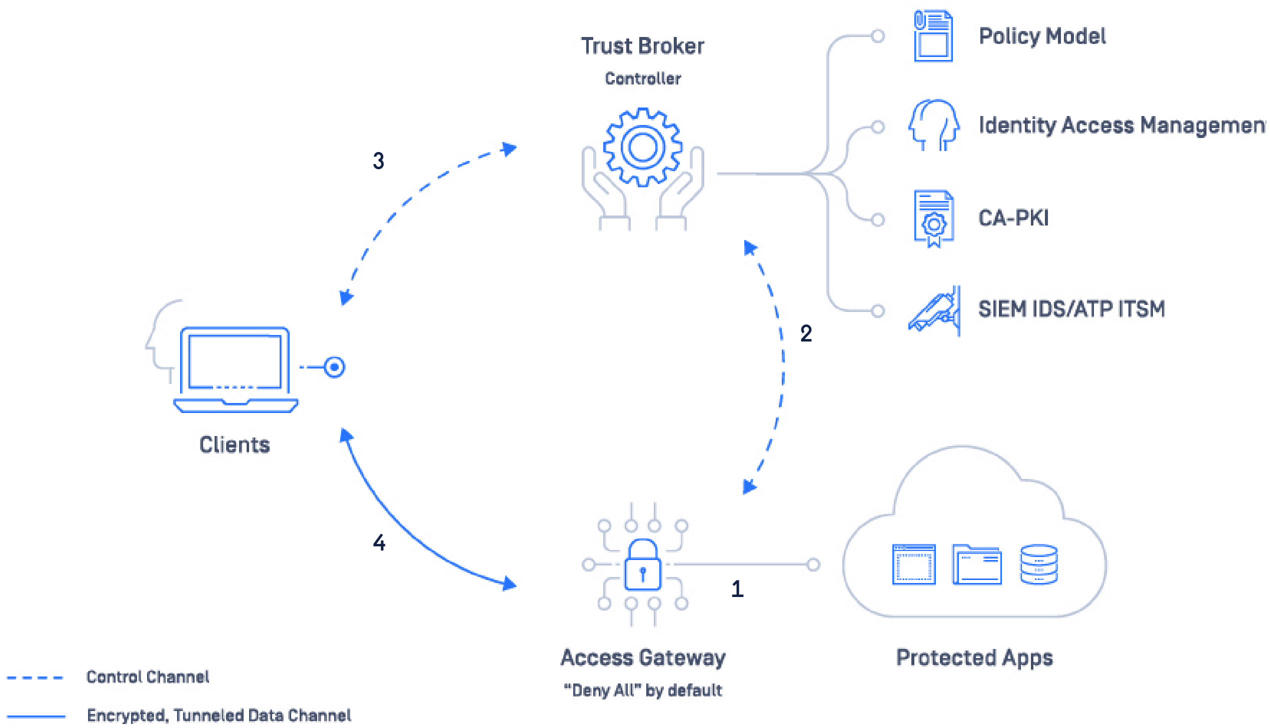
MetaAccess' SDP Architecture

Traditionally, hackers had a wide attack surface through a firewall VPN or LAN connections. Once the user and device connect directly to the LAN or remotely through a VPN, they could access much of the network—that is, they could roam east and west. The organization was at the mercy of either the VPN's security or applications authentication and authorization mechanisms, both of which are commonly open for attack through either known CVEs or zero-day exploits. As a real-world case in point, consider this example where an unpatched VPN server permitted attackers to exploit a CVE and get admin access to a company's server.[11]



As mentioned, Zero Trust Access (ZTA) architecture adheres to the CSA's architecture which has three primary architectural elements: an Access Gateway to protect the resource, a controller to act as a Trust Broker for the gateway, and an app installed on the client device. MetaAccess ZTA uses what is typically referred to as a client initiated zero trust network approach. That is, as explained in the diagram below, the OPSWAT Client sends information regarding the security context to the Trust Broker and ensures the client device and user are properly authenticated and authorized.

[ZTA] Architecture



1. For ZTA, zero-trust is layered on through a dynamic, DENY ALL firewall in the form of the **Access Gateway** in front of applications or network resources being protected. The user facing side of the Access Gateway is configured to block all traffic, and as such, it is impervious to typical network attacks such as DDoS. The gateway is configured to instantly drop any packets that are not specially encrypted and signed, and thereby makes itself invisible to attackers.

2. A Trust Broker controller) acts as the policy engine/ manager. Based on policies, the Trust Broker informs the Access Gateway if a given client is permitted to access an application. Examples include: is the user authorized to access the applications they are attempting to access? Is the device running an up to date virus scanner?

3. The user's device must run an **SDP Client** application to connect. In the case of MetaAccess ZTA, this client app is called the OPSWAT Client. This client app helps to both interact with the ZTA architecture to let the client play its part, but also to optionally check detailed security and compliance policies on the device.

4. IIt is only after the OPSWAT client converses with the Trust Broker, authenticates, gets authorized, and prepares to secure the tunnel, that the client is configured to see the Access Gateway. Meanwhile, in the background, the Access Gateway will have prepared itself to look for the uniquely encrypted and signed packet used to authenticate the Client to the Gateway.

At a lower-level, there is more going on than depicted above. The Trust Broker also integrates with other parts of an organization's security ecosystem to increase security while easing management and monitorability. For example, by leveraging an organization's existing Identity Management System through a SAML integration, ZTA can base authentication and authorization on the centrally managed user and group information. A user can be granted or denied access to an application through ZTA by adding or removing them from an Active Directory group without any change being made directly to the ZTA's configuration.

As initially the Application Gateway is unknown to the Client, when the user attempts to connect an interchange occurs between the Client and the Trust Broker rather than any communication to the Gateway from the Client. As part of that interchange, the Client and Trust Broker exchange keys, certificates, and the necessary other details that enable the Client to establish a mutually authenticated TLS (mTLS) tunnel between itself and the Access Gateway, with the mTLS connection preventing any Man-in-the-Middle (MiTM) attacks.

When ready to connect, the Client first sends a special packet to the Access Gateway to enable what is called Single Packet Authentication (SPA). When the Access Gateway's interface sees that properly signed and encrypted SPA packet, it will permit the inbound connection from the Client, and only that Client. This is cryptographically sound "port knocking"[12], with measures taken to ensure the SPA packet is not decipherable by a MITM, is signed with a certificate pinned to the Trust Broker's CA, encrypted using a fresh public/private key pair, and not at risk of a replay attack.

Ultimately, having established the mTLS tunnel between itself and the Access Gateway, the client is now configured to permit the user to connect to the set of applications that user is authorized to access. Meanwhile, in the background, the client continues to check policy, and will alert the Trust Broker if that user's security or compliance posture changes such that it is no longer compliant with policy, at which point the device can be blocked from further access until it self- remediates.

Technical Use Cases for SDP

1. Place the SDP Application Gateway in front of your most critical systems, making them invisible to attackers and avoiding undue trust of any network or location-thereby also protecting from insider threats and East-West movement of attacks.

2. Encrypt all the way from the client device to the Application Gateway, effectively controlling the security of third-party or public networks, thereby making it safer to trust access from risky locations around the globe.

3. Require client devices to be identified and pass compliance and security checks before connecting to the application gateway, to ensure the endpoints are not the weakest link making it safer to permit personal devices to connect.

4. Regardless of where the user is a working (it could be an airport, from home, or on-premise or other locations); simplify access by providing one way for users to connect, one way to protect, and therefore, one way to configure and support.

5. Require all access to applications or data to pass through the SDP Gateway—even for cloud applications. This enables the same level of control and visibility that was possible when devices and applications were all on-premise.

6. Enable the business to grow faster by easing collaboration. Process owners can securely and easily share specific data or application access to external partners, suppliers, or agencies without requiring the addition or reconfiguration of a VPN or DMZ and do so without increasing the attack surface.

7. In the same way that collaboration is eased with external partners, SDP permits access to be extended quickly and securely to resources during M&A due diligence and post-acquisition while merging operations.

8. Permit cloud-hosted, SaaS applications to securely connect to on-premise networks and access services exposed by APIs, messaging systems, or even permit direct database access..

9. Permit a segment of IoT devices access to the services they require without exposing the traffic or endpoints to attack.

10. Ultimately, modernize by replacing vulnerable VPN gateways. VPNs are exposed to the internet for pre-auth attacks, open broad access to the network, and are difficult to manage when the business expects the capabilities listed above.

SDP as a Next Generation VPN

VPNs have served us well, but now that we have devised an evolutionarily better way to protect resources, there's no reason to use a VPN.

> ***"Gartner predicts by 2023, 60% of enterprises will have phased out most of their remote access virtual private networks (VPNs) in favor of ZTNA and 40% of enterprises will have adopted ZTNA for other use cases."*** [13]

VPNs were designed simply to provide remote access with security as an afterthought. As such, VPN weaknesses cannot stand up to the modern threat landscape; they cannot be stretched or configured to provide the necessary level of protection required. Let's delve into some of these weaknesses:

VPN weaknesses:

1. Once connected, VPN clients typically gain access to a full network—including resources a user is not authorized to access, putting a lot of faith in operating system and application level authentication and authorization controls—which have known weaknesses that in most cases that can be exploited.

2. VPNs are typically exposed to the public internet to permit access from anywhere, which exposes VPNs to many different vulnerabilities like pre-auth attacks. Clients connect first and then are vetted.

3. VPNs are not integrated with the larger security infrastructure, therefore making it harder to achieve and maintain a high level of security resulting in rigidity in the defensive stance with a slower ability to respond to business needs.

4. VPNs are not typically deployed to protect where most attacks originate - internally.

5. VPNs can be difficult to scale up, not just because of the cost per license, but due to the fact that they are often coupled with the firewall or other core services, it can be costly and difficult to scale up and out.

For more perspective on selecting and hardening enterprise VPN and securely working remotely, see this from the US Cybersecurity & Infrastructure Security Agency [14]. Note that while the information sheet does not list using SDP to mitigate the challenges, doing so will help mitigate all the points mentioned.

Meanwhile unlike VPNs, MetaAccess ZTA were designed with security, manageability, and user experience in mind and easily overcome the weaknesses mentioned above:

1. ZTA is granular in terms of permitting access—a least-privileged approach. As such, a hacker that otherwise could exploit system or application weaknesses would not have access by going east-west. Access is limited to only those resources the user is authorized to access.

2. ZTA does not permit a connection to the resource until after authenticating and authorizing the user. As such, there is no vulnerability to pre-authentication attacks as with VPNs.

3. Taking advantage of the ability to limit on a granular, least-privileged approach is much easier; thereby improving security by easing management. ZTA integrates with the existing infrastructure such as IAM to automatically grant/deny granular access to only the resources a user is authorized to access.

4. Whether directly or through automation with IAM tools, ZTA offers integrated Multi-Factor Authentication (MFA), thereby greatly enhancing security by centralizing access control (e.g. ensuing that when an employee is off-boarded or changes roles, their access is removed). MFA is available for end users and administrative users.

5. Access policies can restrict time of day or location access to adaptively apply access policies.

6. ZTA can be easily scaled out and up as additional appliances can easily be added into a highly available clustered pool.

7. ZTA does all of this with a modern, consistent user experience that is the same on premise or remote—effectively "deperimeterizing" from a user standpoint. They do not need to stop and think if they are on-prem or remote and start a VPN client—they always use the SDP client. But meanwhile are still able to launch and use applications as they always have.

Normally, with this number of feature improvements, something would need to be traded away, such as usability, but that is not the case. An SDP like MetaAccess (ZTA) can do all the same tricks a VPN can do—including exposing an entire LAN for remote access. However, why would you do that when you have an easy way to avoid it through SDP?

Understanding tZero Trust Access (ZTA) in MetaAccess | Section 4

Proven Enterprise Level Protection

MetaAccess ZTA builds on deep experience and existing offerings from OPSWAT. The controller and gateway have been integrated into the tried and trusted Zero Trust Access (ZTA) platform which includes the end-point protection capabilities in the form of the OPSWAT Client. Leveraging these technologies, ZTA delivers the broadest set of endpoint security checks on the market.

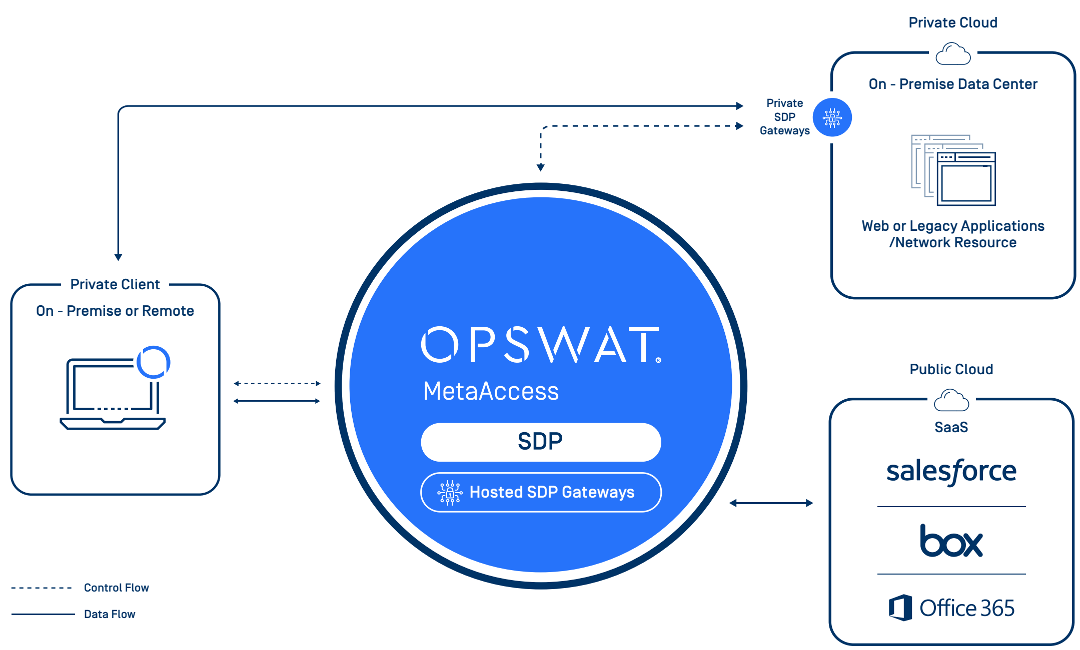
Ease of Deployment and Management

TetaAccess ZTA capability is provided as a cloud-hosted, SaaS offering. Customers can typically do their initial deployment in less than an hour, and then incrementally add the applications and resources to be protected. As with most SaaS offerings, the initial step is registration, in this case through the OPSWAT Portal.

When deploying, the first decision is between the use of an OPSWAT hosted application gateway or a self-deployed gateway positioned in a private datacenter or public cloud hosting service (such as Azure). If most of the applications to be protected are on premise or in a private cloud, then the private gateway should be deployed.

Note that in the diagram below, the Hosted Gateway is provided as part of the OPSWAT MetaAccess Zero Trust Access (ZTA) hosted services (nothing to download or install), and it can be used to control access to cloud services that permit the source IP address to be locked down (permitting traffic only from the SDP Hosted Gateway). The Hosted Gateway can also be used to control on-premise resource access as well, and in that case, the perimeter firewall of the on-premise location would be configured to only allow access from the Hosted Gateway.

As the diagram also depicts, the main advantage of the on-premise gateway is that the traffic flows directly from the client to the on-premise gateway.



If deploying on-premise, multiple, pooled application gateways should be deployed for both availability and scalability. Each gateway can handle thousands of simultaneous sessions. The sessions are distributed in a round robin fashion across the gateways in a pool. If one goes offline, the sessions will be redistributed amongst the other gateways. As such, sufficient provisioning ensures that if a gateway fails, the remainders can handle the distributed load.

The gateways are a lightweight Linux image available for VMware ESXi and Azure. The minimum hardware requirements are:

- **2 CPU Cores; Reserved**
- **4GB RAM; Guest Memory (must be reserved)**
- **10 GB disk space**

Upgrading gateways is easy; a new image can be downloaded, brought up and into the pool, and older gateways successively retired until all are on the latest version.

In addition to the resiliency represented by having multiple load-balanced gateways, care should be taken to ensure multiple, separate network paths to gateways such that if there is a failure in the core of the network, your core's redundancy can enable users to continue to access the gateway. Also, note that it is best not to take the traffic through your own network load balancer, as ZTA is already balancing connections, and in some cases, configuration of the network load balancer could interfere with the operation of ZTA.

The OPSWAT Client, including the ZTA capabilities embedded in it auto-update when OPSWAT releases a new build. Customers do have some ability to control when the update will be applied to a group of devices.

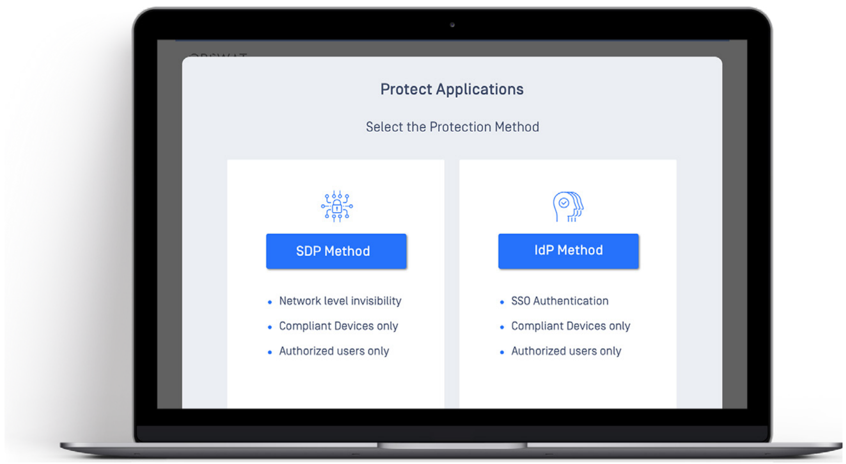
Migrating from your Existing VPN

Given the length of service and the level of dependence on your existing VPN, it would be nearly impossible to transition off it without a migration plan. Because an ZTA overlays on an existing network, it easy to have the existing VPN and ZTA co-exist. It is recommended to start off with a pilot for a couple of critical but narrowly used applications, and then slowly shift applications and network resources to be accessible and protected by the ZTA.

Users can keep their VPN client installed as a fallback while those piloting the ZTA gain confidence. They can use it to continue to access any resources not yet protected by ZTA during the transition. Eventually, once all resources are protected by ZTA, the VPN can be retired—SDP can fully replace any existing VPN.

OPSWAT's Broad Secure Access Solution

While this document focuses on Zero Trust Access' (ZTA) method of application protection, as depicted in the diagram below, Zero Trust Access (ZTA) offers additional ways to secure access. OPSWAT offers the industry's widest set of techniques in a single platform.



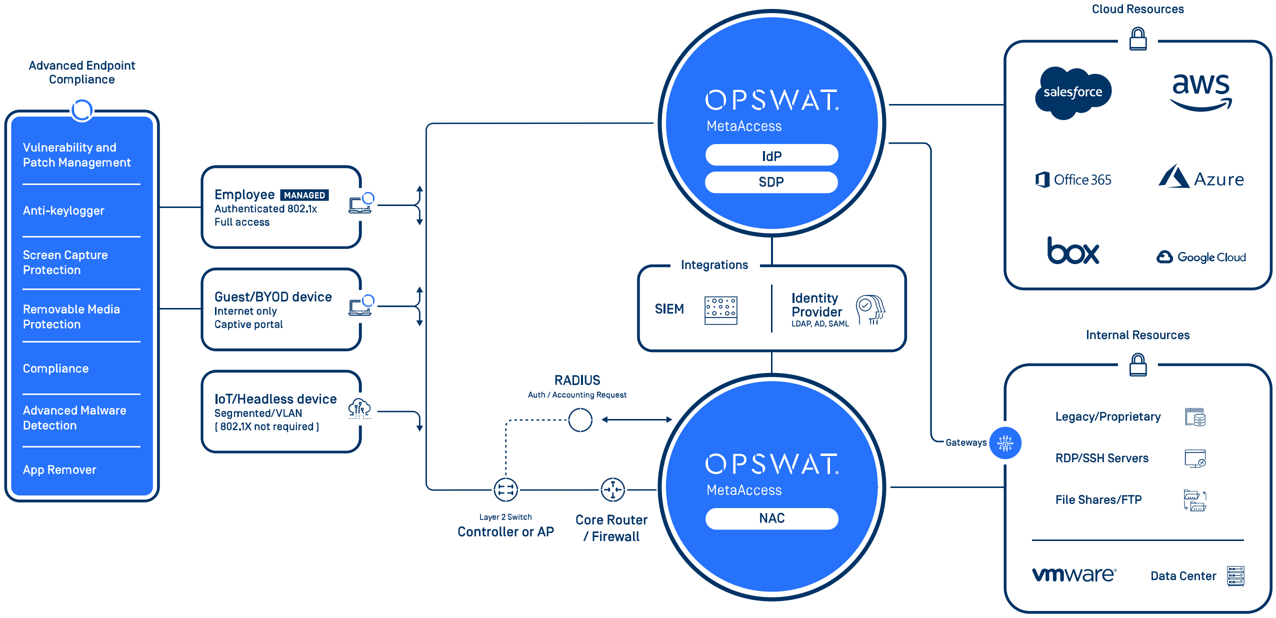
In addition to SDP, Zero Trust Access (ZTA) offers these methods for securing access to resources:

1. **IdP-based method** - A SAML - based approach for protecting applications where it is not practical or possible to put the SDP Access Gateway in front of the resource that needs protecting. For example, some SaaS services do not offer a means to control the source IP address of the traffic, and therefore cannot comply with the tenet of zero-trust that requires all traffic to flow through the zero trust mechanism. The IdP-based approach offered by Zero Trust Access (ZTA) offers a secure alternative method that prevents access to applications until the endpoint is known to be secure and compliant by chaining itself into the SAML authentication flow.

2. **Network Access Control (NAC)** –A full-featured NAC solution that integrates with your on-premise network to protect the devices, data, and applications accessed through it. It includes a RADIUS server with Layer 2 network integration that allows you to authenticate users and devices, control network access using 802.1X and/or by MAC address and assign network privileges for authenticated users and devices. Bulk NAS importing and NAS CIDR notification options are available, along with custom RADIUS attribute creation. Network Access Control and Assignment provides wired port level and wireless SSID control. This control can be done with Dynamic VLAN Assignment, Downloadable ACLs (dACL), and/or Role Based Access such as Roles, Profiles and Filter-Id. Controls can be implemented to restrict access to a specific network VLAN based on allowed host types and/or MAC addresses, a feature particularly useful for assigning IoT devices such as printers, VOIP phones and IP Cameras to a segmented VLAN.

3. **Secure Virtual Desktop Access** - Securing access to applications accessed using Virtual Desktop Infrastructure (VDI) by ensuring the device used to connect to the VDI server is critical, especially when the device is a BYOD. The VDI clients now allow many interactions with the underlying endpoint, and as such it is often important, for example, to prevent screen captures or key loggers. To help ensure the endpoint is secure and compliant before using a VDI client, Zero Trust Access (ZTA) integrates with VDI offerings from vendors like VMware.

4. **Secure Salesforce Access** - Given the level of reliance many companies have on Salesforce, with much of their valuable data on many aspects of their business stored there, securing access and ensuring compliance before users connect can both ensure that data is not compromised and that it is only accessed in a compliant fashion. OPSWAT offers a Salesforce app, available on the Salesforce AppExchange, that integrates with our solution to ensure all risky devices will be denied access to Salesforce until they self-remediate.



Understanding Zero Trust Access (ZTA) in MetaAccess | Section 6

Advanced Endpoint Compliance

As depicted on the left in the diagram above, the OPSWAT Client is used by MetaAccess ZTA to check device security and compliance. This client includes a comprehensive set of capabilities for checking and protecting the device and the data on it. These advanced capabilities include:

- Vulnerability and Patch Management
- Anti-keylogger
- Screen Capture Protection
- Deep Compliance checks
- Advanced Malware Detection
- Potentially Unwanted Application (PUA) Removal
- Removable Media Protection

The OPSWAT client can help protect devices that are on-premise or remote for Windows, macOS, iOS, Android, and Linux. Note that there are some differences in the set of policies supported based upon the openness of the operating system.

When managing thousands of devices, any number of which may be non-compliant at any given time therefore blocking users from accessing applications, the complexity can be overwhelming. This effort can overload the help desk and frustrate users leading to lost productivity. To avoid this conundrum, MetaAccess ZTA offers self-remediation options out-of-the box, minimizing costly help desk calls and helping users get back on task quickly. To maximize productivity, some remediation options can simply be automated, such as updating the virus definitions on local anti-malware software, activating firewall software, and removing unwanted applications even if password protected.

OPSWAT illustrates the endpoint health of the entire environment and delivers control of every device accessing your network and cloud applications, all on a single pane of glass in the MetaAccess portal. Administrators can conduct a detailed security review of any device and monitor which devices access which applications and when. A holistic dashboard illustrates risks, device activities, and current vulnerabilities across the enterprise.

Understanding Zero Trust Access (ZTA) in MetaAccess | Section 7

Conclusion

MetaAccess Zero Trust Access (ZTA) offers the broadest set of approaches in the industry to secure remote access in a zero-trust fashion. While there are several approaches to achieve zero trust at a network level, SDP accomplishes this task in a highly secure, easy to deploy and manage fashion. As discussed in this document, the SDP approach used by MetaAccess Zero Trust Access (ZTA) leverages techniques such as Single Packet Authentication, mutual TLS, zero trust principals and more, to offer this secure approach that can protect cloud or on-premise resources, while also being flexible enough to permit secure access to legacy on-premise file shares.

As you reflect on these security advantages of SDP and shift to considering adopting a solution such as MetaAccess ZTA, the main considerations are:

- Ease of deployment and on-going management compared to alternatives. Easier management further increases security by simplifying the process of onboarding, offboarding, and changing user access helping ensure it gets done correctly.
- Significant help achieving regulatory compliance to meet the standards required for your industry, whether it is PCI DSS,
- SOX, HIPAA, or any of the others listed in the OPSWAT Regulatory Compliance whitepaper.[15].
- For most customers, there are license savings due to the combined solutions—eliminating a separate VPN and set of end point protection products to cover all MetaAccess capabiliites.[16].

Likely future cost savings and peace of mind by avoiding potential breaches, in terms of cost avoided by not having a breach with its related cost of impact on data confidentiality, integrity, and availability, but also potential cost saving by avoiding fines due to breaches.

Right now, it is not a fair fight between hackers and VPN firewall vendors, given the architecture of traditional approaches to application security, hackers will win and there will be more advisories like this one from the NSA.[17] As this paper opened

MetaAccess ZTA offers not only the game changing SDP approach to securing access, it offers a SAML-based and NAC-based approach, as well. The MetaAccess Platform then goes further than other vendors by including industry leading end-point protection in the form of the OPSWAT Client. This advanced endpoint compliance is protecting over 100 million endpoints worldwide. To get more information about MetaAccess ZTA, please visit the OPSWAT Website, and Contact Us to arrange a demo and conversation on your use cases.

Understanding Zero Trust Access [ZTA] in MetaAccess | Section 8

Sources and Reading List

1. Cyber Security & Infrastructure Security Agency. " Alert (AA21-209A) Top Routinely Exploited Vulnerabilities."
https://us-cert.cisa.gov/ncas/alerts/aa21-209a 2021

2. Kindervag, John. "Build Security Into Your Network's DNA: The Zero Trust Network." Architecture."
http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf. 2010

3. Winder, Davey. "How This Chinese Google Hack Has Made Working From Home Safer."
https://www.forbes.com/sites/daveywinder/2020/04/21/how-this-chinese-google-hack-made-working-from-home-safer/. 2020

4. Beyer, Betsy, and Ward, Rory. "BeyondCorp: A New Approach to Security."
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/43231.pdf. 2014.

5. Department of Defense Global Information Grid Architectural Vision.
http://www.acqnotes.com/Attachments/DoD%20GIG%20Architectural%20Vision,%20June%2007.pdf. 2007. pp. 28–30.

6. Microsoft. "Zero Trust Adoption Report.
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdU" 2021

7. Cloud Security Alliance. "Software-Defined Perimeter Architecture Guide Version 2."
https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/ 2018

8. Verizon. "2021 Data Breach Investigations Report (DBIR)
https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf 2021

9. Digital Shadows. "Organizations At Growing Risk From Initial Access Brokers – A Fast Growing Class Of Cybercriminal Who Breach Firms And Then Charge Others To Do The 'Dirty Work.''
https://www.digitalshadows.com/press-releases/organizations-at-growing-risk-from-initial-access-brokers-a-fast-growing-class-of-cybercriminal-who-breach-firms-and-then-charge-others-to-do-the-dirty-work/ 2021

10. Institute for Security and Technology. "Combating Ransomware 2020 - A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force."
https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf 2021

11. Gallagher, Sean. "Unpatched VPN makes Travelex latest victim of "REvil" ransomware."
https://arstechnica.com/information-technology/2020/01/unpatched-vpn-makes-travelex-latest-victim-of-revil-ransomware/. 2020

12. Ranjith, "Fwknop : Single Packet Authorization Port Knocking."
https://kalilinuxtutorials.com/fwknop-packet-authorization-port-knocking/ 2019

13. Weinberg, Neal. "The VPN is dying long live zero trust."
https://www.networkworld.com/article/3487720/the-vpn-is-dying-long-live-zero-trust.html#:~:text=Gartner%20predicts%20that%20by%202023,based%2C%20context%2Daware%20access. 2019

14. Cyber Security & Infrastructure Security Agency VPN Security

15. “Selecting and Hardening Remote Access VPN Solutions.”
https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF 2021

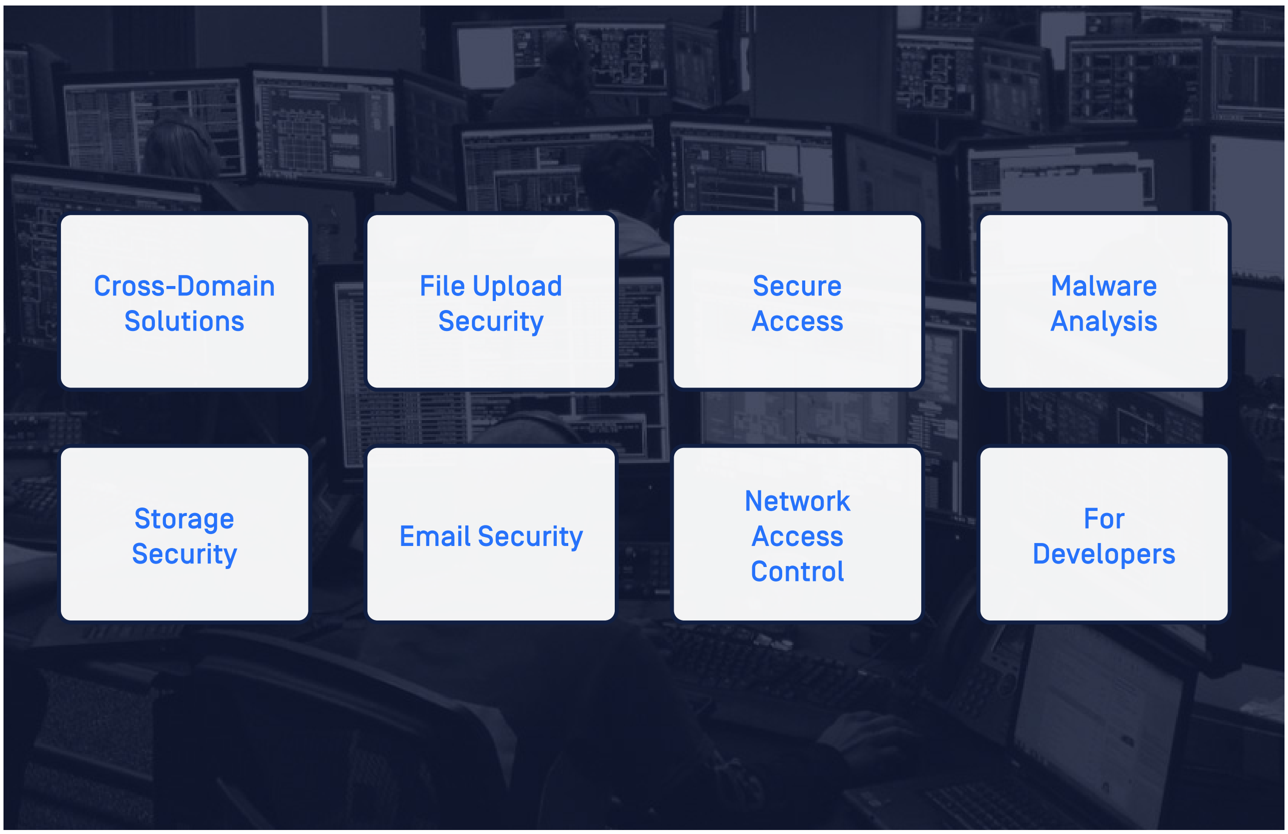
16. OPSWAT Regulatory Compliance Whitepaper
https://info.opswat.com/how-to-achieve-regulatory-compliance-and-certification-with-metaaccess-mx

17. OPSWAT MetaAccess Product Guide
https://static.opswat.com/uploads/files/Product-Guide_compressed-1.pdf?mtime=20210225154430&focal=none

18. NSA Cybersecurity Advisory: “Malicious Cyber Actors Leveraging VPN Vulnerabilities for Attack”
https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1982939/nsa-cybersecurity-advisory-malicious-cyber-actors-leveraging-vpn-vulnerabilitie/ 2019

About OPSWAT

OPSWAT protects critical infrastructure. Our goal is to eliminate malware and zero-day attacks. We believe that every file and every device pose a threat. Threats must always be addressed at all locations —at entry, at exit, and at rest. Our products focus on threat prevention and process creation for secure data transfer and safe device access. The result is productive systems that minimize risk of compromise. That's why 98% of U.S. nuclear power facilities trust OPSWAT for cybersecurity and compliance.



Visit us on LinkedIn, Twitter, Facebook, and YouTube.

Contact us at opswat.com/contact for pricing information, evaluation accounts, technical presentations, or to request a quote.

OPSWAT.

Trust no file. Trust no device.