FORTRA®

DATASHEET (CLOUD DATA PROTECTION)

Fortra ZTNA

Secure access to enterprise private apps and data

Fortra ZTNA is a cloud-delivered zero trust network access solution that provides seamless access to private applications and protects the data stored within these applications, no matter where the user or app is located. Unlike a virtual private network (VPN), ZTNA is a cloud-native service that reduces management overhead, protects the data stored in private applications, and avoids backhauling traffic to deliver a better end user experience.

Challenges

Connections to your enterprise private apps, whether these are deployed in private data centers or in the public cloud like AWS, Azure or GCP, are now coming from countless locations and endpoints — including unmanaged devices and BYOD. While this empowers your hybrid workforce to stay productive, it also expands the attack surface. And the challenge is that traditional access tools like VPNs which work with static security policies, are not easily scalable and thus expose the network to various threats.

Lack of end-to-end visibility and control over data stored in enterprise private apps

Privacy has taken center stage for every organization as new privacy laws impose serious penalties for the leakage of any corporate sensitive information. Organizations leveraging legacy remote access solutions like VPNs do not have visibility of how data is shared and being accessed. With a lack of end-to-end visibility and granular data security, organizations cannot adequately prevent sensitive data from exfiltration.

VPNs add cost, complexity and are difficult to scale

When it comes to remote access to private enterprise apps, organizations often rely on VPNs. But these are typically deployed as hardware within an organization's network near to where applications are deployed. With an increase in the size of the hybrid workforce, workers are spread across multiple locations and geographies, IT is struggling to meet demands around performance and end user productivity as VPNs are not close to where the users are located. This means the traffic needs to be backhauled to a central location before users get access to their applications. This architecture introduces latency and affects performance of these apps and productivity of the workforce.

PRODUCT SUMMARY

Benefits

- Zero Trust access to private applications and data
- Seamlessly discover and onboard private apps on your network
- Prevent data exfiltration from private apps
- Ensure data remains secure as employees, partners and contractors leave an organization
- Integrates with your existing infrastructure
- Helps achieve compliance with local and global regulations

Fragmented IT management with a point product approach

VPNs only cater to applications that are owned and deployed by IT and only address the "access" problem. VPN solutions are typically point solutions and require customers to manage multiple other solutions to achieve zero trust access across all their apps and data. This also requires customers to have large IT and support teams that puts pressure on their bottom line revenues.

Lack of continuous monitoring increases the risk, and affects user experience

Legacy security models that VPNs run on, assume every user and device inside the network is trusted and that puts your infrastructure at risk of unauthorized access. Once a user is inside your perimeter, they have nearly unrestricted access to anything on the network. With an increase in insider threats, VPNs cannot adapt access granted to any malicious insider. To overcome this, IT is forced to define security policies that are overly restrictive and stand in the way of worker productivity.

Solution Overview

Fortra ZTNA is the only ZTNA solution, that goes beyond just providing secure and remote access to enterprise private applications, to secure the data stored in these apps. Whether these applications are deployed in on-prem data centers, or hosted in public and IaaS clouds like AWS, Azure and GCP, ZTNA provides unlimited scalability, better reliability and a much improved end user experience for workers, partners and contractors across all the GEO locations. With a single proxy architecture and a unified agent that also provides secure access to cloud, SaaS and Internet applications, Fortra ZTNA is part of a data-centric tool set from Fortra to deliver a comprehensive cloud security solution.

Visibility of all private applications

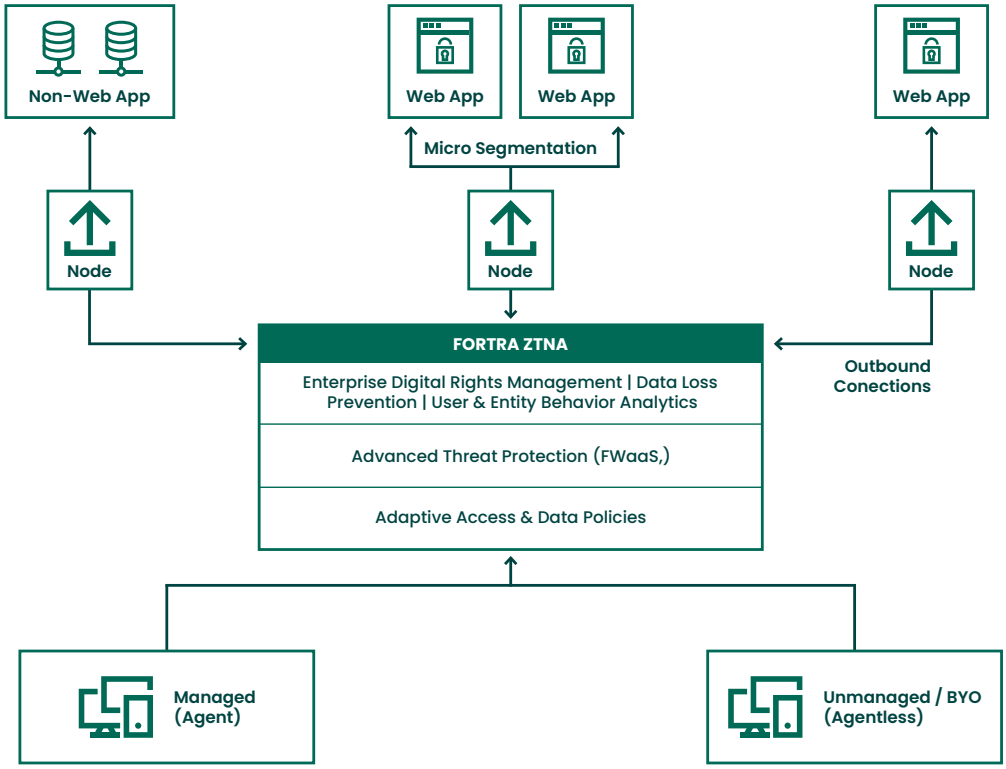
You cannot protect what you cannot see. Before protecting your resources, it is important to know what these resources are and where they are located. Fortra ZTNA provides complete visibility into all applications deployed on your private network, on-prem or in the cloud. Discovery of all applications simplifies onboarding of these apps from your existing VPN solution to ZTNA.

Unified platform with centralized policies and monitoring dashboard

For customers, who have on-prem appliance based products and are looking to a consolidated security stack in the cloud, Fortra offers its cloud data protection product line that provides a unified proxy architecture across its ZTNA, SWG and CASB offerings. With this approach, users have a unified policy infrastructure that allows them to define and enforce global policies that are applicable across all apps and data repositories. A unified approach also allows customers to monitor all user activity across all use cases for accessing internet, private and SaaS applications.

Adaptive access to apps based on user's risk score and device posture

When a connection request is initiated from the endpoint, our agent captures the state of the endpoint device. If the device posture is acceptable, the user is provided a level of access within the app and to the data stored in the app, accordingly. The client on the endpoint continuously monitors the device posture and reports to the platform proxy as soon as it detects any change. This allows customers to implement a true zero trust approach to allow access to all their apps and data.



Data protection engine including digital rights management for private apps

Fortra offers the only ZTNA solution that offers digital rights management (DRM) in addition to the DLP policies for all private applications. With adaptive DLP policies, Fortra ZTNA ensures the data, along with access to private apps, remains secure, reduces false positives, and delivers a better end user experience. As workers share data in the form of files that may have been downloaded from private applications, organizations struggle to ensure data remains safe, especially once it leaves organizational boundaries. Only Fortra protects the data wherever it goes or is stored.

Provide agent-based or agentless access to private apps

Fortra ZTNA provides agent-based or agentless access to enterprise private apps. With agent-based access, customers can get a much richer set of device posture parameters and allows access to all apps, whether they are browser based apps, or apps that require a thick client (TCP and UDP). Agentless access also means customers can get secure access to web based private apps. As most of the customers are moving from thick client based apps to more user friendly, browser based apps, this capability enables them with a much easier deployment model for Fortra ZTNA. If you have contractors and partners, agentless access makes the onboarding of unmanaged devices faster.

Advanced anti-malware engine to protect users from downloading malicious content from private apps

Many enterprise breaches occur when a user unknowingly downloads files infected with malware. Once a device is compromised a hacker can steal any sensitive information stored on the device, including user credentials. Fortra ZTNA inspects the files downloaded from enterprise private apps for any malware, and takes preventive action by blocking the files to be downloaded, if they are infected with a malware. This helps prevent any compromise of the end user devices. It also prevents malware from getting uploaded to enterprise apps and hence prevents lateral movement of malicious files.

Network level segmentation to prevent lateral movement

Fortra ZTNA enables customers to restrict access of a user to a particular application itself.

Here is a comparison of how Fortra ZTNA matches up with your existing VPN solution.

FEATURES	3RD PARTY VPN	FORTRA ZTNA
Prevents lateral movement of users	X	✓
Prevents lateral movement of users	X	✓
Data protection for corporate data stored in private apps	X	✓
High Performance and Scalability	Limited	✓
High Performance and Scalability	X	✓
Unified policies for all SSE use cases including secure access to internet, cloud apps and private apps	X	✓
Unified agent for all SSE use cases	X	✓
Continuous monitoring of all user activity to adjust authentication and authorization levels	Limited	✓
Remote Access	✓	✓
Adaptive access to apps based on user risk score and device posture	X	✓
Support both agent-based and agentless access to private apps	✓	✓

Benefits of ZTNA

Zero Trust access

Fortra continuously monitors the identity of those requesting access to your apps and understands what they need for work. These insights enable a zero-trust approach, providing dynamic identity and context-aware access to data depending on the risk level of the user and device. With both agent and agentless deployment options, Fortra enables secure access to your private apps from any device, whether managed or unmanaged, to support a comprehensive bring your-own-device (BYOD) strategy.

With a built-in Firewall as a Service, Fortra extends inspection of incoming and outgoing traffic beyond HTTP/ HTTPS to include all ports and protocols, enabling granular visibility and access control and into non-web traffic. This provides the ability to apply the same set of security policies across both internet and private access traffic.

Prevent data exfiltration from private apps

Fortra provides built-in protection against insider threats, unintentional data leakage, and ransomware by monitoring anomalous user activity and alerting security administrators to risky or malicious events. This anomaly detection combined with native data loss prevention and digital rights management, helps reduce the risk of both intentional exfiltration, unintentional data leakage, and ransomware. By continuously inspecting traffic coming from the internet and text messages, Fortra also monitors inbound traffic and can prevent malware from being uploaded to a private app reducing the risk to users and the underlying infrastructure.

Simplify migration from your existing VPN

As IT organizations begin moving away from their existing VPN solutions, they lack a lot of information needed to quickly onboard their applications, including visibility into applications their organization uses and how to apply the correct data policies. Fortra helps simplify the migration to a data-centric ZTNA by providing quick visibility into all private apps hosted and accessed within their corporate networks.

Through the onboarding process, you can easily implement granular policies or fine tune existing policies per app, based on the type and sensitivity of the data that resides within the private apps.

Ensure data remains secure as employees leave

Workers come and go and most of the workers take corporate data when they leave an organization. Fortra ensures data remains secure at all times as your employees, contractors and partners leave. With Fortra ZTNA, you can enforce data security policies that enable controls watermarking, redacting information, encrypting files, and setting up expiration dates on documents. These policies can be enforced dynamically based on user's risk, device posture and user location. This gives IT the confidence tokeep the corporate data protected at all times.

Integrates with your existing infrastructure

We invoke the same strong authentication security benefits associated with SaaS apps and web services for legacy, IaaS and private apps. Fortra integrates with your existing multi-factor authentication and identity solutions to reduce user friction and improve overall access controls. This seamless integration with existing access management solutions like Okta, Ping Identity and Microsoft Azure AD, helps organizations cloud-enable their private on-premises enterprise apps without any friction. This scales deployment to a geographically-dispersed workforce while also extending the value of their existing on-premises infrastructure investment.

Help achieve privacy and compliance mandates

Fortra enables organizations to continuously monitor and enforce access control and data protection policies based on the context of devices, users, apps, and data. Tight integration with leading data classification solutions, ensures industry-specific data protection policies can be put in place to meet data privacy regulations. With access limited to only the app and not the broader network, tight access controls are enforced and security is enhanced.

FORTRA

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.

