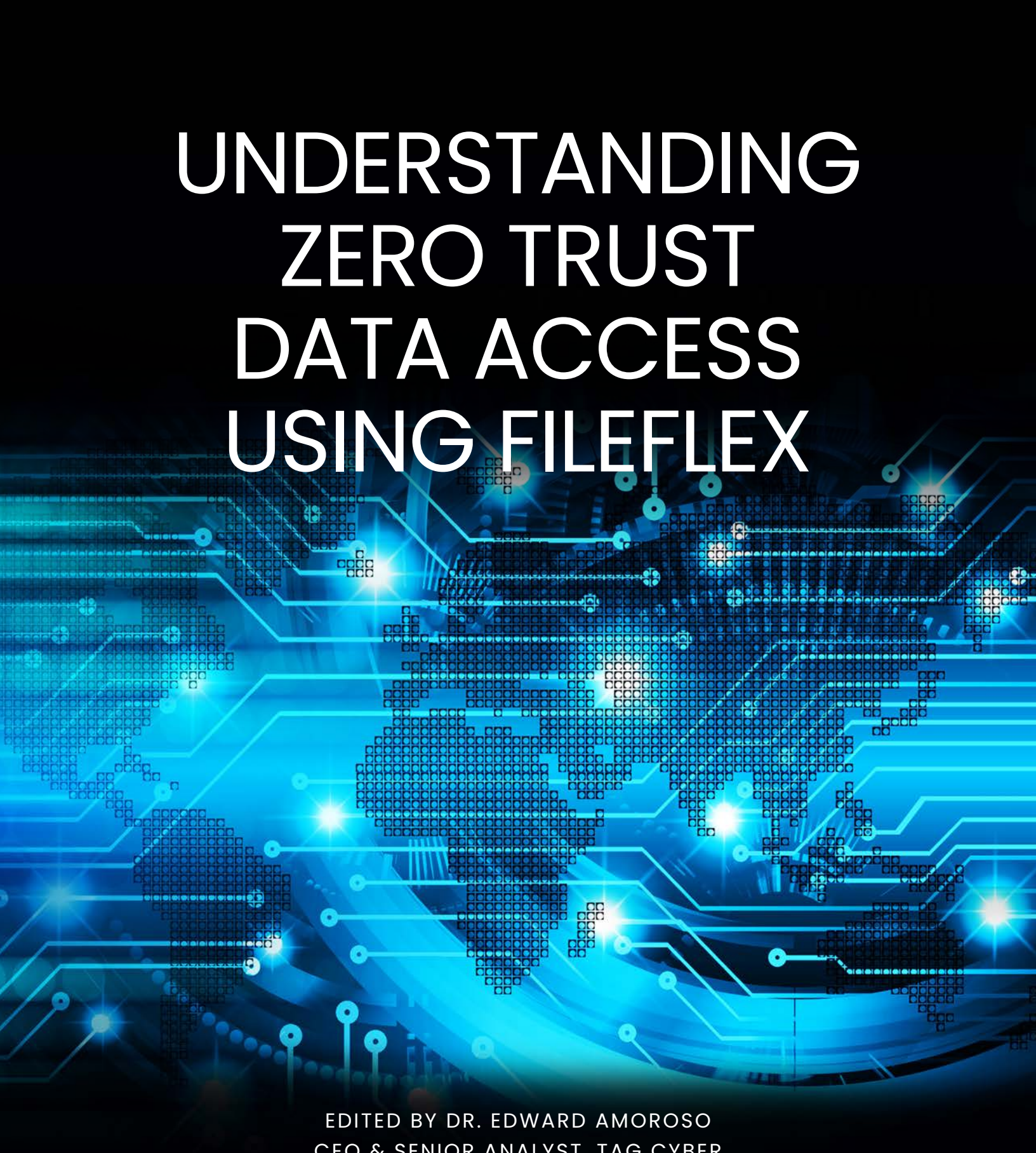
UNDERSTANDING ZERO TRUST DATA ACCESS USING FILEFLEX



EDITED BY DR. EDWARD AMOROSO
CEO & SENIOR ANALYST, TAG CYBER

TAG CYBER qnext

UNDERSTANDING ZERO TRUST DATA ACCESS USING FILEFLEX

EDITED BY DR. EDWARD AMOROSO,
CEO & SENIOR ANALYST, TAG CYBER

This book explains how zero trust data access (ZTDA) can be implemented across an enterprise. The chapters focus on enterprise data sharing, threats to unstructured data, and implementing ZTDA using the commercial FileFlex platform.

HOW DO YOU SECURELY SHARE DATA?

DR. EDWARD AMOROSO, CEO, TAG CYBER

Zero trust network access (ZTNA) is usually deployed to provide internal and external users with work-from-anywhere connections to enterprise applications, without the need for VPN support.

Zero trust data access (ZTDA) provides an effective means for externally sharing unstructured data in a secure manner.

To date, most of the emphasis on *zero trust* in the modern hybrid enterprise has been focused on remote access to network-based resources, usually as a replacement for virtual private networks (VPNs). The resulting zero trust network access (ZTNA) is usually deployed to provide internal and external users with work-from-anywhere connections to enterprise applications, without the need for VPN support.

Obviously, the ability to remotely access a network has always been a critically important function requiring security solutions. Accordingly, many new commercial ZTNA vendors have emerged in this area, several of whom are evolving into more generalized secure network infrastructure providers with cloud-based control. These offerings are sometimes referred to as secure access service edge (SASE) systems.[1]

One aspect of the zero trust equation that has received relatively little attention, however, involves secure remote access to *data*. Users generally view data in the context of files and folders, often hosted in Microsoft SharePoint. As such, one might have expected to see solutions emerge that abstract away the network and application design details in lieu of extending a virtual data access overlay for users working remotely or on premises.

The reality is that solutions to this problem have proven difficult, given the many unique aspects of how organizations create, store, share and protect unstructured data. Luckily, recent advances in a new method known as *zero trust data access (ZTDA)* have led to commercial offerings that can now extend the zero trust equation to remote data access and sharing. This is good news for organizations struggling with this nagging challenge.

This book outlines the basics of the emerging ZTDA model, involving the creation of a secure, remote-access infrastructure that allows for the

internal and external sending and sharing of files and folders, regardless of the details of their underlying network support and hosting implementation. The commercial **FileFlex** platform from cybersecurity company Qnext is shown to provide effective ZTDA capabilities.

In Chapter 2, TAG Cyber analyst **Christopher R. Wilder** addresses risks to unstructured data, while in Chapter 3, TAG Cyber's **Dr. Edward Amoroso** expands on this theme to outline how zero trust data access might work at the file and folder level for customers. Chapter 4 provides an overview of the company's commercial platform for zero trust data access. In the final chapter, TAG Cyber's Dr. Edward Amoroso proposes an action plan for enterprise in this area.

–2–

RISKS TO UNSTRUCTURED DATA

CHRISTOPHER R. WILDER, TAG CYBER

Serious cybersecurity risks can emerge when sensitive unstructured data is not handled and shared securely by an enterprise.

Nearly all data created today is unstructured. The typical enterprise has little administrative control over the inventory, accessibility and organization of its unstructured data, including the shared files and folders of its employees, third-party providers, and even its customers. This control gap creates an undesirable situation, where access to unstructured data is too unmanageable to comply with security policies for local or remote access. The consequences of weak control over unstructured data are as follows:

- ***Unauthorized Disclosure of Sensitive Data.*** When unstructured data is exposed, the consequences can be severe, especially since a high percentage of corporate intellectual property exists in unstructured formats.
- ***Security Compliance Violations.*** The effects of poorly managed, unstructured data can extend to compliance violations, with all the negative impacts one would expect from such deficiencies, especially in regulated environments.
- ***User Privacy Deficiencies.*** The privacy implications of unmanaged data results in non-compliance with standards—such as General Data Protection Regulation (GDPR)—that require a highly granular management of personal data.
- ***Increased Data Theft.*** The more data an organization has, the more likely it will be compromised. When there is a vast amount of unstructured data, determined hackers have an easier time avoiding detection as they gain valuable insights within the enterprise.

These risks clarify how important it has become for organizations to deploy an effective solution for managing and securing unstructured data. The data's underlying representation and use is unlikely to change in such a deployment. Instead, security teams must find ways to integrate good solutions into existing environments so they are not disrupted or slowed down.

Although structured data offers plenty of sensitive information, the real prize that hackers and data thieves are interested in is unstructured data.

Although structured data offers plenty of sensitive information, the real prize that hackers and data thieves are interested in is unstructured data. Unstructured data includes sensitive information in emails and messaging applications such as Slack, along with meeting notes, proprietary source code and the like. Enterprises must be proactive when tackling this growing challenge by implementing the following three steps to identify, quantify and control the risks of unstructured data:

- *1) Identify and Understand the Data Landscape.* The first step in any effective data protection and governance program is to ensure access and visibility into all data sources so that potential risks are known. Not having a comprehensive understanding and insight into enterprise data brings an array of adverse outcomes, such as a lack of governance, compliance and privacy regulations.
- *2) Classify and Quantify the Data.* Data classification is a method that uses related technologies and advanced pattern matching to review and compare unstructured data to file types, thereby identifying and normalizing the characteristics of unstructured data. While data classification tools help with visibility and risk analysis, data quantification maps various risk profiles to ensure regulatory adherence to governance or compliance frameworks, such as HIPAA, PII, GDPR, etc.
- *3) Control the Data.* Proactive data control and risk management allow enterprises to apply risk-mitigation policies for each file based on their risk profile.

Conclusion

CISOs, IT leaders and data owners must understand the roles, responsibilities and outcomes of effective data risk management. Traditional data management has shifted from manually gathering information and creating reports to ensuring continual governance, oversight and risk reduction. Forward-thinking security leaders leverage automated data risk management solutions to provide comprehensive coverage that identifies, quantifies and controls unstructured data, thereby ensuring compliance and confidence when protecting sensitive information.

ZERO TRUST DATA ACCESS METHODS

DR. EDWARD AMOROSO, CEO, TAG CYBER

A ZTDA sharing arrangement makes it just as easy to share a folder with an external business partner as with a local work colleague.

Zero Trust Data Access (ZTDA) is a new model that allows enterprise teams to securely send and share unstructured data across organizational boundaries.

A new method known as zero trust data access (ZTDA) has emerged for protecting unstructured data in the enterprise. It is related to the adjacent zero trust network access (ZTNA) that allows access to networks without regard for an enterprise perimeter. ZTDA also provides secure access, but the focus is on data; it exists under the assumption that perimeters cannot offer a protective ring around data stores, such as SharePoint.

Access Model

Much like the related zero trust network access model, the ZTDA model does not rely on the use of an enterprise perimeter for securing data. In fact, the existence of a corporate firewall managing policy between the inside and outside of an enterprise has no effect on the ability of an employee to share a file, directory or folder with other users, regardless of where they might be situated with respect to the sharing user's network.

This implies that an overlay is required to provide application-level security for file sharing. This should come as good news for security designers, because application-level enforcement of policy is always more flexible and feature-rich than an underlying network counterpart. For example, trying to support a file access policy using traditional 5-tuple TCP/IP metadata is neither easy nor effective.

As depicted in Figure 3-1, the operational goal is that the owners of a file, directory or folder have the ability to create a means for sharing with users via a ZTDA security facility that supports access policy, identity management and credential checking. If working properly, a ZTDA sharing arrangement makes it just as easy to share a folder with an external business partner as with a local work colleague.

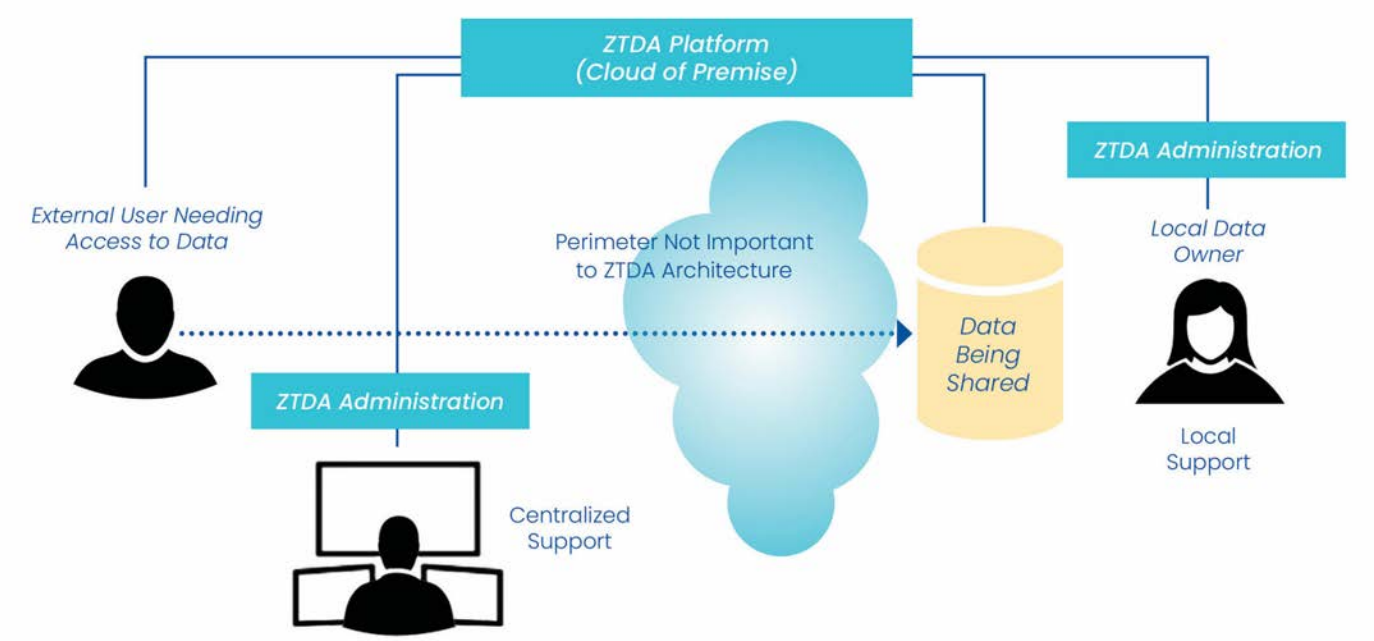


Figure 3-1. ZTDA Architecture

The decision on whether to manage ZTDA functionality from the cloud or premise can be determined by the organization, based on local factors. The coordination of centralized and local data owner policy support can also be arranged by the organization. The goal should be to maximize the flexibility of file and folder sharing with external entities, while also maintaining security and compliance at the organizational level.

Implications for File Sharing

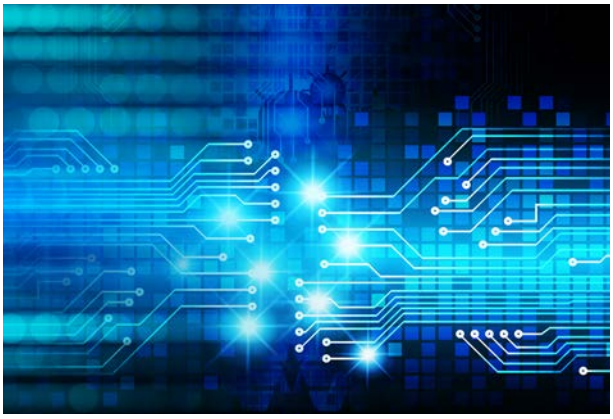
The advantages of ZTDA architecture for sharing are significant and help address many of the challenges that have existed for several years for organizations trying to interact with third parties, customers and other external actors. The more obvious advantages of ZTDA are listed below, but please note that different commercial implementations obviously include their own functionality:

- ***Secure External Sharing.*** This is ZTDA's primary goal, as it solves the problem that most businesses face when they have no idea how to securely share files or folders with external partners. Most of the time, unsecure email attachments or links to a public file sharing platform are used; this might be fine for non-critical data, but sensitive files require more secure handling, which is provided by the ZTDA model.
- ***Reduced Security Burden.*** Introducing a ZTDA overlay allows for the simplification of corporate perimeters and other security tools. VPN access and other means of external sharing are often no longer needed.

Email security overlays might also be removed in lieu of the flexibility afforded by ZTDA sharing platforms for enterprise data owners.

- ***Local Management and Control.*** The definition of management and control policy is moved closer to the data owner with ZTDA solutions. This is helpful, because the data owner will then have the ability to define highly granular policy rules for their files, directories and folders. Obviously, centralized ZTDA controls can also be implemented to complement local handling.

The implementation of ZTDA by commercial vendors is becoming more common. In the next chapter, we showcase this method in the context of the FileFlex platform from commercial solution provider Qnext. The TAG Cyber analyst team has worked with Qnext to review its ZTDA design and has concluded that it compares favorably with the objectives of the model for corporate cyber risk reduction.



THE FILEFLEX ENTERPRISE COMMERCIAL PLATFORM FOR ZERO TRUST DATA ACCESS

DR. EDWARD AMOROSO, CEO, TAG CYBER

This brief chapter provides an overview of the salient features of Qnext's FileFlex Enterprise, a commercially available platform that implements ZTDA for enterprise customers.

Founded in 2016, IT security company Qnext offers the FileFlex Enterprise platform, which supports data access and sharing for enterprise. This commercial, zero trust-based solution is designed specifically to make business processes more effective and secure by supporting sharing and unified access across on-premise, hybrid and cloud infrastructure.

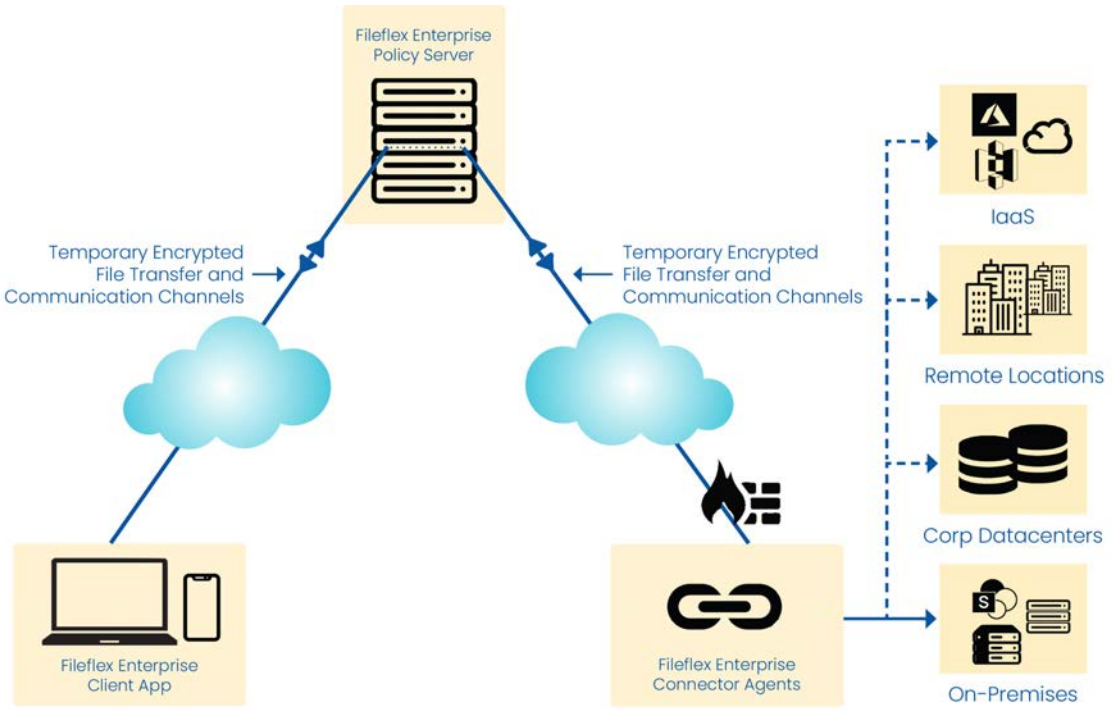


Figure 4-1. Simplified FileFlex Enterprise Architecture

The goal of the FileFlex Enterprise platform is to eliminate unauthorized access to data and services, while making access-control enforcement as granular as possible.

FileFlex Enterprise Architecture

The FileFlex Enterprise solution is designed as an overlay service, built on top of existing data, application and service infrastructure. Thus, the platform's security, control and functionality operate independently of the details of the underlying network, resulting in portability across environments. FileFlex Enterprise also includes encrypted access to data, thereby enabling secure sharing with the ability to manage permissions at a highly granular level.

One unique aspect of the FileFlex Enterprise platform is its policy-decision point for unstructured data access. This is an important feature for enterprise teams hoping to control both structured and unstructured data, as it is not commonly found in most zero trust network access (ZTNA) and application access (ZTAA) platforms. FileFlex fills this gap for both threat avoidance and compliance reporting.

Zero Trust Support

As suggested above, a primary design goal for FileFlex Enterprise is its focus on zero trust. This reflects the obvious changes in hybrid architectures that allow data to be accessible, shared and used across heterogeneous network environments. This patented platform includes the following specific features that enable zero trust:

- ***Confidentiality Requirement.*** Sensitive information is protected from access by unauthorized users and groups.
- ***Infrastructure Separation.*** Data is made available to authorized users without having to give them access to infrastructure.
- ***File Sharing and Transfer.*** Required tools and capabilities are included to enable the sharing and transfer of files and data between users.
- ***VPN Replacement.*** Access to data is no longer dependent on the provision of a virtual private network (VPN).

The goal of the FileFlex Enterprise platform is to eliminate unauthorized access to data and services, while making access-control enforcement as granular as possible. This allows security administrators to match their data-access policies with the objectives of individual business units.

Resource Access Approach

FileFlex Enterprise also offers support for remote access to resources that might be located on cloud-hosted, on-premise and SharePoint storage and puts them under a single pane of glass. A key aspect of its virtual data security overlay is that users have access to network resources without being on the network infrastructure; this separation helps keep unauthorized users away from network resources.

Access is provided in real time via the FileFlex Enterprise connector agent, with the security being invisible to the user. This stands in contrast to other solutions that either replicate information to another server to which they have access using enterprise file synchronization and sharing (EFSS) or

give direct access to the infrastructure via a VPN or remote desktop software. FileFlex Enterprise abstracts the infrastructure from the data, thereby protecting the organization's infrastructure from direct and unauthorized access.

File Synchronization

FileFlex Enterprise's file sync and share (FSS) and EFSS cloud-sharing solutions all provide the ability to share files. The main difference, however, is that cloud-sharing solutions do not have the capability to access the organization's infrastructure remotely, meaning organizations need cloud solutions for file sharing, and VPNs for remote access.

In addition, FileFlex Enterprise allows for the sharing of any file in the entire hybrid-IT multidomain infrastructure, while cloud solutions can only share files that are duplicated to their servers. That is because cloud solutions are based on a centralized cloud architecture, while FileFlex Enterprise is an overlay built on a zero trust architecture. Cloud solutions create fragmented separate silos, compromise privacy and require sharing and duplication, thereby increasing the threat surface. They also lack the ability to access and share self-hosted and MS-hosted implementations of SharePoint. The FileFlex Enterprise solution addresses all these issues, along with much more.

PROPOSED ZTDA ACTION PLAN FOR ENTERPRISE

DR. EDWARD AMOROSO, CEO, TAG CYBER

There are three high-level management tasks that should be present in most practical ZTDA action plans.

Enterprise teams interested in implementing zero trust data access (ZTDA) can create and tailor a ZTDA action plan consistent with local requirements, constraints and objectives by following the three high-level management steps outlined in this chapter.

The goal of implementing zero trust data access (ZTDA) to protect unstructured data in the enterprise can only be reached through proper management and oversight. Reducing organizational dependence on perimeters for external data access, often through the replacement of legacy virtual private network (VPN) solutions, is easier said than done. Therefore, enterprise teams are strongly advised to emphasize careful planning.

This chapter introduces a general action plan for any enterprise that seeks to implement secure external data access under the assumption that traditional firewall perimeters will not serve as the main compliance control or security mediation component. Instead, the use of ZTDA solutions, such as those from Qnext, are assumed to be the goal.

While every enterprise organization certainly has its own unique requirements, constraints and objectives, there are three high-level management tasks that should be present in most practical ZTDA action plans. Readers are advised to peruse these details and then use this high-level guide as the basis for tailoring their own local ZTDA implementation action plan.

Step 1: Assessment of Existing External Data Access Posture
The first step is to perform an assessment on how the organization currently supports secure remote access to enterprise data. Such data is usually represented as files and folders, often hosted in Microsoft SharePoint. This assessment should take inventory of how the organization creates, stores, shares and protects unstructured data, while including all aspects of external data access, such as those from customers and third parties.

One challenge that might emerge in this step is that a typical enterprise might include a myriad of different, and often incompatible, solutions for external data access. These could include one approach for employees working virtually (perhaps using a VPN), another approach for suppliers requiring data access (perhaps using tunneling solutions), and yet another solution for merged companies or acquired entities.

Step 2: The Prioritization of Functional and Assurance Requirements for Data Access

Once the assessment of existing external data access has been completed, it is recommended to perform a prioritization step. This involves the enterprise team explicitly designating the relative importance of requirements in two key areas: security and compliance. Furthermore, these should be further broken down into two types of requirements: functional and assurance. These areas of emphasis can be combined into a decision matrix, as seen in Figure 5-1.

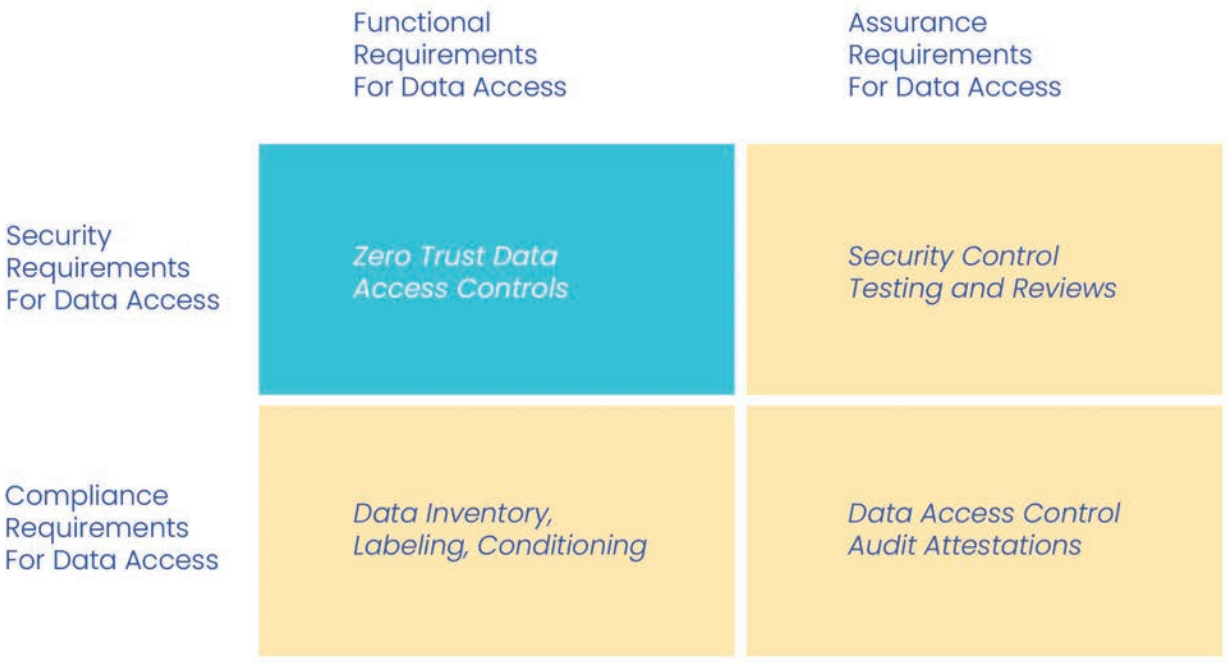


Figure 5-1. Matrix of Prioritization Requirements for External Data Access

Typical enterprise teams will find that their organization's mission guides the relative importance placed on ZTDA requirements in the matrix. For example, banks and financial institutions will highly prioritize the assurance aspects of compliance, whereas less regulated entities, such as retail organizations, might place a higher priority on the functional aspects of security.

Step 3: The Review, Selection and Trial of a Suitable ZTDA Platform
The final step in the ZTDA action plan involves the review, selection and trial of suitable ZTDA vendors. The inventory performed in the first step will help define the integration and migration aspects of the proposed plan. The prioritized matrix entries in the second step will help create a suitable review rubric for the various commercial ZTDA vendors under consideration.

As one might expect, this book includes considerable details on the Qnext FileFlex platform, and buyers are advised to include this platform in their ZTDA action plan. Nevertheless, TAG Cyber analysts are always available to assist enterprise teams in their review of all possible commercial vendors in a given solution area. Enterprise buyers of ZTDA are thus encouraged to reach out to TAG Cyber for assistance in this regard.

FOOTNOTES

CHAPTER ONE

[1] *Customers of TAG Cyber's Research as a Service (RaaS) can review modern ZTNA and SASE commercial offerings either through the perusal of curated libraries on the TAG Cyber RaaS portal or through live tailored engagements with expert analysts*

ABOUT TAG CYBER

TAG Cyber is a trusted cybersecurity research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay- for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

ABOUT QNEXT

Qnext mitigates the risk of ransomware crises by offering a proprietary Zero Trust Data Access platform called FileFlex Enterprise. Built with patented technology, FileFlex Enterprise is an overlay solution that enables any major sector organization—from healthcare and financial to public transportation—to unify remote access, sharing and governance of unstructured data storage across entire hybrid-IT and multicloud infrastructures.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Dr. Edward Amoroso

Publisher: TAG Cyber LLC. ("TAG Cyber"), TAG Cyber, LLC, 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman, (lgoodman@tag-cyber.com), if you'd like to discuss this report. We will respond promptly.