Zero Trust Remote Data Access and Collaboration - *Technology Primer*

fileflex enterprise

"By 2023 60% of enterprises will phase out most of their remote access virtual private networks (VPNs) in favor of a Zero Trust Architecture" – Gartner

We have seen dramatic change in how employees work and where they work from in the 21st century. Tools such as Software-as-a-Service, VPNs, remote desktop and cloud storage now allow organizations to contract with a remote, virtualized work-force and gig-based workers. The result of these enabling technologies has been our modern distributed workforce.

But having the tools to enable a distributed workforce has introduced significant issues with security and privacy. For example, providing remote network access via a VPN also provides access to the entire network infrastructure. Storing files for remote access, sharing and collaboration with third-party cloud providers introduces compromise to the privacy and confidentiality of those files as they can be legally inspected and secretly exfiltrated by third-parties. These issues are inherent to the technologies used and can prove difficult and very technical to control.

The switch to zero-trust

Secondly, it has become increasingly clear that the traditional approach of using perimeter defences to secure an organization is inadequate. The perimeter approach of using firewalls and anti-virus software is now being augmented with zero-trust measures. Zero-trust is an approach of always authenticating and always verifying all transactions all the time with a "never trust, always verify" model where access to data is secured and controlled through a zero-trust policy engine.

The emergence of Hybrid IT

Third, with the introduction of Infrastructure-as-a-Service providers such as Amazon AWS and Microsoft Azure, the IT infrastructure of organizations has moved from on-premises only to a hybrid structure of on-premises and cloud services. Although these new services have great administration tools for IT, they sadly lack tools for end-users. Further, they transfer some governance and control to the third-party.

New, much more secure technologies that conform with zero-trust process-es need to be deployed to ensure that remote access and shared data and collaboration are safe for these new work- force norms.

The Remote Worker Trend will become the new norm for Enterprise.

The remote workforce has escalated by 400% in the past decade – according to a recent GetApp Report. And with the arrival of COVID-19 and pandemic contingency planning – the remote workforce evolution is bound to accelerate. New, much more secure technologies that conform with zero-trust processes need to be deployed to ensure that remote access and shared data and collaboration are safe for these new workforce norms.

Introduction

This paper outlines in detail the zero-trust security architecture and robust feature set of FileFlex Enterprise remote data access and collaboration platform for all content located on a hybrid IT infrastructure.

FileFlex Enterprise – A zero-trust solution for Hybrid IT

FileFlex Enterprise is the world's first remote data access, sharing and collaboration solution designed from the ground up to be zero trust compliant. FileFlex Enterprise provides unified access across on-premises and multi-cloud storage solutions for a secure hybrid IT data access, sharing and collaboration solution.

What Makes FileFlex Enterprise Different?

From a single pane-of-glass FileFlex Enterprise provides IT controlled access, sharing and collaboration to all content located on your hybrid IT infrastructure – no VPN required. And securely move, copy or migrate data between any content location. This includes remote office, on-premises corporate server, department NAS, an individual's PC, private cloud, public cloud, SharePoint or Infrastructure-as-a-Service storage such as Microsoft Azure, Google Cloud or Amazon S3.

FileFlex Enterprise augments traditional perimeter-based security by always authenticating and always verifying all transactions all the time with a "never trust, always verify" model where access to data is secured and controlled through a zero-trust policy engine. It is the perfect tool for organizations that are moving their cyber-security paradigm from the traditional perimeter approach to the zero-trust model.

- Unlike a VPN which conforms to a perimeter access model, FileFlex Enterprise conforms to a zero-trust model which is inherently more secure whereby information access is controlled and all users and all devices must always be authenticated.

- FileFlex Enterprise provides access to data without providing access to the infrastructure. Competitive solutions either replicate information to another server to which they have access (EFSS) or they give direct access to the infrastructure (like a VPN or remote desktop software). FileFlex Enterprise abstracts the infrastructure from the data. This protects against direct and unauthorized access to the organization's infrastructure.

- FileFlex also enables organizations to manage their information from a reduced threat surface perspective. Data can be accessed and shared from where it exists today, behind existing security controls and requires no additional controls to provide an additional layer of authentication, encryption and governance over business information while significantly reducing the risk associated with cyber-attacks such as data exfiltration, phishing and ransomware.

- In addition to communicating through encrypted channels, FileFlex Enterprise also includes the option of encrypting the data stream itself. Double encryption is enabled via the PKI server and ensures that data is protected in transmission all the way from the sender

to the receiver to protect it against snooping, intercept and man-in-the-middle threats.

- Access control is extended to the user and device through the use of multi-factor authentication, SSO, device authentication, enforced password policies and session timeout policies.

- FileFlex Enterprise brings data governance to remote data access, sharing and collaboration. IT controls sharing permissions and user permissions over all storage locations even to file level granularity, and it honors Active Directory, LDAP and device permissions. The administrative console includes a view of all activities of all users that can be monitored in real-time or exported to your incident management software.

FileFlex Enterprise augments traditional perimeter-based security by always authenticating and always verifying all transactions all the time with a "never trust, always verify" model.

The Components of the FileFlex Zero Trust Architecture

FileFlex Enterprise has a unique patented architecture designed to:

1. Protect confidentiality of sensitive information by providing access to data without providing access to the organization's network infrastructure
2. Provide IT the tools they need to control file sharing
3. Protect the transfer of information
4. Allow for only authorized access to content and,
5. Protect user credentials

The FileFlex Enterprise solution is comprised of 3 main components. All 3 components are required in order to make the solution work. The 3 components are:

- FileFlex Enterprise server (and PKI server)
- FileFlex Enterprise Connector Agent
- FileFlex Enterprise Client App

All 3 components use encryption (AES256 symmetric encryption) in various ways in order to protect the user data, internal data, tokens and communication channels. The use of encryption coupled with architectural design and process flow ensures privacy, security, protection of credentials and authorized access to content.

Diagram 1 outlines a high-level architecture of the overall solution and a logical view of the interaction between the broader 3 main components of the system.

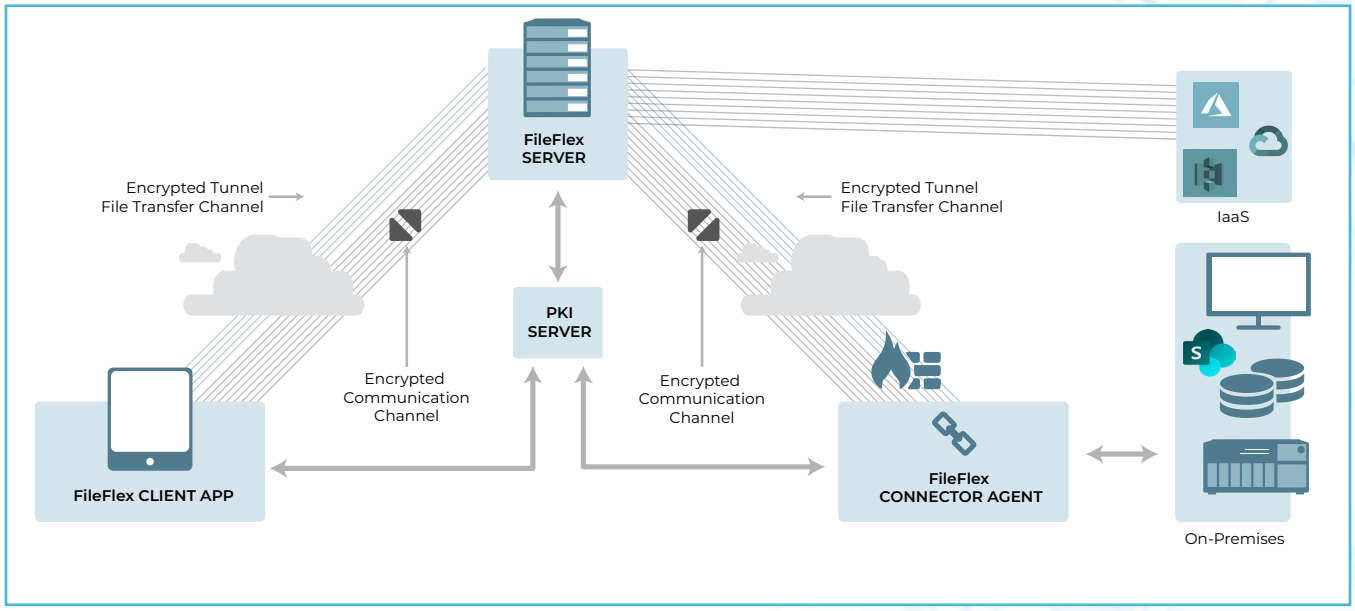

Diagram 1 - Zero Trust Architecture of FileFlex Enterprise

The FileFlex Enterprise Server

The FileFlex Enterprise Server is a public facing server that is accessible on the internet and provides access to the service. The server manages access rights to the service by validation and authentication and acts as a relay service between the authenticated users and the content sources that they have rights to access. The FileFlex Enterprise server does not hold any user content data and only manages and enforces the rights and permissions of authorized users of the system. It acts like a switchboard to connect users to their files in their source locations and like a policeman to enforce access policies. Thus, it helps protect the organization because it does not store any files or content and it does not store any credentials.

It is important to understand that the FileFlex Enterprise server is actually a cluster of servers that act together to behave as one and provide the functionality of the FileFlex server / service. It is also important to understand that all the server components mentioned here are virtual servers and not physical appliances and reside in a VM on a single physical machine. However, most of these individual server components may be spread across different physical machines in the cluster for enhanced robustness and security.

The public-facing FileFlex Enterprise 'web' servers are separated from the protected connector agents by a firewall. The public servers are responsible for communicating with the FileFlex users, while the connector agents are responsible for accessing remote data.

> ***"The FileFlex Enterprise server does not hold any user content data and only manages and enforces the rights and permissions of authorized users of the system"***

All external server communications are performed on encrypted channels. The FileFlex Enterprise server only communicates with the connector agent & client application. Connections are made using HTTPS. The server uses dedicated ports to communicate with both the FileFlex connector agents and the FileFlex client application which must be open inbound to server and open as bidirectional.

FileFlex Enterprise PKI Server

> ***"The FileFlex Enterprise PKI server offers double encryption, which is a feature that allows end-to-end encryption from source all the way to destination"***

A public key infrastructure (PKI) is a set of roles, policies and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption.

The FileFlex Enterprise PKI server offers double encryption, which is a feature that allows end-to-end encryption from source all the way to destination. This is a very effective protection against man-in-the-middle and impersonation, snooping and intercept to provide very strong security of data transfers. When selected, the content owners will be able to select whether or not they want to enable double encryption on a per-content-source basis. A side effect of such a configuration (when double encryption is enabled by the content owner) is that the content cannot be consumed from a web browser. Users will still benefit from traditional single tunneling encryption as well as other security options, which allows for browser-based content consumption.

The FileFlex Enterprise Connector Agent

The FileFlex connector agent is a software only component that runs on a device located on the corporate infrastructure behind the corporate firewall. The connector agent can access any device or storage located on the same infrastructure, on behalf of the user using the local permissions of the user. The main purpose of the connector agent is to perform requested task (access, relay and manipulate data) located on the same infrastructure, on behalf of a user as if the user were physically present on that infrastructure. The connector agent is also responsible for encryption and decryption functions for all data transmission, as well

as managing revisioning and aspects of collaboration functions.

There exist multiple flavors of the connector agent for all types of devices, OS & architecture.

OS:	Windows, Mac, Linux
CPU:	Intel, ARM
Devices:	NAS, Routers, Servers, Desktops, Laptops

"The connector agent is also responsible for encryption and decryption functions for all data transmission."

All external communications from connector agent to the FileFlex Enterprise server are performed on encrypted channels. Connections are made using HTTPS. The connector agent is designed to only communicate with the FileFlex Enterprise server by establishing an outbound connection using a number of secure measures to ensure that connections are only to designated FileFlex servers. By establishing outbound connections, this ensures that no new ports need to be open on the corporate firewall thus eliminating the risk of external access to the connector agent inside the corporate infrastructure. The connector agent uses dedicated ports to communicate with the FileFlex server which must be opened outbound only and as bidirectional.

FileFlex Enterprise Client App

The FileFlex Enterprise client app provides a mechanism for the user to access, browse, manipulate and share any content from a single dashboard. The FileFlex Enterprise app works in conjunction with the FileFlex server to allow the user to perform these actions securely with assigned privileges and enforce permission activities such as download, view-only, edit and upload. FileFlex does not use link-based sharing. Every user must log into the system using the client application, be authenticated to the server, their privileges are communicated and bound to their app. The client app, in conjunction with the server, assists in enforcing the rules and privileges assigned to the user. When FileFlex generated links are used and copied into an email, the link never gives direct access to the content. Instead FileFlex generated links open the FileFlex app and authenticate the user. This user authentication is a key component to give IT control and tracking over the file sharing of the organization and to mitigate against spoofed trusted sources.

FileFlex Enterprise is account-based, not device-based, meaning a user logs into their account from any device – whether Windows or Mac PC, or iOS or Android smartphone or tablet, or web browser. When the user logs in, they get access to every connector agent that is bound to their account as determined by IT and enforced by the server. Those agents can be located on any and every network and facility the organization has globally and all accessed through the client app via a single-pane-of-glass dashboard and bound to the users account to allow access, sharing and collaboration of any file in the organization no matter where located all the while staying under the control of IT.

"The connector agent is designed to only communicate with the FileFlex Enterprise server by establishing an outbound connection using a number of secure measures to ensure that connections are only to designated FileFlex servers"

All external communications are performed on encrypted channels. Connections are made using HTTPS. The client app is designed to only communicate with the FileFlex Enterprise server on outbound bidirectional communication channels. The client app uses dedicated ports to communicate with the FileFlex server which must be open as bidirectional.

How It Works

When a user wants to access, share, collaborate, stream or manage something, they navigate to and click the file in the client app. The client app makes a request to the FileFlex Enterprise server and the server determines whether the user has the privilege

to access and perform the request. If it does, the server knows the connector agent that the user is bound to that has the data. The server contacts the connector agent and forwards the request along with a unique token ID to the connector agent. The connector agent receives the request along with the token ID which it uses to pull the user's AD/LDAP credentials from it's encrypted DB. The connector agent then impersonates the user and navigates the infrastructure and performs the request on behalf of the user using the user's credentials. The connector agent accesses the data, encrypts the data and streams it over the encrypted communications tunnel back to the user almost instantly.

"Every user must log into the system using the client application, be authenticated to the server, their privileges are communicated and bound to their app."

"Seamlessly supports secure zero-trust access, sharing and collaboration from dedicated IaaS servers with suppliers such as Amazon, Azure and Google"

Protection Against Specific Vectors Used To Deliver Malware

To further understand the security benefits of FileFlex, it is important to understand how it helps protect against specific vectors used to deliver malware or to extract confidential information:

"FileFlex mitigates the download of self-propagating trojans, keyloggers, worms, spyware or rootkits"

Vector to deliver malware: The embedding of malware in email links and attachments targeting your organization

By far the most common method of sharing files is either to attach the file to an email or to embed a link to a cloud-based file sharing service. The email can spoof the sender and disguise the attachment/link such that the receiver in your organization thinks it is a legitimate file from a trusted source. FileFlex mitigates the download of self-propagating trojans, keyloggers, worms, spyware or rootkits that can be introduced through the use of spoofed email senders with embedded links to cloud-based file sharing services and the use of disguised email attachments. With FileFlex you are giving share recipients controlled access to files in their source locations. The access is always through the FileFlex application and never through the use of attachments or external links. The share notification emails or share notification links used by FileFlex always make the recipient open the app to get access to the files. Access to the shared files itself goes through user authentication and layered security.

Vector to extract confidential information: Man-in-the middle, snooping and intercept

FileFlex protects against man-in-the-middle, intercept and snooping using 3 levels of encryption. 1) All communications are sent through AES 256 encrypted tunnels; 2) The optional PKI server (at no additional cost) can encrypt the data stream itself from sender to receiver; and 3) the secure enclaves of Intel SGX can be used to generate the encryption keys to protect communications even on systems that themselves are compromised by malware.

"FileFlex protects against man-in-the-middle, intercept and snooping using 3 levels of encryption. "

Vector to extract confidential information: Unauthorized access

FileFlex has many mechanisms to protect against unauthorized access such as two-factor authentication, device authentication, single sign-on, permission management, password management, share expiry and session timeout.

"FileFlex has many mechanisms to protect against unauthorized access"

Optional Intel SGX Hardened Encryption

Intel Software Guard Extensions (SGX) bring a fundamental change to security by providing hardware-level trusted execution of applications. FileFlex Enterprise leverages Intel SGX to provide platform hardened generation of encryption keys. When used with Intel SGX, FileFlex can deliver enhanced integrity and enhanced security of all data that is accessed by a user and with improved prevention of man-in-the-middle, impersonation, snooping and intercept attacks **even on a system that is compromised** (at the application level).

Intel Software Guard Extensions (SGX) Technology is a set of CPU instructions from Intel that allows user-level code to allocate private regions of memory, called enclaves, that are encrypted and protected from other processes running at higher privilege levels on the system. The Intel SGX enclaves or isolated portion of physical memory is not visible to the application layer, the OS layer or even the BIOS to protect select code. Intel SGX was designed to be used for implementing secure computation such as crypto computation, remote computation and other types of secure computation that no other apps or process on the system is allowed to access.

When used with enabled SW – SGX provides a silicon-hardened secure solution, ensuring the integrity of sensitive data even if the system is compromised by malware.

"Intel Software Guard Extensions (SGX) bring a fundamental change to security by providing hardware-level trusted execution of applications"

FileFlex Enterprise uses the secure enclaves of Intel SGX to generate encryption keys and guarantee their privacy. FileFlex uses an Intel SGX compliant client and connector agent to protect the encryption keys, both sender and receiver exchange data with a secure data encryption for transmission in the most secure way possible to protect the security of data in silicon from sender to receiver. This prevents man-in-the-middle attack, snooping and intercept even on a system that is compromised by malware because malware is unable to access the encryption keys that were used to secure the data.

It also protects against data tampering and the malicious corruption of data to eliminate virus re-transmission through infected files from sender to receiver.

Secure Processes of FileFlex Enterprise

The architecture of FileFlex functions using a set of secure processes to protect how it accesses, secures and transmits data. These include processes for user authentication, secure data transmission, accessing data, protecting credentials, use of anonymous tokens, request management and permission management.

User authentication - Sharing is done and consumed in the app using patented technology to authenticate users and does not permit open links that can be forwarded or shared on social media. Because users are authenticated, FileFlex Enterprise provides organizations control over shared files. Sharing can be revoked at any time on an individual contact or file-by-file basis. This protects against unauthorized downloading, unauthorized copying and unauthorized distribution. When a folder is used as a data room to allow external uploading, that uploading is done in-app so that users are authenticated and the spoofing of trusted sources is mitigated.

Secure data transmission The FileFlex connector agent accesses information, encrypts it and sends it back through a gated system. Double encryption ensures that the transmitted data is encrypted all the way through from sender to receiver. It is the ideal solution to address threats such as man-in-the-middle; snooping and intercept.

Information data - Neither users nor the FileFlex Enterprise server can access the storage infrastructure. The connector agent fulfills the request, encrypts it and sends it back to the server who then sends it back to the user. This process, which abstracts the data from the infrastructure, does not let anyone have direct access to the corporate infrastructure. Think of it like a bank teller. When you want money from your bank, you are not allowed into the vault to get it yourself – you must make the request to the teller, who then validates your credentials before fulfilling your request for you. When it comes to accessing your information, the connector agent acts like the bank teller. By using the FileFlex server and the connector agent as a proxy, FileFlex Enterprise protects against direct/unauthorized access to the information.

Protecting credentials – To protect user and device credentials, FileFlex Enterprise uses an exchange of anonymous secure tokens instead. Each request between the client and the server and the connector agent is made by a secure anonymous token exchange. FileFlex changes the encryption key every session and tokens are available only per session, then another token is generated for each session and each request. For each request, the process generates tokens to establish a secure connection between the FileFlex client and the server and the server checks permissions to see if the request is allowed. If the request is allowed, the FileFlex client then generates another token with the connector to establish a secure connection between the server and the connector agent. The connector agent fulfills the request, gets the data, encrypts it and sends the encrypted data back via the secure connections already established to the client via the server. Data is encrypted from the source to the destination. The use of tokens protects user and device credentials since they are not stored on the FileFlex Enterprise server, the service provider or with Qnext.

"FileFlex Enterprise itself has ... processes for user authentication, secure data transmission, accessing data, protecting credentials, use of anonymous tokens, request management and permission

Request management - When the secure data channel is established , it can only be established outbound from the connector agent and only to the FileFlex Enterprise server that the connector knows the address to. All inbound requests are refused and data can only be sent to one pre-determined address – that of the authenticated FileFlex Enterprise server. This process protects against server impersonation and spoofing.

"FileFlex Enterprise provides organizations control over shared files"

Active Directory and LDAP integration - Since typical EFSS solutions store your files on third-party servers, they introduce a level of complexity to access that storage by adding a layer of access authentication. This creates more work for sysadmins to manage permissions, modifications and termination. With this extra admin work, the critical time window surrounding user termination is extended and this brings with it significantly more risk.

FileFlex Enterprise on the other hand supports integration with Lightweight Directory Access Protocol (LDAP) and Active Directory (AD). When a user is deleted from AD, they instantly lose access to any storage through FileFlex Enterprise and all their file sharing is turned off. When you add a new user, they can automatically only access storage as allowed by your Active Directory. FileFlex Enterprise also allows the import of AD users on either an individual or group basis and then sync to those users/groups such that when a change is made in AD, it is immediately enforced within FileFlex. This reduces risk associated timing delays or human error caused by having to manage the deletion as two separate actions in two separate silos and the additional layers of administration common to EFSS is unnecessary.

Other user access protections – In order to protect against unauthorized access or stolen credentials, FileFlex also supports universal two-factor authentication (U2F), single sign-on (SSO), device authentication, enforced password policies and session timeout policies.

Restricted administrator access – Even administrators cannot use FileFlex to access any restricted information beyond what their own permission levels permit.

"Each request between the client and the server and the connector agent is made by a secure anonymous token exchange"

IT Dashboard and Management Toolkit

FileFlex Enterprise layers its security with a set of management tools for IT putting them in ultimate control over the security of information in the organization via the FileFlex Enterprise Server Management Console. The toolkit includes strong IT control over file access and sharing with the ability to monitor and enforce security controls and policies.

The control panel works together with existing tools such as Single Sign-On (SSO), multi-factor authentication like TFA, U2F, device fingerprinting, device locking, and login controls for users for strict or relaxed rules and by integrating with Active Directory and LDAP for file access, permission and rights management. It is used to specify and enforce encryption policies for access to and transfer from storage repositories which can be customized on a case-by-case basis. It can customize security levels for users on a user-by-user basis and/or departmental basis. It includes activity logging and includes tools to allow export or integration with 3rd party monitoring and incident management tools and it allows IT to integrate with and enforce their antivirus support for all documents uploaded to the corporate infrastructure by remote users during access and sharing.

"FileFlex Enterprise layers its security with a set of management tools for IT putting them in ultimate control over the security of information in the organization"

The admin panel can also be used to prohibit sharing of select files, folders or devices on an organizational basis, group basis or on a user by user basis. This is an ultimate IT control mechanism that allows remote access of PHI, PII and sensitive data, but ensures that it stays in its source location and copies are not shared with anyone.

This powerful layer gives IT an incredible number of controls that allow IT to adjust FileFlex Enterprise to meet the company's GRC (Governance, Risk Management and Compliance) requirements for security, governance, compliance. They are both powerful and flexible giving IT back control over how files are accessed and shared in your organization.

Additional Security Features of FileFlex Enterprise

Hybrid point-to-point communications – As part of the protection framework to secure communications against man-in-the-middle, snooping and intercept, FileFlex Enterprise uses an encrypted hybrid point-to-point communications structure. Using a secure token exchange, the FileFlex Enterprise server establishes an encrypted tunnel between files in their source locations behind your firewall and the user's device. FileFlex Enterprise limits the role of the server to be only used to facilitate the communication. None of your files or folders are stored on the server and you can even host the FileFlex server yourself, under your own GRC, on your own hardware and on your own property.

"Using a secure token exchange, the FileFlex server establishes an encrypted tunnel between files in their source locations behind your firewall and the user's device"

Secure, view-only option, downloading prohibited – Via the user administration panel, administrators can make selected files, folders or devices 'view-only' with downloading of shared content prohibited. FileFlex also allows users to set their sharing options so that downloading is not permitted. As a result, no unauthorized copies are made of files that are shared and the organization and users maintain control over the privacy of files shared. FileFlex Enterprise can be used for the sharing of Personal Health Information (PHI) and Personally Identifiable Information (PII) and aid compliance to privacy regulations such as HIPAA and GDPR because downloading of PII can be prohibited.

Device authentication – Device Management is a security mechanism designed to ensure that only authorized devices can use FileFlex Enterprise. Device management uses device fingerprinting to uniquely identify a corporate user's device. This device fingerprinting is used with the user's FileFlex login credentials to authenticate both the user and device as a type of two-factor authentication for better security. This is a preferred method of two-factor authentication as it is both secure and un-intrusive for the user. For example, if an adversary tricked a user to reveal their username and password through phishing, they would still be unable to access organizational storage as those credentials are only accepted when sent in conjunction with the device fingerprint from devices that have been authorized by the FileFlex administrator.

Device management can only be set up and administered by the FileFlex administrator. If device management is enabled, then users are prohibited from using the FileFlex Enterprise web client. They must use the FileFlex Enterprise native clients for Windows, Mac, Android or iOS.

"FileFlex Enterprise can be used for the sharing of Personal Health Information (PHI) and Personally Identifiable Information (PII) and aid compliance to privacy regulations such as HIPAA and GDPR because downloading of PII can be prohibited"

Support for Single Sign-On – Single sign-on (SSO) is an authentication process that allows a user to access multiple applications with one set of login credentials. SSO is a common procedure in enterprises, where a client accesses multiple resources. It streamlines workflow, minimizes phishing, improves compliance, provides detailed user access reporting and improves

productivity by eliminating credential reauthentication and help desk requests.

FileFlex Enterprise supports SSO and supports the SAML (Security Assertion Markup Language) open standard as well as the following custom versions from the following providers: OneLogIn; Google; Microsoft Azure; HelloID; MiniOrange; Okta and TraitWare. There is also a custom SSO configuration option to support other standard SAML providers.. To use SSO with FileFlex, it needs to be set up and enabled by the FileFlex administrator.

"only authorized devices can use FileFlex Enterprise"

Virus scanning - Supports active virus scanning using your AV software of choice to track down viruses, worms, trojans, spyware and malware that may be hidden in transferred documents.

The antivirus settings allow you to define which antivirus software on the host machine will be used to scan and files uploaded to it. Note: The antivirus software must already be installed and running with a valid license on the host machine.

Windows Defender is the default antivirus software for Windows based platforms. You can also select ClamAV and F-Secure SAFE from the 'Select an antivirus' dropdown. Other platforms can be used by selecting CUSTOM from the dropdown, then in command box enter the command line for your antivirus software.

Role/permission management - FileFlex is designed to allow administrators to manage access rights or roles on an individual or group/department basis. They can create their own custom access rights category or can use one of the three pre-defined roles already created.

"Supports active virus scanning using your AV software of choice"

"Administrators manage access rights or roles on an individual or group/ department basis"

Grouping users into departments – FileFlex Enterprise allows administrators to group users who have the same permission sets and content repositories. Permissions and content access can then be changed on a user-by-user basis as required. This makes it easier for administrators to secure PHI, PII and sensitive information for large groups of users.

Enable/disable network browsing - The Enable/Disable Network Browsing feature allows administrators to enable or disable network browsing. Network browsing is enabled by default. Network browsing enables users to browse all the devices on the same local network as the device being added that their credentials allow and that have sharing enabled within their operating system configuration.

Share expiry – FileFlex allows users to set a share expiry on a user-by-user and file-by-file basis. This makes maintenance of file shares and clean up much easier.

Password management and policy – To hep protect credentials, FileFlex Enterprise allows administrators to set the password strength (i.e. require complex alphabetical and numerical permutations), minimum password length and account lockout after failed logins. It also allows users to reset forgotten passwords without IT intervention. Additionally, FileFlex Enterprise monitors and logs all access login attempts and will notify both users and the administrator of a failed login lock-out. To protect login credentials, user passwords are hashed using a secure hash algorithm.

Session timeout policies – To protect against unauthorized access via an unattended computer, FileFlex Enterprise provides administrators to set shorter sessions. Once the users exceed the inactivity period, their session will expire and they will be required to login again. The Administrator can also control whether the user can select to stay signed in after turning off the App. The ability to force the user to manually sign in every time is a desired security feature

for many IT as it limits threats for unauthorized access.

Remote activation - Remote activation provides administrators greater flexibility on granting and managing access for remote users to authenticate and access remote content on the corporate infrastructure. IT will be able to make corporate content globally available to the remote corporate users and provide permission access through the users domain credentials. This provides IT a single point from which to managed access and ensure that all access is controlled via domain credentials.

Operations and incident management – If any file sharing solution is architected in a way that creates an additional and disparate silo, it creates a red flag for enterprise risk management programs. If that shared data cannot be analyzed in the context of your business it has failed many compliance requirements. To ensure risk is minimized, the FileFlex Enterprise activity log can be imported to the most popular risk management and SIEM systems using common import protocols.

All remote access and sharing is permission-based - All sharing is permission-based to confirmed contacts only. It's not a link that can be forwarded or shared on social media. Allowed sharing can be revoked at any time on a contact-by-contact or file-by-file basis. Sharing can be restricted to 'view only' and downloading of shared files can be prohibited on a file-by-file or contact-by-contact basis to prevent unauthorized access and unauthorized downloading.

Appendix – Third Party Audits

CISO Level Third-Party GDPR Compliance Evaluation

FileFlex Enterprise technology for secure remote file access, sharing and collaboration supports and augments an organization's GDPR compliance endeavors. FileFlex utilizes an organization's existing investment in technology and combines a rapid deployment capability and ability to support the enforcement of the compliance and auditability controls required by GDPR. This is achieved by using an organization's existing storage and keeping files in their source locations without copying or moving files to third-parties or secondary locations and without the use of cloud storage.

FileFlex Enterprise has been evaluated by an independent, third party CISO level information security firm who has reviewed the information security supporting capabilities introduced through the use of FileFlex Enterprise as it relates to compliance with the European General Data Protection Regulation (GDPR). The following is a summary of that evaluation. The GDPR compliance evaluation in full can be obtained by contacting a Qnext representative.

"FileFlex Enterprise technology for secure remote file access, sharing and collaboration supports and augments an organization's GDPR compliance endeavors"

Control of Data Transfers - The control of data transfer is a key requirement of GDPR. Unlike traditional cloud storage services, FileFlex Enterprise includes technology, which when used with policies and appropriate user behavior, controls data transfer as follows:

It does not require a mandatory data transfer of file copies to redundant servers which may or may not be located in geographies that are outside of GDPR jurisdiction enabling organizations to control and decrease the number of unstructured data copies they require.

Does not depend on the governance, risk management or compliance policies (GRC) of third-parties that may or may not be in compliance.

Provides the organization granular controls over who a user is permitted to share with.

Supplies view-only sharing where downloading is restricted.

Reduces Complexity - FileFlex Enterprise is a technological control that reduces complexity. The organization's existing infrastructure and existing information security investment and associated controls are utilized to share files while existing identity and access controls such as enterprise active-directory are used to enable authenticated and approved file access. These capabilities enable a rapid deployment model while relying on existing security controls and storage infrastructure to deliver collaboration and file share.

Data Minimization - GDPR mandates that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This principle should be delivered in the technology stack with the key aspect being the limitation on the amount of data that is in-scope. When files are duplicated on public, private or EFSS clouds, in addition to the source location, multiple images and data resides with the service provider typically on-line,

near-line, in redundant locations or off-line in backup managed and controlled by the service provider. Utilizing FileFlex technology enables organizations to limit the storage of personal data to what is necessary and achieve this goal by significantly reducing the footprint of organization data.

Accuracy - GDPR mandates that personal data shall be accurate, and where necessary, kept up to date. Keeping in-scope PII accurate and up to date is a challenge for organizations as the volume and copies of the data grows. FileFlex enables organizations to maintain far less copies of the same data enabling them to keep more accurate and up to date.

Storage Limitation - GDPR mandates that personal data be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This principle is further supported by FileFlex software via limiting the number of unstructured data copies that must be maintained, and through the use of auditing capabilities, enabling time limited sharing of files. This aspect in conjunction with view-only mode, supports the protection of PII and aids the prevention of data leakage requirements within GDPR.

Integrity and Confidentiality - GDPR mandates that personal data be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organizational measures. FileFlex supports integrity and confidentiality of data using technical controls such as Active Directory and LDAP integration, enforcement of file share permissions, allowing IT control over who users can share with and support of confidentiality controls by significantly enabling the organization to limit the number of data copies required for collaboration.

Accountability - GDPR mandates that the controller shall be responsible for, and be able to demonstrate compliance with the GDPR. The extensive logging integration within FileFlex supports this core principle while the integration with LDAP systems such as Active Directory enables controllers to attest to this principle using capabilities that they are already familiar with.

Control - GDPR requires the enterprise to control the processing of all personal information, yet the rise of shadow IT takes control away from the IT department and disperses it across the business functions. FileFlex minimizes the underlying need for Shadow IT existence in the first place, specifically around file sharing and access to unstructured data. Corporate users and external users can share and collaborate under organizational IT control and a secure framework, with little need to duplicate data or use of user-controlled services. This in turn, creates a smaller foot-print for attack vectors while enabling the collaboration features users require.

Supports Privacy by Design Mandates - GDPR requires the use of Privacy by Design techniques which means that enterprises must begin and utilize information security in a 'baked-in' approach vs 'bolted-on' approach that is prevalent in the industry. GDPR aims to transition information security from an after-thought to fundamental requirements.

Appendix - HIPAA Compliance

FileFlex Enterprise is the ideal file sharing and collaboration tool for HIPAA Covered Entities and HIPAA Business Associates. That is because the FileFlex server is hosted either by the HIPAA Covered Entity itself or by the HIPAA Business Associate that provides FileFlex to the HIPAA Covered Entity. No Protected Health Information (PHI) or Personally Identifiable Information (PII) is ever stored or transferred to Qnext or third-parties.

Security of data-in-motion - The data-at-rest is stored on the HIPAA entity or associate's already HIPAA compliant and secured storage infrastructure and data-in-motion is encrypted and transferred through servers hosted by the HIPAA covered entity or the HIPAA business associate.

Downloading can be prohibited - When used according to HIPAA compliance policies, files can be shared in view-only mode and downloading to local devices prohibited.

Compliant file collaboration with no local copies - File collaboration is from the HIPAA entity or associate's source location and no copies are stored on remote devices or third-party servers.

Restrict sharing and collaboration to HIPAA entity or associate contacts - Sharing and collaboration can be limited to HIPAA covered entity or business associate contacts.

"FileFlex Enterprise is the ideal file sharing and collaboration tool for HIPAA Covered Entities and HIPAA Business Associates"

