

FILEFLEX BY QNEXT

Cybersecurity Product Analysis Whitepaper

Author:

Edward Dubrovsky MBA MSc OSCP CISSP
Managing Director, CTO - Cyberithm

Contents

Executive Summary	2
FileFlex as a key technical security control in digital transformation	3
Abstract & Approach	4
About Cyberithm	4
Introduction	5
Managed File Transfers and Enterprise File Sharing and Sync	5
Cybersecurity challenges with MFT/EFSS system	5
Attack surface Analysis	5
Governance, Risk, Compliance	7
Authentication and Identity Management	7
Operations and Incident Management	7
Extended Whitepaper	8
Conclusion	10

A man in a dark suit and a red and white checkered tie is looking at a tablet. The background is a blurred office setting. The title 'Executive Summary' is overlaid on an orange banner.

Executive Summary

A small inset image of a woman with brown hair smiling.

Over the last two decades, large enterprises and small businesses alike have become increasingly engaged in digital transformation frequently deploying a mix of traditional on-premise and cloud solutions. Throughout this significant shift into a hybrid model organizations have cemented their reliance on digital information to meet business objectives.

Managing the associated risk with securing vast amounts of information while enabling collaboration and sharing of the same with the appropriate and authorized parties is a challenging endeavor. Information may exist in numerous places, including local storage, cloud, email and instant messaging platforms, to name a few.

While most enterprises employ numerous safeguards to control sensitive information, given the increase in cybersecurity incidents world-wide it is clear that these controls are inconsistent and management of security controls at different points in the enterprise is not effective.

FileFlex enables organizations to manage their information from a reduced surface perspective, information 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 phishing and ransomware.

Integration with existing LDAP and active directory provides centralized management of user accounts and associated privileges and enables seamless collaboration, while reducing the attack surface as compared to other solutions in the market.

This white paper provides an analysis of FileFlex from an information security perspective, including benefits, risks and business drivers to deploy FileFlex.



FileFlex as a key technical security control in digital transformation

Digital transformation has enabled the spread and shift of digital technologies from the traditional IT department and into the business units. While digital transformation has enabled the creation of new sales channels and customer engagement models enabling further efficiencies in supply chain and cost reduction, it has also introduced the need to increase the security around data as it moved and shared across these new channels.

In addition, with almost half the human population on the planet connected to the Internet the need to reach customers, suppliers and other stakeholders is a key factor to fuel organizational growth. With this growth, the need to provide access to information is an important function that requires careful consideration to ensure that information is shared in such a manner where the possibility for data-loss is minimized and where intellectual property, as well as other organizational information assets are only shared with appropriate stakeholders while enabling ease of collaboration and minimizing impact on constrained IT department and infrastructure resources.

Data may exist in three modes:

Data-at-Rest: is defined as data that is currently stored in existing file servers, storage devices such as SAN, NAS and similar locations across the enterprise.

Data-in-Motion: is defined as data that is traversing enterprise networks or data in movement.

Data-in-Use: is defined as data movement at the end-point where users may be copying data to a USB thumb drive, printing or even cut/paste between various applications, are just some examples.

FileFlex provides capabilities that allow organizations to better control Data-in-Motion and Data-in-Use scenarios, while allowing enterprises to retain their investments around existing infrastructure supporting their Data-at-Rest strategy.

ABSTRACT & APPROACH

This white-paper is aimed at analyzing a new software product that supports secure file transfer and collaboration by introducing a paradigm changing capabilities to secure information sharing without changing the existing infrastructure for organizations, while enabling existing technology, processes and standards to be retained and enforced. This 3rd party analysis aims to review the information security supporting capabilities introduced through the use of QNEXT's FileFlex solution, as well as the performance of a Threat Risk Assessment (TRA) on the product.

Cyberithm took the approach of reviewing the product from an adversarial perspective, and while a complete vulnerability assessment and penetration testing assessments were conducted against the product in a typical deployment architecture, the analyst has been provided with such information as typically would not be available to an external adversary.

The following components have been reviewed as part of the assessment:

- FileFlex capabilities along the spectrum of Detect, Prevent and Respond as related to Cyber-security
- Method of communications and name resolution
- Typical deployment architecture
- High-availability and susceptibility to DoS (Denial of Service)
- Identity and privilege management
- License activation processes
- Credential management and caching
- Communication ports
- Database security
- Certificate management processes
- Logging and Alerting capabilities and integration with SIEM technologies
- Review of phishing use-case risk reduction

ABOUT CYBERITHM

Cyberithm Inc. is a Canadian information security company with a three-decade experience in the Canadian and international technology markets. Our experience is in providing organizations information security services that encompass ethical hacking and security framework assessments such as NIST, ISO27002, NERC CIPv5 and PCI. Cyberithm consultants have been engaged to provide CISO level consulting in organizations of all sizes from SMB to Fortune 500 organizations and have been featured extensively on TV and print media.

INTRODUCTION

What is MFT (MANAGED FILE TRANSFER) & EFSS (ENTERPRISE FILE SYNC & SHARE)

Managed file transfer is a software package or service that enables the transfer of information from one system to another. EFSS is referred to as a software or service that enables enterprises to share documents and information with external or internal parties.

According to the Ponemon Institute's "2016 Cost of Data Breach Study: Global Analysis," which queried 383 organizations that suffered at least one breach in 2016, the average cost per breach was \$4 million. That figure rose to \$7 million in the U.S. Forty-eight percent of data security breaches are caused by acts of malicious intent. Human error or system failure account for the rest.

Given the costs associated with information breaches or leaks, it is clear that any solution which handles information movement for an enterprise must incorporate significant security capabilities to protect the information and ensure confidentiality is maintained and authentications of both sending and receiving parties and integrity of the information as it moves from one system to another.

CURRENT CYBER CHALLENGES

Given the increased demands of enterprise users, customers and other stakeholders, organizations must implement a solution to sharing information with various internal and external entities. While there is little argument that data classification remains one of the most difficult journeys an organization can embark on, the ability to share data in a controlled, coherent and secure manner remains a critical aspect of doing business. All this must be achieved without impacting access to information or business productivity.

Moreover, data classification and indeed the identification of where data resides requires significant and costly controls such as Data Loss Prevention (DLP) technologies that frequently fail to achieve ROI due to the fact that data and copies of data may reside on different locations within the enterprise and outside it, in such locations as cloud storage, mobile devices, non-corporate devices and even backup locations. Therefore, solutions that enable minimization of the data storage locations while introducing easily enforceable controls are capable of significantly reducing the attack surface while requiring low "care and feed" efforts.

At the same time, adversaries are increasing pressure on organizations worldwide to gain access to that same information with the intent to utilize such information for malicious use. In turn, organizations are beginning to realize that it is critical to assess their current information sharing posture and implement appropriate controls to protect their information and intellectual property.

While in the not so distant past organizations simply looked for the easiest avenue to share information, today, finding an FTP file sharing mechanism is an exception rather than the norm. Organizations quickly adopted solutions that incorporated encryption in file transfers using such protocols as FTPS/SFTP & TLS to encrypt file sharing technologies and just as quickly realized that most, if not all solutions created several challenges that solutions in the current market seem unable to address.

The attack surface

One of the key activities an organization can perform to reduce its overall risk to information security incidents is reduction of their attack surface. It goes without saying that if the available attack surface is minimized, the ability for an adversary to successfully breach through an organization's defenses becomes more difficult.

At the same time, the organization can manage a smaller environment better than a large and complex one. Overall, this translates to lower risk posture.

With the increase rise in popularity of cloud services and infrastructure, it appears somewhat simpler to migrate functions to the cloud thereby reducing the on-premise infrastructure components. However, if we review how such services operate, especially in the MFT or traditional EFSS solutions, we quickly realize that information must now exist in at least 2 logical locations (and frequently 3 to accommodate required data backups), typically where the information was created such as on premise infrastructure, as well as within the file sharing infrastructure.

In addition, given that a typical customer does not have access or understanding of where the information is stored in the cloud, it may very well be that a single piece of information may reside on premise and multiple images may also reside at the service provider, typically on-line, near-line, in redundant locations and perhaps even in off-line backup images managed and controlled by the service provider where the customer has little control.

This posture significantly increases the attack surface and also reduces control the organization may need over their information. Finally, with this type of an overall design, the ability to apply enterprise governance and risk management practices in the cloud is very challenging, if not impossible as discussed in the next section.

Governance, Risk and Compliance

Governance, risk management and compliance (GRC) issues around information have become focal topics to organizational information security strategies. GRC supports information security programs by housing information about enterprise security posture, management of relevant processes, policies and standards, manages and enumerates risks and applies regulatory intelligence to existing controls.

There is ever growing pressure on organizations to achieve more with less resources and to empower employees, business associates and customers using the latest technologies. Companies require increasingly larger market data sets and deeper granularity to feed predictive models, forecasts and other business activities throughout the day. Enterprise collaboration systems, social media, mobile devices and the cloud are great for innovation, free thinking and creativity. However, they can quickly become a compliance headache without the proper policies and enforcement systems in place. Specifically, on the compliance side, the ability to report and apply correlation to events are key as organizations must be able to respond and report on their security posture.

Therefore, any MFT or EFSS solutions must be able to integrate into enterprise GRC programs and support requirements. This means that supporting extensive logging and auditing capabilities, account management, integration into enterprise LDAP, auditability, support of strong encryption methodologies, non-repudiation and policies are just some of the key requirements of such solutions.

Authentication and Identity management

One of the largest markets within Cybersecurity is identify and privilege management. As many attack vectors focus on gaining or escalating privilege to admin, the need to monitor and manage privileges becomes critical. It is important to note that adversaries are focused on gaining access to privilege accounts with the main goal of gaining access to information that can be exfiltrated and sold for monetary gain.

Typical MFT or EFSS solutions introduce an additional level of complexity by frequently requiring the creation and management of an additional layer of authentication. While this is not necessarily bad, it does place additional responsibility for system administrators to manage such activities as identity creation, authentication complexity management, account modification and termination.

Based on experience in the field in performing hundreds of maturity and risk assessments on organizations of all sizes, there exists a critical time window between when a user is terminated and when all the user's access privileges are terminated. This window introduces significant risk organizations.

Operations and Incident Management

The increase in the number and severity of security incidents, in addition to the brand and reputational damage caused by information leaks, has forced organizations to assign greater strategic importance to security. It is no longer acceptable to implement technology solutions that are lacking in information security controls and capabilities. Solutions must also support the significant investment organizations have made in existing technology, processes and people.

Governments are increasingly moving to legislate, adopt and enforce regulations, while at the same time information security frameworks require organizations, whether governmental or commercial, to comply with strict requirements both in serving customers and also in case of a security breach. Because of these increased regulatory and compliance requirements when an incident occurs, the responding team is no longer solely composed of IT personnel, rather executives must be notified in addition to legal, marketing and government entities.

While security incidents are increasing in frequency, any solution that manages transfer and delivery of information must fully support incident management processes and support the ability for rapid investigation of information movement to truly integrate with existing information security programs.

Therefore, if any solution is architected in a manner that creates an additional and disparate silo, it does not lend itself to be fully integrated into enterprise risk management programs, and as such cannot be analyzed in the context of the business and will likely fail compliance requirements, but worst, may not be truly effective in that context.

EXTENDED WITEPAPER

The extended version of this whitepaper explores and analyses the following subjects in order to draw its final conclusion.

- **FILEFLEX PRODUCT ASSESSMENT**
 - Complete technical assessment of the FileFlex product and its ability to mitigate risks by providing a unique solution in the MFT/EFSS market space. Evaluates risk areas and maps them to potential impact and assesses FileFlex's mitigation approach.
 - Detailed architectural analysis of the FileFlex system as it relates to security.
- **RISKS AND THREAT ANALYSIS**
 - Threat Risk Assessment (TRA) was conducted against a typical FileFlex environment.
 - Detailed testing methodology and findings are provided and available in the extended whitepaper.
- **TECHNICAL SECURITY ANALYSIS**
 - Numerous industry assessments tests performed on the FileFlex infrastructure.
 - Assessments included an ISO27001/2 maturity assessment, vulnerability assessment and penetration testing.
 - Detailed testing methodology, including a list of industry standard analysis software tools used for testing.
 - Detailed reports and assessment results to support conclusion.

CONCLUSION

FileFlex is an advanced file sharing solution that provides secure file sharing with internal and external stakeholders using minimal additional infrastructure requirements. Communication between the various components are encrypted using advanced encryption technologies that are deemed unbreakable at the time of the assessment. The solution integrates well into an enterprise environment and can be deployed on-premise or in a cloud environment that is either managed by the enterprise or through a 3rd party managed service provider. The solution offers confidentiality, integrity and availability capabilities (CIA) with minimal impact on existing processes and infrastructure.

At the time of the assessment, the FileFlex solution offered no exploitable attack surface using publicly available exploits and attack techniques.

Given the overall FileFlex solution offers little additional infrastructure to control file sharing processes, while creating zero additional foot-print for file storage, the solution provides a compelling technology control to improve security posture for any organization.