MARKETSANDMARKETS™

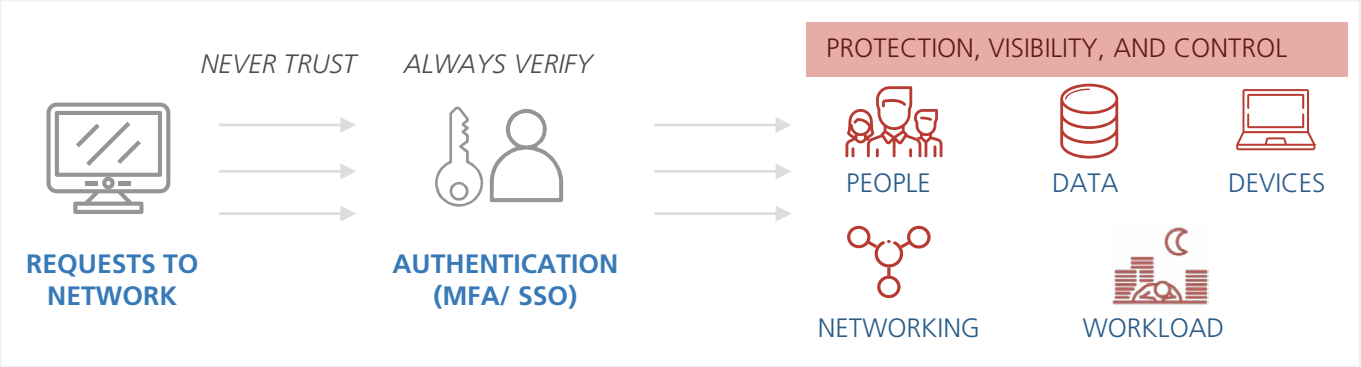
ZERO TRUST SECURITY MARKET

AND REVIEW OF ZERO TRUST DATA ACCESS

Sponsored By
qnext

INTRODUCTION

The Zero Trust Network, or Zero Trust Architecture model is based on the principle of **"NEVER TRUST, ALWAYS VERIFY";** which means that no users or devices both inside and outside an organization network should be automatically trusted.



Thus, based on the architectural framework, every individual, machine, or application within or outside of the enterprise perimeter must be constantly authorized and authenticated before they are granted access to the organization's infrastructure.

Over the last few years, there have been increasing incidents of privacy breaches and information thefts, with a whopping 140%+ jump in compromised volume of records during 2020 as compared with the previous year. However, it must be noted that several factors can affect the reported numbers; including organizations that choose not to disclose data breaches publicly while some even wait to report the incident.

Nonetheless, growing digital transformation has opened new avenues of data monetization; with data becoming the core pillar for strategic business excellence. However, with increasing digital footprint, the subsequent breaches and misuse of data have necessitated the need for stringent regulatory guidelines to face the increased risk of data privacy and security.

Moreover, due to the global pandemic, remote working is increasingly being accepted as the new normal across businesses globally and thus further bolstering the use of cloud deployments and storage platforms. Consequently, it is an ideal scenario to infer that in the given context and scenario a Zero Trust architecture presents a necessary architectural model for all organizations with the slightest iota of digital footprint.

In recent years, inspiring developments in the Zero Trust technology has transpired, including the unveiling of the industry's first **Zero Trust Data Access (ZTDA) platform** – "Qnext's FileFlex Enterprise"; that facilitates remote access and data sharing across hybrid IT infrastructure (on-premises, cloud-hosted, and SharePoint storage). Interestingly, FileFlex Enterprise also adheres to HIPAA and GDPR compliance which further augments its business use case.

Overall, the Zero Trust security model is poised to grow substantially over the coming years, with some prominent companies competing in the Zero Trust marketplace including networking vendors such as Cisco, Akamai Technologies, and Palo Alto Networks as well as Okta, Check Point, Qnext Corporation, Trend Micro, IBM, Google, Microsoft, VMWare, and Varonis Systems, among many others. This paper covers key aspects of the segment of the Zero Trust model, its ecosystem, evolution, technologies/solutions used, and the role of Qnext Corp. in innovating the segment of Zero Trust Data Access.

THE EVOLUTION OF ZERO TRUST

Traditionally, most organizations have been highly reliant on firewalls and perimeter-based network security to guard their infrastructure from external threats. This setup can create a resilient external network, considering people, workflows and policy changes are not considered into perspective. Perpetually, most common security lapses have been due to the neglect of security measures for internal networks and associated entities. Thus, instead of entrusting that all the data within the corporate firewall is safe, the Zero Trust model has evolved as a robust security framework that verifies each access request as though it originates from an uncontrolled network.

Officially coined in 2010, the evolution of the Zero Trust security framework has coincided with the high adoption of mobile and IoT devices, and the corresponding explosive rise in associated applications and services that are connected to enterprise networks. The idea of a Zero Trust security landscape was originally sparked by a highly sophisticated APT attack which began in 2009, known as Operation Aurora, that gained access to the private networks of a dozen large enterprises.

The evolution of Zero Trust was established from the need to think beyond the firewall and ensure secure access to all applications, for any user and device. In 2014, Google moved away from its VPN and privileged network access model to BeyondCorp, its own version of a Zero Trust security framework. BeyondCorp suggests three key ideas: connecting from a specific network should not determine the services a user can access; access should be granted based on user and device information; and all access requests must be authenticated, authorized, and encrypted.

The increased shift to cloud environments and an ever-increasing remote workforce has established the Zero Trust security model as a new way of looking at security architecture and consequently managing access control policies for all organizations going forward.

PRINCIPLES OF ZERO TRUST

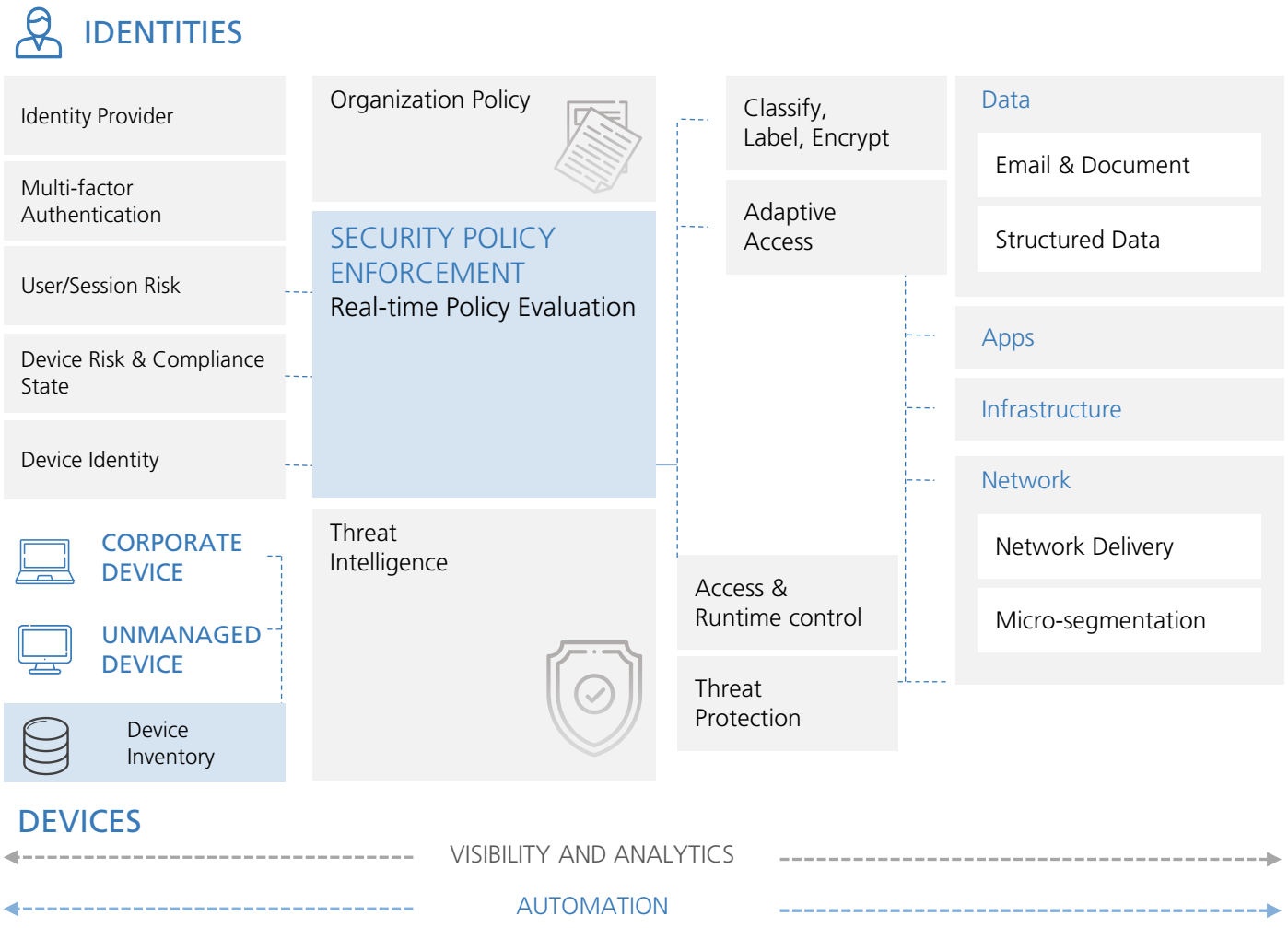
- Zero Trust networks use micro-segmentation to enhance security and fasten incident response and remediation. Micro-segmentation is the practice of breaking up security perimeters into smaller separate and secure zones in the network. A person or device that has access to one of these zones will not be able to access any of the other zones without separate authorization.
- Zero trust security is based on the Principle of Least-Privilege (POLP) and Just-In-Time (JIT) access, which means, granting users only as much access as needed.
- Zero Trust ensures strict controls on user/ device access with SSO and MFA/ 2FA. It also ensures how many devices are accessing the network and that every device is authorized. Any user that accesses files, applications, or cloud storage devices must be authenticated, authorized, and verified for secure access.
- Zero Trust verifies each access request with rich intelligence and analytics capabilities to detect and respond to anomalies in real-time.
- Implementing a Zero Trust model requires monitoring and logging all activities related to data access to provide a strong parameter to defend against future instances of data breaches and security threats.

ZERO TRUST **SECURITY MARKET ECOSYSTEM**

In a Zero Trust model, every access request is strongly authenticated, authorized in policy constraints, and inspected for anomalies before granting access. In addition, regardless of the request that originates or the resources it accesses, Zero Trust teaches us to "never trust, always verify."

A Zero Trust security model relies on automated enforcement of security policy to ensure compliant access decisions throughout the digital estate. Zero Trust controls and technologies are implemented across six foundational elements, such as identities, devices, applications, data, infrastructure, and networks. In the figure below, the security policy enforcement engine provides protection by analyzing signals based on threat intelligence in real-time. The engine at the core ensures that identities and devices are verified and authenticated before they are granted access to data, applications, network, and infrastructure. Additionally, automation along with visibility and analytics is applied continuously throughout the ecosystem.

ZERO TRUST SECURITY MARKET ECOSYSTEM



Source: Microsoft Zero Trust Vision Model and MarketsandMarkets Analysis

The major components of the Zero Trust model work together to deliver end-to-end coverage. They are as follows:

KEY COMPONENTS OF THE ZERO TRUST MODEL

KEY COMPONENTS	DETAILS
Identities	Identities secure and authenticate all users across the digital infrastructure.
Devices	Once an identity has been granted access to a resource, the data can flow to a variety of different devices—IoT devices, smartphones, BYOD, managed devices, on-premises workloads or cloud-hosted servers. This diversity creates a massive attack surface area, which requires constant monitoring. The compliance status of all devices is checked before granting access to the IT infrastructure.
Apps	Applications and APIs may be present on legacy on-premises, cloud workloads, or modern SaaS applications. These monitor user permissions based on real-time analytics.
Data	The security teams are highly focused on protecting data. Data must remain safe even if it leaves the devices, apps, infrastructure, and networks. Data is accordingly classified, labeled, encrypted, and restricted based on organizational policies.
Network	All the users and devices over the internal network infrastructure must not be trusted. The internal communications must be encrypted and authenticated. Further, microsegmentation and least privilege access must be applied to minimize lateral movement of malicious actors across the network.
Infrastructure	Infrastructure (whether on-premises servers, cloud-based VMs, or containers) represents a critical threat vector. In infrastructure, JIT access hardens defense; it uses telemetry to detect attacks and anomalies, and automatically blocks and flags risky behavior.

Source: Secondary Research, Industry Experts, and MarketsandMarkets Analysis

KEY TECHNOLOGIES/FUNCTIONS THAT BUILD A ZERO TRUST ARCHITECTURE

No single specific technology is associated with a zero trust architecture; it follows a holistic approach that incorporates several different principles and technologies

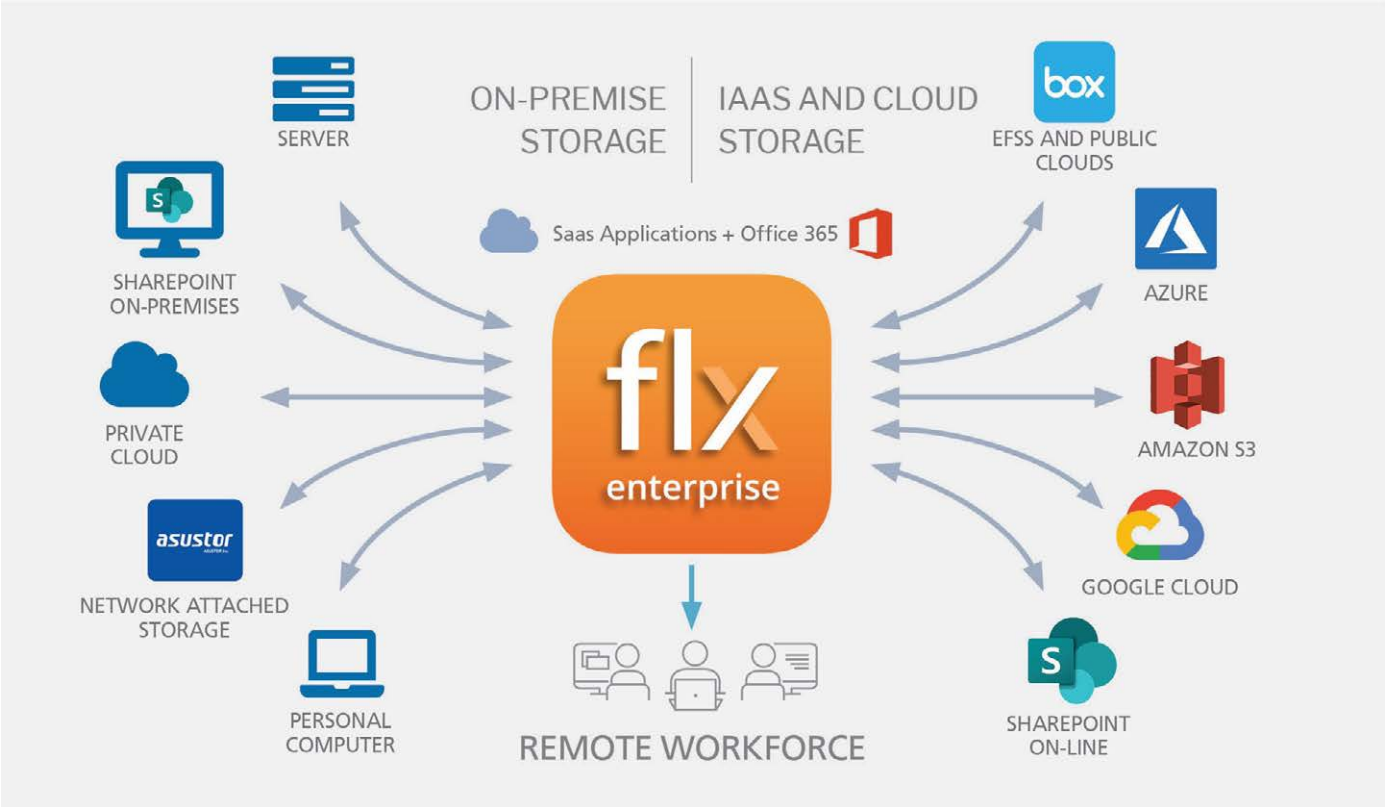
KEY TECHNOLOGIES	DETAILS
Network Security	Zero Trust network security solutions ensure that any person/ device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter must be strictly verified before granting access. The Zero Trust framework directs that only authenticated and authorized users and devices can access applications and data.
Data Security	Zero trust data security solutions strengthen the data security of organizations by restricting the lateral movement of threats and data breaches within the infrastructure of companies.
Application Security	The entire stack of applications and back-end software that enable clients to interface with businesses is a common attack vector that must be defended. Zero Trust offers a comprehensive solution to securely access applications from any user, device, or location. With the Zero Trust model, better visibility is achieved across all applications as all resources are continuously verified before access is permitted.
Identity and Access Management (IAM)	Zero Trust in an IAM strategy enables frictionless access that gives users access to a network from anywhere while maintaining tight security. Organizations are gradually implementing Zero Trust by enforcing strong authentication using MFA and SSO approaches to strengthen security and provide smooth access to end-users.
Endpoint Security	Extending Zero Trust to endpoint security solutions secures enterprise networks when accessed through various endpoint devices, such as smartphones, tablets, desktops, laptops, and other remote wireless devices. Endpoint security monitors traffic on connected devices to identify intrusions and threats from viruses, trojans, malware, and advanced threats, such as zero-day malware and APTs.
Security Orchestration Automation and Response (SOAR)	Automation helps keep all Zero Trust security systems to be monitored continuously for subsequent threat detection and remediation. SOAR solutions enable organizations to gather data from various sources and respond to security incidents from a single system. Moreover, they can control and manage security alerts, and prevent unauthorized access and data breaches on critical applications with the use of automated systems and data-driven analysis.
Security Information and Event Management (SIEM)	Zero Trust security relies on SIEM to continuously monitor the Zero Trust ecosystem to detect, investigate, and prioritize threats. SIEM constantly analyses networks and system activities to prevent malicious attacks post authentication.

User and Entity Behavior Analytics (UEBA)	UEBA, an employee monitoring and data analytics tool powered by ML, detects anomalous device behavior, which is followed by quick response and remediation.
Application Programming Interface (API)	In a Zero Trust security environment, an API security solution is used to detect all forms of API attacks on the internal or external APIs. These solutions are capable of monitoring API traffic and automatically discovering anomalous API behavior in the API environment of organizations.
Security policy Management	Zero Trust security policy management solutions provide IT and security teams the ability to control and manage security policies across hybrid IT environments. The policy engine is the core of zero trust architecture. It decides whether to grant access to any resource within the network.
Policy Server	The Policy Server enables the Zero Trust framework to authorize services and facilitates tracking and control of files at a micro perimeter level, thereby, ensuring the benefits of Zero Trust security.
Compliance	One of the goals of Zero Trust security is to help the company achieve compliance with HIPAA, PCI, GDPR, FISMA, CCPA, and any future data privacy and security laws.
Intelligent Analytics	Intelligent security analytics provides comprehensive insights to quickly detect and prioritize threats across on-premises and cloud-based environments in real-time.

HOW IS FILEFLEX INNOVATING ZERO TRUST?

FileFlex Enterprise, developed by Qnext Corp., is a Zero Trust overlay service that unifies remote access, sharing and governance of data storage across multiple environments - on-premises, cloud-hosted and SharePoint storage. The FileFlex Enterprise Zero Trust Data Access (ZTDA) solution eliminates the need to use Virtual Private Network (VPN); it authenticates and authorizes every transaction for remote access and data sharing on the network infrastructure. It uses innovative file and folder level micro-segmentation to reduces lateral movement within the corporate network by threat actors and malicious insiders.

FileFlex Enterprise can optionally add an additional layer of security with computing devices that have an Intel processor with Intel Software Guard Extensions software (Intel SGX), a layer of silicon-hardened communications is achieved for added protections against shared data being snooped or tampered with at any stage of access or transmission.



Source: Secondary Research and MarketsandMarkets Analysis

Major features that showcase the Zero Trust Data Access technology are listed below:

No VPN: FileFlex Enterprise provides access to data without giving access to the infrastructure. With FileFlex Enterprise, one can securely access and share data on the hybrid IT infrastructure, such as, in cloud-hosted, on-premises, SharePoint, corporate data centers, and remote offices without a VPN.

VM: FileFlex Enterprise is a software-only solution that runs on a VM. It does not require the additional purchase of hardware or storage.

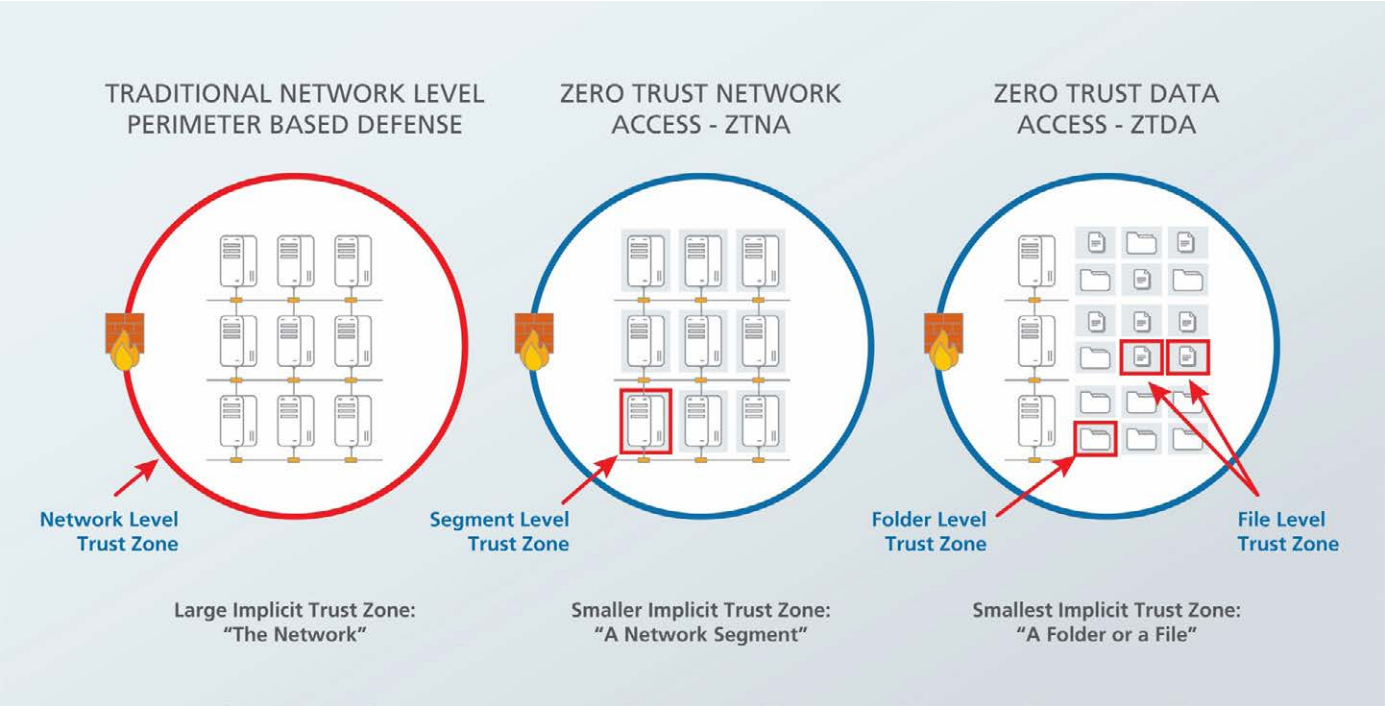
Integrations: FileFlex Enterprise integrates into existing security tools like SSO (Okta, HelloID, OneLogin, TraitWare, MiniOrange), Anti-Virus (Kaspersky, ESET, F-Secure, McAfee, Norton), and MFA. It also integrates with Active Directory and Lightweight Directory Access Protocol (LDAP) for file access share permissions and user rights management.

FILEFLEX ENTERPRISE INTEGRATIONS

LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)	ACTIVE DIRECTORY (AD)
MULTI-FACTOR AUTHENTICATION (MFA)	ANTI-VIRUS
SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)	SINGLE SIGN ON (SSO)
UNIVERSAL 2nd FACTOR DEVICE U2F and YUBI	AZURE ACTIVE DIRECTORY (AD)

Source: Secondary Research and MarketsandMarkets Analysis

File/Folder Micro-segmentation: The FileFlex Enterprise solution from Qnext employs a unique file/folder level micro-segmentation approach to data access that greatly reduces the impact of a hacker's lateral movement within an organization's infrastructure.



End-to-end encrypted: The data, when accessed remotely, is end-to-end encrypted. Optional double encryption (an encrypted SSL micro tunnel and an encrypted data stream) provides end-to-end encryption from source to destination to protect against man-in-the-middle, snooping, and intercept. Also, data is never duplicated, at rest or stored inside servers and all users are verified, it remains in the source location with all end-users being verified.

Security features: Its key security features are MFA, device authentication, and AES 256 hybrid P2P double encryption, real-time activity logging and audit to file and folder level, and integrations into SIEM software. By using detailed auditing and integration with enterprise SIEM technology, FileFlex provides a faster response to security incidents.

IT admin control: The IT admin has complete control over file access permissions down to file level granularity. The admin has the right to restrict to 'access only' and 'view only'.

Compliance with regulatory requirements: FileFlex Enterprise includes powerful administrative controls to ensure that files remain where they should, i.e. within their geographic location and are only shared with the people, and in the regions, where it is legally appropriate. FileFlex is an ideal collaboration tool for meeting the compliance requirements with regulations, such as HIPAA or GDPR.

Global partnerships: Intel, Microsoft, and Hewlett Packard Enterprise.

Flat fixed pricing: FileFlex is a software-only service-based technology. Hence, no employee needs a public cloud account to access files remotely. As a result, organizations can utilize all the existing infrastructure (storage resources, servers, etc.) in the corporate network without any additional investment.

	ENTERPRISE	ENTERPRISE PLUS	ENTERPRISE CUSTOM
Monthly Pricing	USD 10.95/ per user	USD 9.95/ per user	Not revealed
Number of Users	Up to 100	101 to 1000	Over 1000 users

ABOUTMARKETSANDMARKETS

MarketsandMarkets™ provides quantified B2B research on more than 30,000 high growth niche opportunities/threats with a potential to impact 70% to 80% of worldwide company revenues. It has 7,500 customers worldwide including 80% of global Fortune 1000 companies as clients. Almost 90,000 top officers across Ten industries worldwide approach MarketsandMarkets™ for their pain points around revenue decisions.

Our 850 full-time analysts and SMEs at MarketsandMarkets™ are tracking global high growth markets following the "Growth Engagement Model – GEM". The GEM aims at proactive collaboration with the clients to identify new opportunities, identify most important customers, write "Attack, avoid and defend" strategies, identify sources of incremental revenues for both the company and its competitors.

MarketsandMarkets™ is determined to benefit more than 10,000 companies for their revenue planning and help them take their innovations/disruptions early to the market by providing them research ahead of the curve.

MarketsandMarkets's flagship competitive intelligence and market research platform, "Knowledgestore" connects over 200,000 markets and entire value chains for a deeper understanding of the unmet insights along with market sizing and forecasts of niche markets.

For more information, please visit: **www.marketsandmarkets.com**