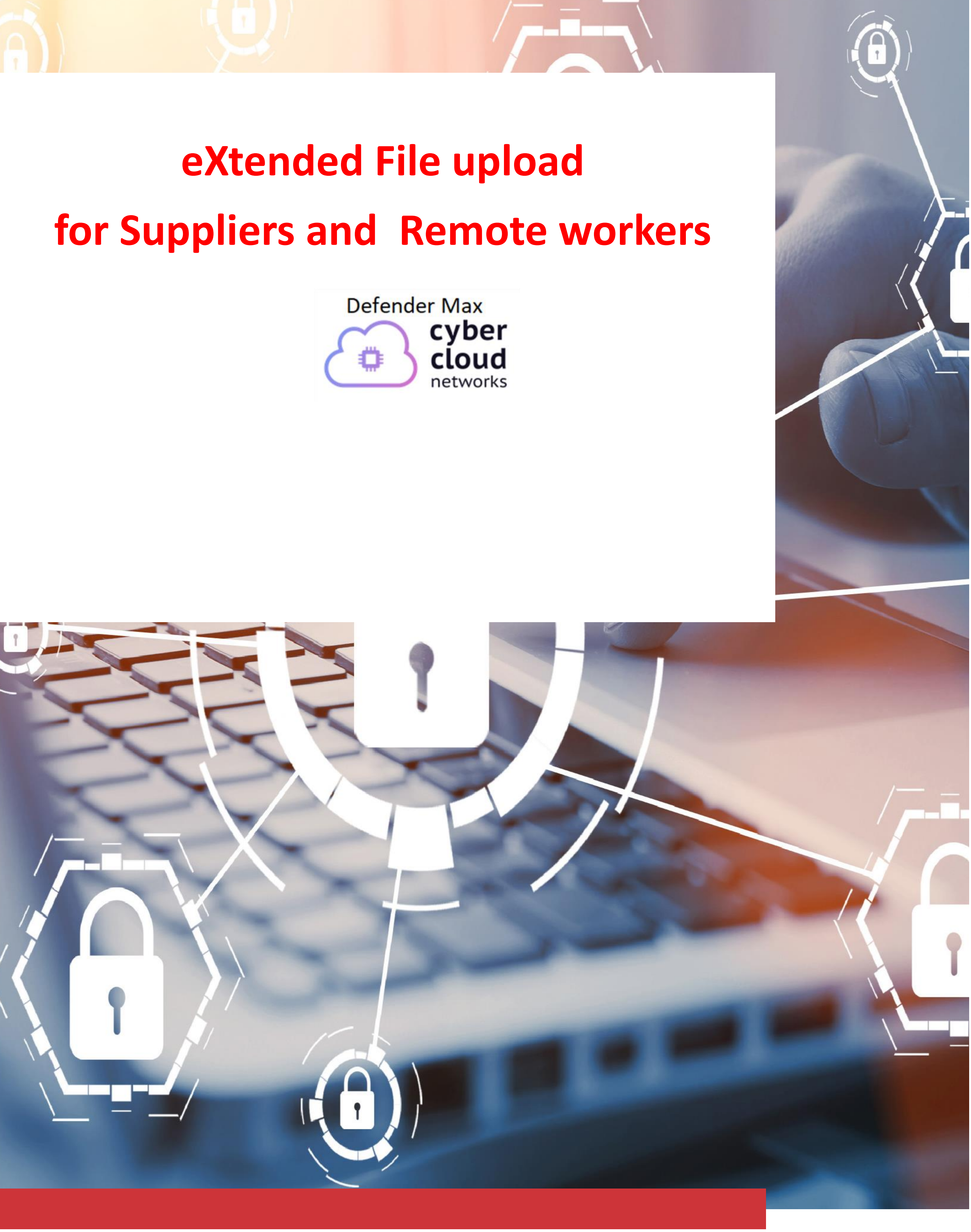
eXtended File upload

for Suppliers and Remote workers

Defender Max
cyber
cloud
networks



Secure File Exchange

Easily transfer any file securely to anyone

In an era dominated by digital collaboration, the need for a robust and secure file upload platform has become paramount. Defender Max Safe emerges as a next-generation solution, seamlessly combining manual and automatic methods of secured file transfer. Whether as a Software as a Service (SaaS) or an on-premise platform, Defender Max Safe ensures secure file transfers with unique integration capabilities, drawing from Cyber Cloud Networks Defender framework.

Introduction

In the fast-paced landscape of digital collaboration, the significance of secure file uploads cannot be overstated. Defender Max Safe emerges as a cutting-edge solution, seamlessly blending manual and automatic methods for secured file transfer. Whether deployed as a flexible Software as a Service (SaaS) or as a robust on-premise platform, Defender Max Safe stands at the forefront, integrating seamlessly with corporate security engines through Cyber Cloud Networks Defender framework. This white paper delves into the pivotal role played by Defender Max Safe in addressing the imperative need for secure file uploads. It explores the multifaceted features, diverse deployment modes, and the embedded Defender Max framework technologies that collectively position Defender Max Safe as a next-generation, comprehensive solution for organizations dealing with eXtended file uploads. From protecting against unauthorized access to ensuring compliance with industry regulations and preventing data loss, Defender Max Safe is engineered to deliver a secure, efficient, and customizable file upload experience in an ever-evolving digital environment.

Importance of an eXtended File Upload Platform

In the dynamic landscape of digital information exchange, the need for a secure and efficient eXtended File Upload platform is paramount. The significance of such a platform is underscored by several critical factors, including:

1. Protection Against Unauthorized Access:

Secure file upload serves as a robust safeguard against unauthorized access. By enforcing stringent access controls, it ensures that only individuals with the proper authorization can access and interact with the uploaded files. This fundamental security measure prevents data breaches and maintains the confidentiality of sensitive information.

2. Prevention of Data Loss:

One of the primary concerns in file management is the potential loss or corruption of crucial data. A secure file upload platform mitigates these risks by implementing reliable mechanisms to safeguard against data loss. Through secure transfer protocols and storage practices, organizations can ensure the integrity and availability of their important files.

3. Compliance with Regulations:

Organizations operate in a regulatory landscape that mandates adherence to various laws and industry-specific regulations. Secure file upload platforms play a pivotal role in helping organizations achieve compliance with these regulations. This includes data protection laws and industry standards, ensuring that the organization conducts its file transfer operations within the bounds of legal and regulatory frameworks.

4. Protection Against Malware:

The threat of malware poses a constant challenge to data security. Secure file upload platforms act as a frontline defense against malware-infected files. By incorporating robust scanning and filtering mechanisms, these platforms detect and prevent the upload of malicious files, thereby safeguarding the overall security of the organizational environment.

Platform Specifications of Defender Max Safe: A Comprehensive eXtended File Upload Solution

Multiple Safes per Corporate:

Defender Max Safe supports the creation of multiple Safes, facilitating organized file upload environments for distinct corporate entities such as suppliers, IT, Marketing, Engineering, and Finance.

Support for Local Storage and Cloud Storage:

Defender Max Safe ensures a seamless and integrated experience by natively supporting a spectrum of storage options, both locally and in the cloud. This robust integration extends to well-established cloud storage providers, including Google Storage, AWS S3 Buckets, and Azure Blob, allowing organizations to leverage the scalability and reliability of these cloud ecosystems. Moreover, Defender Max Safe seamlessly integrates with Microsoft SharePoint, empowering users to synchronize and share files effortlessly within their corporate environment. Defender Max Safe readily connects with FTP and SFTP servers, ensuring versatility in catering to various storage preferences.

Web Portal Support:

The platform offers a user-friendly web portal, providing a seamless interface for users to interact with and manage their respective Safes.

White Label of Safe Portal:

Organizations have the flexibility to white-label their Safe portals, allowing for a customized and branded user experience.

SFTP Support - Automatic Transfers:

Secure File Transfer Protocol (SFTP) support enables automatic and secure file transfers, ensuring the efficient exchange of files within the platform.

SFTP Support with Unique OTP Mechanism:

Enhanced security is achieved through the integration of a unique One-Time Password (OTP) mechanism for SFTP support, adding an extra layer of authentication.

Remote Agent – Folder Monitoring:

A Remote Agent feature enables monitoring of folders in remote networks, branches, and sites, enhancing the platform's reach and usability.

Fast Lane for Streaming File Upload:

Corporate users have the capability to establish a "Fast Lane" for streaming file uploads, ensuring swift and efficient data transfer.

Isolation Mode – No Direct File Upload to Internal Corporate Network:

An isolation mode prevents direct file uploads to the internal corporate network, adding an additional layer of security.

Approval Mode – Safe Administration Approval for Uploaded Files:

File uploads can be subjected to an approval process by Safe administration, ensuring that only authorized content is accepted.

API File Transfer Support (Sync, Async):

The platform supports API-based file transfers, providing both synchronous (Sync) and asynchronous (Async) transfer options.

User Support - Guest, Local, LDAP Users, SSO:

Defender Max Safe accommodates various user types, including guests, local users, LDAP users, and offers Single Sign-On (SSO) capabilities.

OTP Email Support for SFTP and Web Portal:

One-Time Password (OTP) authentication is extended to email support, enhancing the security of SFTP and web portal access.

File Sharing with Remote Users (Including Large Files):

Users can securely share content, including large files, from the corporate environment to remote users through the platform.

Scan Uploaded/Shared Files with Multiple Security Engines:

Files uploaded or shared undergo thorough scanning using multiple security engines, ensuring comprehensive threat detection.

File Type Identification Support:

The platform supports the identification of file types, aiding in categorizing and managing diverse file formats.

Utilizing Multiple Security Engine Categories:

Integration with various security engine categories, including Sanitization, Sandbox, ML/AI, AV, DLP, and Container, aligns with existing corporate security measures.

Chaining Multiple Security Engines for Specific Flows:

Security engines can be chained together for specific file flows, allowing organizations to customize security protocols.

Customized Scanner Addition for Unique File Types:

Organizations can add customized scanners for unique file types, embedding them seamlessly within the orchestration flow.

On-Demand Security Engines Enablement via Cyber Cloud Networks Defender Framework:

Security engines can be enabled on-demand through the Cyber Cloud Networks Defender Framework, providing flexibility and scalability.

Load Balancing for Multiple Security Engines:

Load balancing capabilities optimize performance by distributing the workload across multiple security engines.

Multiple Actions: Monitor, Scan, Alert, Block, and Replace Content:

The platform supports diverse actions, including monitoring, scanning, alerting, blocking, and content replacement, providing a spectrum of response options.

Build Multiple File Forwarding Flows:

Organizations can construct multiple file forwarding flows, such as Cloud storage to SFTP, Microsoft Sharepoint, CIFS to SFTP, Web Portal to Cloud Storage, etc., tailoring file transfers to specific needs.

Single Sign-On Support for Integration with BigIP F5, Pulse, Azure:

Integration with major Single Sign-On providers like BigIP F5, Pulse, and Azure enhances accessibility and user convenience.

Custom Web Forms for Files:

The platform allows the creation of custom web forms for files, facilitating the secure insertion of corporate files through designated forms.

Integration with MFT and Collaboration Solutions:

Seamless integration capabilities extend to Managed File Transfer (MFT) and collaboration solutions, streamlining workflows and enhancing interoperability.

Integration with Data Diodes for Secure Isolated File Transfer:

Integration with Data Diodes ensures secure and isolated file transfer, adding an extra layer of protection for sensitive data.

AI-Based Insights for Content Inspection:

Leveraging Artificial Intelligence (AI), the platform provides insightful content inspection (Q124), enhancing the depth of threat analysis and identification.

Deployment Modes of Defender Max Safe: Tailoring Security Solutions to Your Needs

SaaS Consumption-Based Model: The SaaS (Software as a Service) Consumption-Based Model offered by Defender Max Safe introduces a flexible and scalable approach to secure file upload. Organizations opting for this model pay based on their usage of both files and Defender engines. This on-demand consumption model ensures cost-effectiveness, allowing businesses to align expenses with their actual usage patterns. Users benefit from the convenience of accessing the platform through a cloud-based service, eliminating the need for extensive infrastructure investments.

Hybrid Model: SaaS Consumption with Integration to Corporate Infrastructure: The Hybrid deployment Model seamlessly blends the advantages of the SaaS Consumption-Based Model with the integration capabilities of corporate infrastructure. In this configuration, Defender Max Safe operates as a cloud-based service, offering the benefits of scalability, accessibility, and easy management associated with SaaS. Simultaneously, the platform integrates with the organization's existing corporate infrastructure, fostering a cohesive and interoperable environment. This integration ensures a harmonious coexistence between cloud-based security solutions and on-premise systems, accommodating diverse organizational needs.

On-Premise Model: Full Isolated On-Premise Solution (Sizing Based on Resources): For organizations seeking the highest level of control, security, and customization, the On-Premise Deployment Model of Defender Max Safe provides a full isolated solution. This model involves hosting the entire platform on the organization's premises, granting them complete authority over the infrastructure and resources. Sizing considerations are based on the specific needs and capacities of the organization, ensuring optimal performance. The On-Premise Model is ideal for businesses with stringent security and compliance requirements, enabling them to maintain a secure file upload environment within their physical infrastructure.

Key Considerations for Deployment

Scalability: All deployment modes of Defender Max Safe are designed to scale seamlessly, adapting to the evolving needs of organizations.

Interoperability: Regardless of the chosen deployment mode, the platform ensures interoperability with existing corporate systems, promoting a cohesive and integrated security ecosystem.

Customization: Each deployment mode allows for customization to align with the organization's unique requirements, ensuring that Defender Max Safe caters to specific business objectives.

Security Control: The On-Premise Model provides organizations with enhanced control over their security measures, while the SaaS and Hybrid models offer the convenience of cloud-based security solutions.

Cost-Efficiency: The SaaS Consumption-Based Model is tailored for cost efficiency, enabling organizations to pay for usage as they leverage the platform's file upload and Defender engine capabilities.

Embedded Defender Max Framework Technologies: Advanced Guardians of Data Security

In the ever-evolving landscape of cybersecurity, the Embedded Defender Max Framework Technologies stand as advanced guardians of data security, reinforcing the core principles of confidentiality, integrity, and availability. This formidable trio—ML File Scanning, Multi-Scanning Anti-virus, and File Sanitization—represents a cutting-edge approach to securing eXtended file uploads within the Defender Max Safe platform.

As data becomes the lifeblood of digital ecosystems, the imperative to fortify defenses against evolving threats is paramount. The Embedded Defender Max Framework Technologies epitomize a proactive and dynamic defense strategy, harnessing the power of machine learning, multi-layered antivirus defenses, and intelligent file sanitization. This amalgamation of technologies not only detects and neutralizes existing threats but also adapts to emerging risks, ensuring a resilient and anticipatory shield for organizations navigating the complexities of secure file transfer.

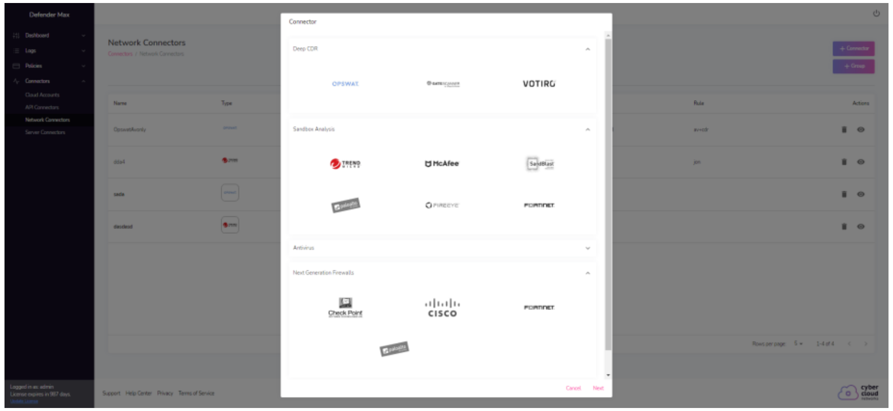
In this era of heightened cyber threats, the Defender Max Framework stands as an embodiment of innovation and vigilance, offering organizations a robust defense against unauthorized access, data loss, compliance breaches, and malware intrusions. As we delve into the intricacies of ML File Scanning, Multi-Scanning Anti-virus, and File Sanitization, it becomes evident that these technologies are not merely features; they are the vanguards of a new era in data security, redefining the standards for safeguarding sensitive information in an interconnected digital landscape.

ML File Scanning: Defender Max Safe employs cutting-edge Machine Learning (ML) File Scanning, a dynamic and intelligent mechanism designed to analyze file content using sophisticated algorithms. ML enables the platform to adapt and evolve its threat detection capabilities based on patterns and behaviors, enhancing its ability to identify and thwart emerging and complex threats. By leveraging ML, the platform ensures a proactive defense against potential security breaches and malicious activities embedded in uploaded files.

Multi-Scanning Anti-virus: The Multi-Scanning Anti-virus feature within the Defender Max Framework signifies a robust line of defense against a multitude of known and unknown viruses. By integrating multiple antivirus engines, the platform enhances its detection accuracy and resilience, effectively mitigating the risks associated with diverse malware strains. This approach provides a comprehensive shield, ensuring that files undergoing scanning are subjected to a thorough examination from various antivirus perspectives, thus fortifying the overall security posture.

File Sanitization: File Sanitization is a critical component of the Defender Max Framework, offering a proactive strategy to neutralize potential threats within files. This process involves the removal or neutralization of malicious elements, such as embedded scripts, macros, or hidden vulnerabilities, without altering the core functionality of the file. By implementing File Sanitization, the platform ensures that even if files contain potential risks, they are rendered harmless before being integrated into the corporate environment. This preventative measure significantly reduces the chances of security incidents resulting from file uploads and enhances the overall resilience against sophisticated cyber threats.

In summary, the Embedded Defender Max Framework Technologies—ML File Scanning, Multi-Scanning Anti-virus, and File Sanitization—form a formidable trio, collectively contributing to a multi-layered defense strategy. This framework not only identifies and neutralizes existing threats but also evolves alongside emerging risks, positioning Defender Max Safe as a stalwart guardian of data security in the realm of eXtended file upload platforms.



Licensing Note for Defender Max Safe: Enabling Limitless Connectivity and Scalability

In embracing a user-centric and scalable approach, the licensing model for Defender Max Safe has been meticulously designed to provide organizations with unparalleled flexibility and accessibility. The licensing structure is characterized by two fundamental principles:

1. **No User Count Limitation:**

Defender Max Safe liberates organizations from the constraints of user count limitations. There are no arbitrary ceilings imposed on the number of users who can benefit from the secure eXtended file upload platform. This user-friendly approach ensures that organizations can seamlessly onboard and engage users across various departments, suppliers, and collaborators without any hindrance.

2. **No Connector Number Limitations (API, Web, Agent, SFTP):**

Recognizing the diverse channels through which users interact with the platform, Defender Max Safe imposes no limitations on connector numbers. Whether it's through APIs for automated processes, the web portal for user-friendly interactions, agents facilitating remote access, or secure file transfer protocol (SFTP) for automated transfers, organizations can leverage an unrestricted number of connectors. This lack of limitation fosters an environment where organizations can embrace a variety of connectivity options without being encumbered by arbitrary restrictions.

The absence of user count and connector number limitations aligns with the overarching ethos of Defender Max Safe— providing organizations with a dynamic and scalable solution that adapts to their unique operational requirements. This licensing freedom empowers organizations to scale their usage organically, ensuring that the platform evolves seamlessly alongside the organization's growth and changing needs. With Defender Max Safe, the focus is not just on securing files; it's also on liberating organizations from the shackles of rigid licensing structures, allowing them to harness the full potential of the eXtended file upload platform

XFT Platform – Architecture

Enabling Defender Maxx XFT platform, will deliver any corporate the ability to have multiple scanning options , including Manual and automatic file uploads and sharing via Web portal , SFTP and Agent.

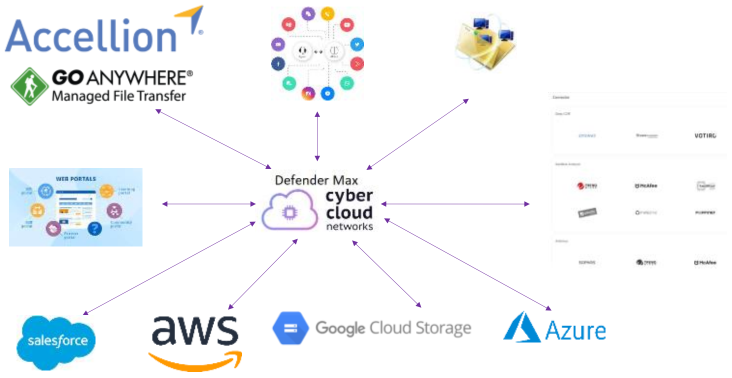
Platform will enable ability to intercept files received via API connectors by Mobile Applications, Web Portals and SaaS applications.

Platform will be able to monitor , scan and clean files on Local CIFS bases file servers or Cloud Storage services, such as AWS S3,Azure Blob and Google Storage.

Platform will also enable connectivity to existing file sharing platforms and SFTP/FTP servers.

The various connected file services are utilizing our Zero trust file approach, that enables Static and Dynamic analysis via our Defender Framework as well as existing Corporate cyber security engines.

Scan File uploads of any App


Accellion
GO ANYWHERE®
Managed File Transfer
WEB PORTALS
Defender Max
cyber
cloud
networks
salesforce
aws
Google Cloud Storage
Azure