eXtended OT / IT secure File transfer

XFT Platform Defender Max

cyber cloud networks

Defender Max cyber cloud networks

“In the age of digital transformation, safeguarding your corporate data is not an option; it's a necessity. Introducing Defender Max, a next-generation eXtended file scanning platform that redefines security through a perfect blend of manual and AI automation, offering a seamless File Orchestration Platform. Whether as a SaaS service or on-premise, Defender Max is your fortress against cyber threats , providing Unparalleled secure file scanning with unique Integrations to your corporate security engines and services from Cyber Cloud Networks Defender framework.”

In an era where data is the lifeblood of organizations, the demand for robust and secure connectivity between Operational Technology (OT) and Information Technology (IT) networks has never been more critical. Defender Max emerges as the ultimate eXtended file transfer scanning platform, bridging the gap between these two domains with unparalleled efficiency and innovation. In this digital age, where cyber threats loom large, Defender Max stands as a beacon of trust, offering a comprehensive solution to secure data transfer.

Defender Max's Vision

Defender Max envisions a world where data flows seamlessly between OT and IT networks, ensuring efficiency, scalability, and, most importantly, security. Its mission is to revolutionize data security by introducing novel approaches to file scanning, orchestration, and connectivity, setting new benchmarks in the realm of cybersecurity.

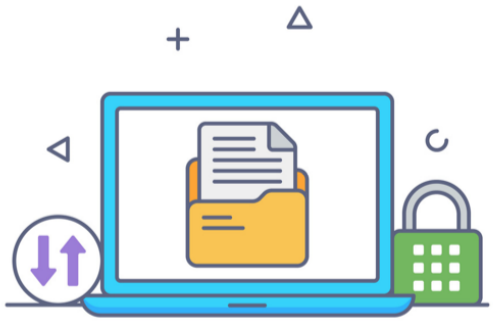
"The Defender Max platform serves as a sentinel guarding the critical juncture where IT and OT networks converge, ensuring airtight security through a combination of cutting-edge technologies."

Addressing Critical Needs:

The need for a robust eXtended file transfer scanning platform becomes evident when considering the challenges faced by organizations. Defender Max addresses the critical aspects of secure file transfers, including the necessity for patch updates in IT and OT applications. Beyond conventional security measures, it recognizes the significance of isolating file updates to prevent malicious intrusions into OT network assets.

Defender Max's impact is not confined to theoretical concepts; it has manifested its capabilities in real-life implementations across diverse industries. For instance, in a large manufacturing facility, Defender Max seamlessly integrated with existing security engines, providing a centralized platform for secure file scanning. This implementation resulted in a significant reduction in the time spent managing user accounts, ensuring compliance with standardized access restrictions, and successful integration of Single Sign-On (SSO) systems.

In the healthcare sector, Defender Max played a pivotal role in securing the transfer of sensitive patient data between OT and IT networks. The platform's ability to scan files with multiple security engines, including sanitization, sandboxing, machine learning, antivirus, and data loss prevention, ensured the confidentiality and integrity of healthcare information.



Secure Data Transfer

Key Features and Innovations

Defender Max boasts a rich set of features, including web portal support for manual file scanning, diverse user authentication options, and automation technologies for user account management. Its support for Secure File Transfer Protocol (SFTP) with a unique One-Time Password (OTP) mechanism ensures not only secure transfers but also ease of use.

Deployment Flexibility

Recognizing the diverse needs of organizations, Defender Max offers flexible deployment modes. Whether through a Consumption-Based SaaS model, a Hybrid model integrating with corporate infrastructure, or a fully Isolated On-Premise solution, organizations can choose the deployment mode that aligns with their specific requirements.

Why Defender Max?

1. **Patch Updates: Ensuring Seamless Security**

In the dynamic landscape of IT and OT, staying abreast of software updates and patches is non-negotiable. Defender Max facilitates this process with utmost security. For instance, consider a scenario where a critical security vulnerability is identified in the control systems of an industrial plant. Timely patching is imperative to mitigate potential risks. Defender Max acts as a secure conduit, allowing the seamless transfer of these patches while mitigating the risk of cyber threats during the update process. By providing a dedicated platform for the secure transmission of updates, Defender Max ensures that critical

systems remain protected without compromising operational efficiency.

2. **Security Policy Compliance: A Non-Negotiable Imperative**

Compliance with security policies is the cornerstone of a resilient cybersecurity strategy. Defender Max acknowledges the gravity of secure file transfer as an integral part of organizational security policies. For instance, in a financial institution handling sensitive customer data, compliance with data protection regulations is paramount. Defender Max guarantees that each file transfer adheres to the stipulated security policies, preventing the inadvertent flow of malicious updates into the OT network. This meticulous adherence to security protocols not only safeguards critical assets but also ensures the organization's compliance with industry regulations and standards.

3. **Isolation Mode: Fortifying Network Defenses**

Defender Max introduces a groundbreaking Isolation Mode to fortify network defenses. Imagine a scenario in which software updates need to traverse from the internet connection to the OT network. The Isolation Mode acts as a shield, preventing direct file upload pushes to the internal corporate network. This added layer of protection is exemplified in scenarios where a multinational corporation seeks to update its manufacturing execution systems. By isolating the transfer of files, Defender Max ensures that potential threats are contained within the OT network, shielding the broader corporate infrastructure. This innovative feature is pivotal in preventing unauthorized access and maintaining the integrity of critical systems.

Platform Specifications Unveiled: Elevating Defender Max's Capabilities

Defender Max stands out as a cutting-edge eXtended file transfer scanning platform, distinguished by its robust platform specifications that cater to the diverse and intricate needs of secure data transfer. Let's delve into the key features with examples illustrating their professional applications:

Web Portal Support: Defender Max provides a user-friendly web portal for OT network administrators to manually scan files/packages. In a manufacturing facility, the OT administrator accesses the web portal to initiate manual scans on files received from external suppliers. This ensures that no malicious content enters the OT network, maintaining a secure operational environment.

User Authentication: The platform supports various user authentication methods, including Guest, local, LDAP users, and Single Sign-On (SSO). A healthcare institution adopts Defender Max with LDAP integration, facilitating seamless authentication for healthcare professionals. This enhances the overall user experience and bolsters security measures.

Desktop Client for Monitoring: Defender Max offers a client for OT and IT desktops to monitor external storage devices (Disk on Key, CD) and local folders for scanning. In a research laboratory, scientists utilize the desktop client to monitor external devices for files containing critical research data. This ensures that only clean and secure files are transferred to the IT network, preserving research integrity.

SFTP Support with OTP Mechanism: Automatic transfers are facilitated through Secure File Transfer Protocol (SFTP) with a unique One-Time Password (OTP) mechanism for enhanced security. A financial institution employs Defender Max for secure financial report transfers between IT and OT networks using SFTP with OTP. This safeguards sensitive data during transit, meeting regulatory requirements.

Remote Agents for Parallel Transfers: Remote agents integrate with the central network, enabling file transfers to multiple sites in parallel. A multinational corporation deploys Defender Max to efficiently distribute software updates across global offices. This simultaneous transfer reduces time and ensures uniformity in software versions.

Isolation Mode and Approval Mode: Isolation mode prevents direct file uploads to the internal corporate network, while approval mode allows Safe administration to approve uploaded files. In a research and development environment, Defender Max's isolation mode ensures a rigorous approval process for files uploaded by external collaborators. This guarantees that only approved files integrate into the internal network, safeguarding valuable research assets.

Multiple Security Engines: Defender Max scans uploaded/shared files with multiple security engines, including Sanitization, Sandbox, ML/AI, AV,

DLP, and Container security. An aerospace engineering firm benefits from Defender Max's multi-engine approach to inspect design files thoroughly before sharing them internally or externally. This ensures compliance with industry standards and mitigates potential threats.

File Type Identification and Customized Scanners: The platform supports file type identification and allows the addition of customized scanners for unique file types. A legal firm employs Defender Max to identify and scan diverse document types, including proprietary legal formats. This ensures compliance and security in document transfers, crucial for maintaining client confidentiality.

On-Demand Security Engine Enablement and Load Balancing: Security engines can be enabled on-demand via Cyber Cloud Networks Defender framework, and multiple engines are load-balanced for optimal performance. A technology company dynamically adjusts security engine usage based on network traffic using Defender Max. Additional engines are activated during peak periods, optimizing overall performance and responsiveness.

Multiple Actions: Defender Max offers multiple actions such as Monitor, Scan, Alert, Block, and Replace content. An e-commerce platform employs Defender Max to monitor and scan customer data files. Automated actions, like blocking or alerting administrators, ensure swift responses to any suspicious activity, fortifying cybersecurity measures.

Integration with Data Diodes: Integration with Data Diodes ensures secure isolated file transfer, enhancing data integrity and preventing unauthorized access. A government agency secures classified document transfers between IT and OT networks using Defender Max with Data Diode integration. This maintains the highest level of confidentiality and compliance with security protocols.

AI-Based Insights for Content Inspection: Defender Max incorporates AI-based insights for advanced content inspection, providing enhanced security intelligence. A research institution benefits from Defender Max's AI-based insights, identifying patterns and anomalies in research data files. This proactive approach allows for timely security measures and protects valuable intellectual property.

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