mxlayer

Email Security Made Easy

Advantages

- Designed with Multi-tenancy Partners and Service Providers in Mind
- %100 White Labeling Full Branding Support
- Open to Partnerships Public/Private Local Clouds On-prem Installation Licenses
- Complete Email Security Business Continuity and Long Term Archiving

MX Layer UMG Unified Mail Gateway

Scalable and Powerful SaaS Cloud Email Security

MX Layer Unified Mail Gateway ensures the security of your email server in public and private cloud environments. You can easily activate UMG licenses for your email services running at your own cloud in your office or in your preferred cloud service provider. UMG instantly maximizes your email security.

MX Layer UMG is designed to work in all environments that require next level email security. You can receive MX Layer SaaS services from our public cloud or you can use it in your private cloud environment with on-site licensing. In line with the data regulation laws of your country where your business is located, it is possible to set up and run services on your local cloud and harmonize data security and portability.

Decisions Powered by Artificial Intelligence

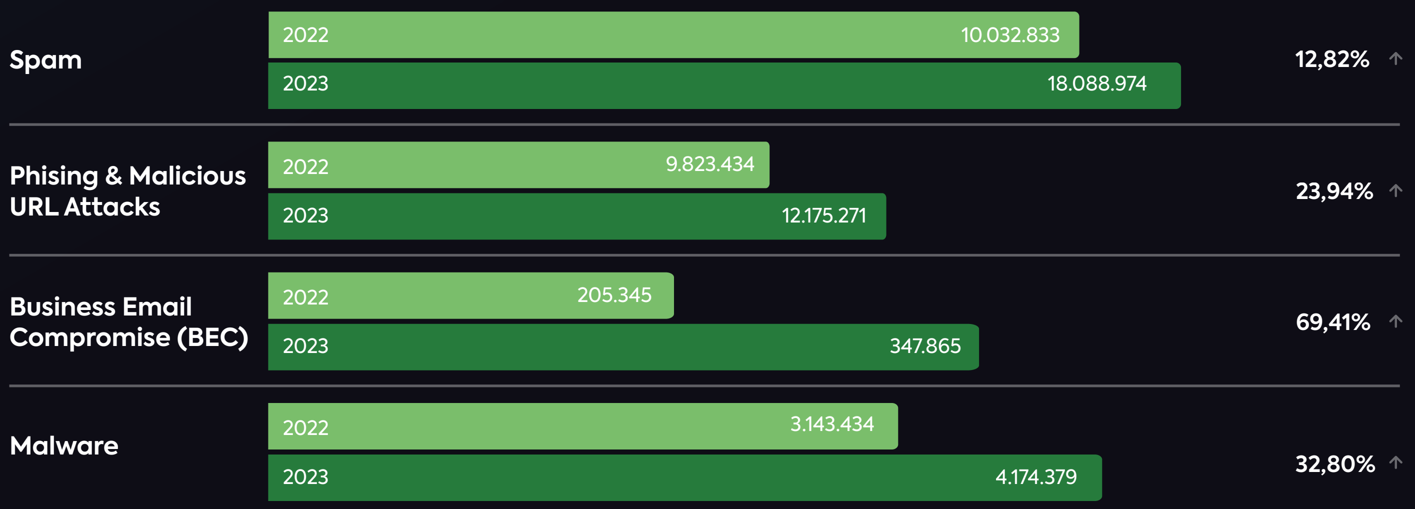
AI Protection Against Email Based Zero-Day Threats

Successfull cyber threats that businesses face often start with email messages. This fact is well known by the hackers who create malware.

Hackers tend to create personalized cyber threats using popular artificial intelligence tools. Developers of security products, on the other hand, use AI and machine learning to understand cyber threats before they are classified and to warn and protect the target organization before the threat materializes.

Threats known as zero-day attacks, can be easily understood with artificial intelligence and machine learning models. Queries that reach zero-day data collection centers from different sources are evaluated with AI tools. Even messages that generate these queries have not yet been identified as threats, AI can recognize they contain threats and immediately generates alarms. The queries, considered as the identifying fingerprints of new threats, are turned into intelligence, distributed with updates and made available to all users with traditional scanning tools.

Distribution of Recent Email Borne Threats



Stop Email Based Threats Before They Start

According to research, 91% of successful cyber attacks start with an email message. The rate is so high because direct access to targeted individuals is the easiest way via email. The most important reason for this situation is due to basic security vulnerabilities related to the design of email communication.

Email security products are designed to close these gaps. In addition to strong anti-spam and anti-virus protections, it is also a necessity to implement email specific security applications that have become industry standards in email communication. When all these come together with the right implementation plans, cyber threats are prevented before they turn into damage.

Proven Performance with Hundreds of Thousands of Users

MX Layer UMG provides an easily customizable security platform for thousands of users on the SaaS email security cloud with different needs. Our goal is to provide all these different needs with a stable performance and to meet expectations for services that are uncertain who will actively use them and when.

MX Layer SaaS Email Security Cloud, which is constantly updated in terms of both security and performance, offers you this experience with the MX Layer Unified Mail Gateway UMG product. It is not only security oriented, but also allows you to meet your compatibility requirements at the highest level.

Protection Independent of Your Email Server Brand

The UMG platform is designed as a Unified Mail Gateway to protect both open source email server environments and Microsoft Exchange environments. UMG not only protects email communication, but also allows you to easily perform daily administrative tasks such as queue management, traffic monitoring and logs that cannot be easily done in your existing environment. In addition, it simplifies the lives of administrative and technical teams with compliant email archiving and access to deleted old emails.

UMG has enhanced integrations with Zimbra OSE and MS Exchange Server that delivers extra user authentication capabilities like 2FA Multi Factor Authentication with SMS and Mobile App. You can easily harden your Webmail security and create Self Service Password Reset functionality integrated directly to your MS Active Directory and LDAP authentication sources.

Differentiated Management Tools at All Tiers with Multitenancy

With UMG, it is possible for different users to manage multiple organizations in your organizationand the security policies of separate domains belonging to each organization. With Multitenant management tools, administrators can be classified into three different management levels and different authorizations can be defined for each of them and all of them can be controlled from the top with a single administrator. Administrators and end users can be separated by using different visual themes and logos for each domain and organization.

Email Security Made Easy by MX Layer

Due to the nature of the Cyber Security, there is a certain level of difficulty in the use of products and platforms. The UMG platform is based on a product that has been used by thousands of companies and email users with different levels of knowledge, capturing profile diversity and built accordingly. Even the most difficult security rules and policies are handled with an email-specific approach and are organized for easy implementation. Advanced policy mode is also available for different levels of implementation.

Antivirus / Antispam & URL Filtering

MX Layer UMG's advanced antivirus and antispam protection features ensure that your organization's email security is always up-to-date and effective against the latest cyber threats. It uses signatures from various third-party vendors to create an advanced and universal intelligence database against current cyber threats.

UMG's URL scanning feature also provides an additional layer of security by scanning and analyzing all URLs in emails to detect links to malicious websites, allowing your company to protect against cyber attacks.

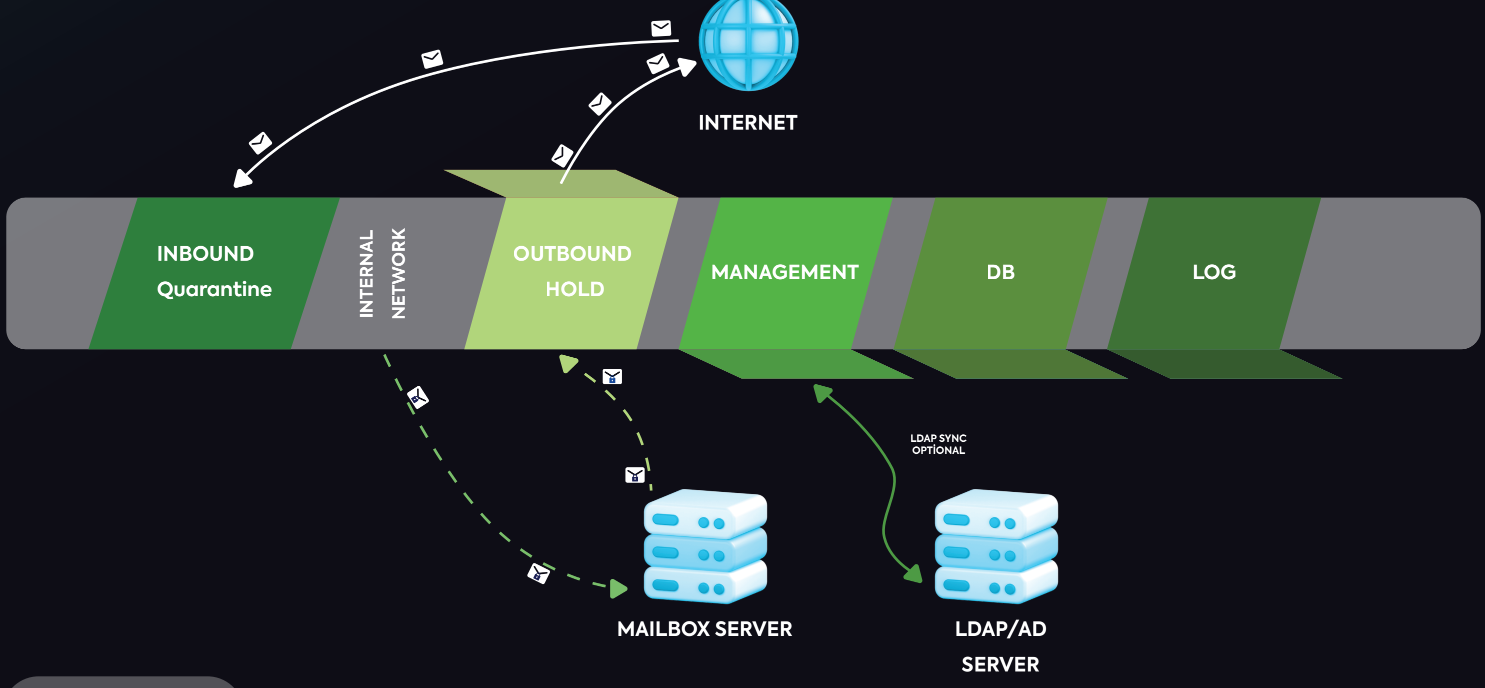
Outbound Gateway Protection

The MX layer's outbound gateway protection helps prevent outbound spam and IP blocking while improving email delivery and continuity. With reporting and tools provided by the outbound filtering solution, it automatically detects network abuse and allows you to lock out compromised users.

Spam, Malware and Phishing Protection

MX Layer UMG's exceptional functionality protects your vital communications against sophisticated email threats such as business email compromise BEC, ransomware, phishing and malware thus providing comprehensive protection you can trust.

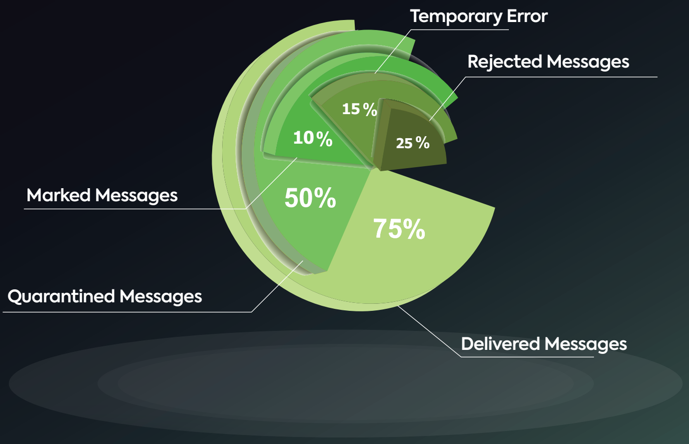
Single Site On-prem Installation Scheme



mxlayer

Visual Support for Security Teams

Graphs that instantly show real-time email traffic to cybersecurity teams, making it easier to tighten security policies.



Advanced Log Discovery Capabilities

Mail messages are logged extensively at every stage of the flow giving you verbose information for trouble shooting. All user and administrator activities are logged for compliance. With Rest API calls, any logged information can be fetched in raw or json formats making MX Layer ready to integrate with external SIEMs.

Technical Specifications for On-site Installations	UMG-VM01	UMG-VM02	UMG-VM03
Hypervisor Support	VMware ESXi , XenServer, MS Hyper-V, KVM		
Operating Systems	Rocky Linux 8, RedHat EL 8		
File System Support	EXT4, XFS		
Number of Virtual Servers*	8	19	23
Number of Virtual CPUs	34	84	104
Total Disk Space	850 GB	2.5 TB	3 TB
Total Log Disk Space	1 TB	3 TB	3 TB
Total Memory	128 GB	256 GB	296 GB
Processing Performance (Messages/Hour), (100 KB Delivered Message Size without any delay)			
Email Send/Receive	25000	50000	100000
Message Scanning AS + AV + URL	20000	40000	75000

* Virtual platforms are scalable and configurable for resilience. Performance, Redundancy and Load Balancing levels can be increased with expansion of server numbers. Services are not interrupted while scaling.

MX Layer on Public Cloud or On-Prem

FEATURES

1 Platform Specifications

- PaaS and SaaS Ready Cloud
- Single and Multi Site On-Prem Installations
- CRM Ready API Built-in WHMCS Support
- Integration Ready with Documented Rest API
- Runs on Redhat or Compatible Linux

2 Inbound Security

- Multiple AS/AV Engines
- Commercial and Free Signature DBs
- Realtime URL Filtering and Sanitizing
- Zero-Hour and Sandbox Options
- Anytime URL Sanitizing Option

3 Identity & Authentication

- External Authentication Sources
- LDAP and Active Directory Ready
- Password Challenging with IMAP Mailbox
- Passwordless Login with SMS and IMAP
- MFA Ready with SMS and Mobile APP

4 Outbound Security

- DLP Policy Chain with Prohibitive Actions
- Custom and Predefined Sender Quotas
- Counters for Anomaly Detection
- Disclaimer and Signature Ready with Variables
- Dedicated IP Management Option

5 Target Compatibility

- Compatible With Any MTA
- Enhanced Integration with Zimbra
- Enhanced Integration with MS Exchange
- Single Domain Multiple Mail Server Support
- Optional Mailbox Ready Installations

6 Compliance

- Business Continuity for Always On Messages
- Long Term Immutable Archiving Support
- Traffic and Management Logs with Discovery
- SIEM Integrations with Rest API and Syslog
- Long Term Log Storage with Time Stamping

mxlayer

Partnering with MX Layer

You can register MX Layer Email Security partnership program more than one way.

• Licensing UMG to your customers through the MX Layer SaaS platform is the fastest and easiest way of activating MX Layer partnership. You can start serving your customers as our **SaaS Solution Sales Partner** in a very short time and with zero investment cost.

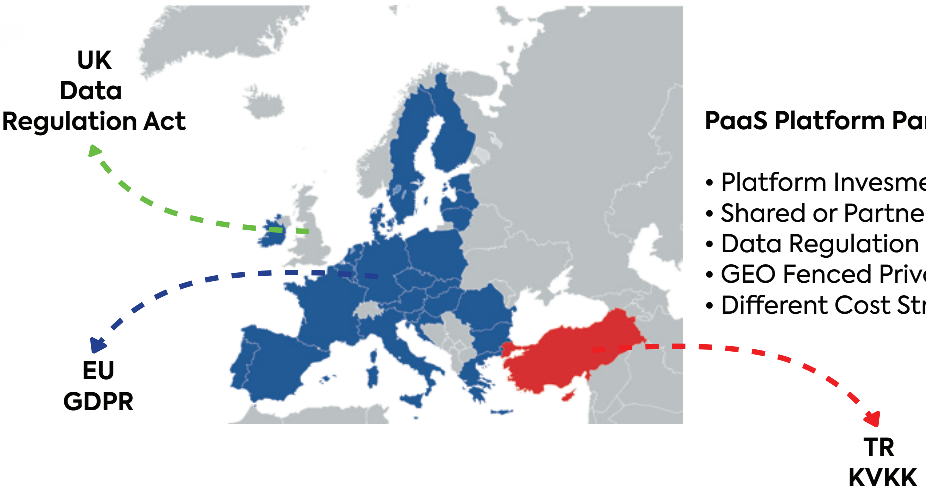
• It is possible to produce a SaaS platform within a certain geographical boundary and create an Email Security Cloud of your own brand in order to provide services in accordance with the data policies of the relevant borders. You can choose our MX Layer **PaaS Platform Partner** program to create this platform.

• MX Layer UMG **On-site License Sales Partner** program will be the right choice for the on-prem installation and service needs of your customers of certain sizes and subject to strict data regulations.

MX Layer Partner programs are designed for your different needs. Let's discuss for registering the right program.

SaaS Solution Sales Partner

- SaaS Solution on MX Layer Cloud
- No Upfront Costs, Training Requried
- Branding Support, White Labeling
- Customer Based Discounts
- Volume Based Discounts



PaaS Platform Partner

- Platform Invesment Costs
- Shared or Partner SaaS Platform
- Data Regulation Boundaries
- GEO Fenced Private Cloud
- Different Cost Structures

On-site License Sales Partner

- Customer Based On-site Licensing
- Customer Site On-prem Installations
- User Based Multi Location Licences
- Cpu Core Based Unlimited Licenses
- Installation and Platform Training Required

mxlayer

Email Security Made Easy

Las Vegas, NV, US

Partners Wanted!

MSPS

TELCOS

LOCAL CLOUDS