zix®

COMPATABILITY GUIDE

Zix works in your environment because our products are based in standards such as SMTP, SAML and OATH. We have thousands of customers using Zix in diverse environments, and we know that we can leverage your existing IT investments and quickly deploy Zix to provide enhanced email security.

The Zix Compatibility Program recognizes the products and services that work with Zix. In some cases, the interoperation comes about from mature standards interoperability. In other cases it comes from additional features such as X-header scanning.

We created the compatibility program to give you assurance that Zix fits with each element of your email, security and regulatory compliance ecosystem.

Zix Support for Standards

Zix Compatibility Program requires support for standards, which ensure that Zix will interoperate with many different complementary solutions in your organization.

SMTP interoperability ensures that Zix can examine, filter and encrypt any email-based traffic without impacting other solutions within your email infrastructure. This includes solutions such as email servers and services, enterprise information archiving, and secure email gateways.

Zix can integrate with third-party products through the syslog standard to provide reporting within a Security Information and Event Management solution, in addition to providing alerts within the Zix management framework.

Zix supports open authentication through support for the SAML 2.0 standard for exchanging authentication and authorization data between security domains. Zix also supports the OAuth standard to enable users to gain access to protected information without requiring a new identity and password.

We understand that your environment may be complex, and the Zix Compatibility Program provides peace of mind that Zix email security will work with your existing IT ecosystem and investments.

Let's examine how Zix works with complementary solutions and provide a sample list of the providers in each category.

Email Servers and Services

More than 15 years of experience and thousands of customers demonstrate that Zix solutions work with a wide variety of email servers and services. SMTP interoperability and dedicated integration with leading providers such as Google and Microsoft ensure email is sent and received securely, regardless of which provider you are using.

Zix solutions work with:

- Microsoft Outlook and Office365
- Google G Suite and Gmail
- Groupwise
- IBM Notes
- PostFix
- SendMail
- Zimbra
- Yahoo and AOL

Sender → **Mail Server or Service** → **Gateway Encryption** → **Recipient**

zix
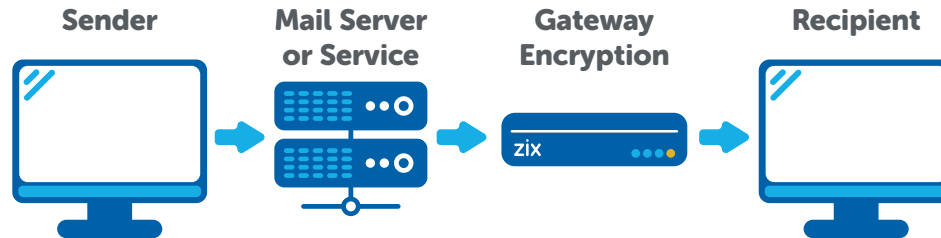
Enterprise Information Archiving

Archiving message content from email systems is used by many organizations for compliance, risk management, governance and cost optimization. ZixEncrypt offers a gateway architecture that encrypts email at the edge of the network, allowing your emails to be archived in the clear and easily retrievable. In addition, ZixEncrypt's transparent delivery allows many of your partners to decrypt their email at the edge of their network, meaning you aren't affecting their ability to archive either. Zix's support for TLS can also be used to help your partners archive.

ZixMail, our end-to-end email encryption, supports a feature called corporate key, which allows companies the capability of decrypting email for business continuity. This means your archived emails are always retrievable.

Zix email encryption solutions work with many information archiving solutions, including those from:

- Commvault
- Dell EMC
- Global Relay
- HPE
- Mimecast
- Proofpoint
- Smarsh
- Veritas

Sender   Mail Server or Service   Gateway Encryption   Recipient

Clear text email

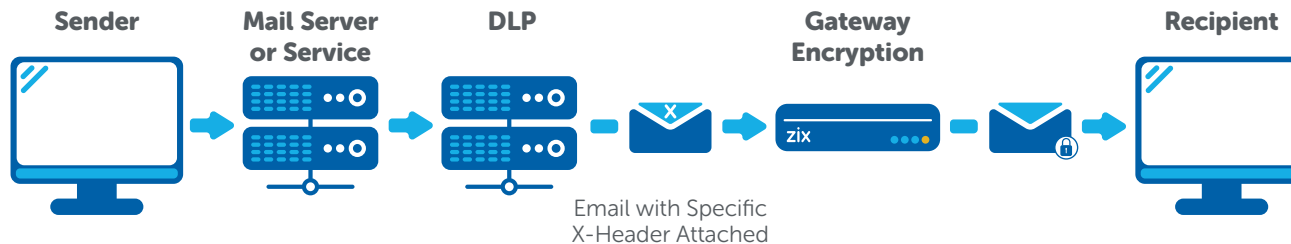Archive
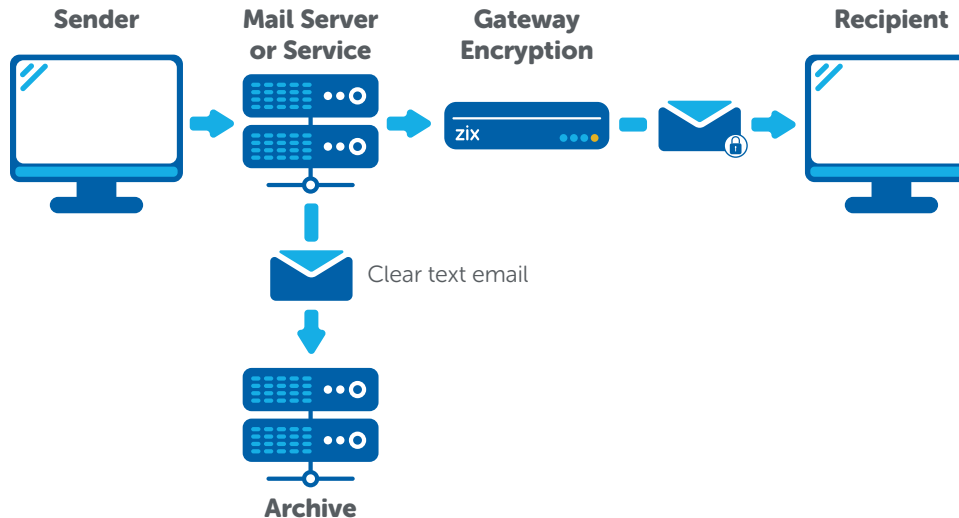
Enterprise Data Loss Prevention

Organizations use enterprise data loss prevention (DLP) to prevent inadvertent or accidental exposure of sensitive information to unauthorized users. ZixEncrypt includes DLP features that enable emails to be quarantined by policy, giving your employees, managers and IT administrators the chance to correct a message sent in error. Zix can also be used in conjunction with other DLP solutions to ensure that emails with sensitive information are protected with encryption by policy, without requiring any extra work by users.

Zix Email Encryption supports X-header filtering. This allows DLP solutions to instruct Zix Email Encryption on the disposition of email. For example the DLP solution could define which messages should be encrypted. This has an advantage over using DLP routing. Since every email can flow through Zix Email Encryption, the Zix Encryption Network can be leveraged. This provides an additional level of security with every email sent between Zix customers being encrypted.

Zix works with many enterprise DLP providers, including:
- Digital Guardian
- Fidelis Security
- Forcepoint
- Intel Security
- Symantec

Sender   **Mail Server or Service**   **DLP**   **Gateway Encryption**   **Recipient**

Email with Specific X-Header Attached

Authentication and Single Sign On

Authentication is an important component of email encryption. When email is securely delivered using a Zix secure web portal, customers can use the native authentication of Zix, or they can use the credentials they have already established with their customers.

Zix secure web portals support Google and Microsoft OAUTH for customers that send encrypted emails to consumer email accounts. This eliminates the need for the user to register or remember yet another password.

For organizations with a single sign on solution (SSO), Zix secure web portals act as the SAML 2.0 service provider (SP) and the SSO solution acts as the identity provider (IP).

When a user tries to access the secure web portal that has been configured to use SSO, the user signs on to the IP and is then redirected back to the Zix secure web portal after being authenticated.

Zix also supports SSO, where the user signs into the IP and then uses a custom link to access the Zix secure web portal without being required to sign in.
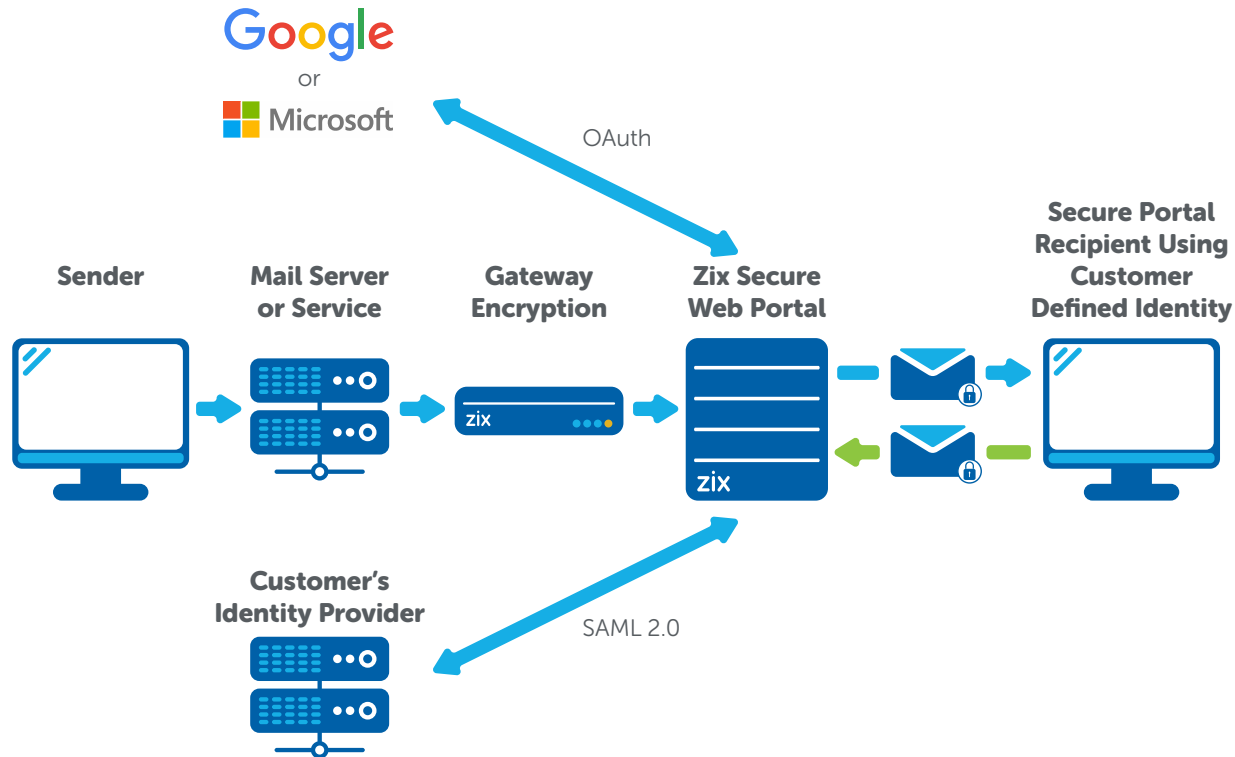
Zix will work with any SAML 2.0 Identity Provider, including:
- CA Technologies
- Dell Technologies
- Entrust
- IBM
- Micro Focus
- Okta
- Oracle
- Ping Identity
- SailPoint

Authentication and Single Sign On *cont'd*

Google
or
Microsoft

OAuth

Sender

Mail Server
or Service

Gateway
Encryption

Zix Secure
Web Portal

Secure Portal
Recipient Using
Customer
Defined Identity

Customer's
Identity Provider

SAML 2.0

Network Security and Unified Threat Management

Network security is a given for all organizations, and Zix works with it, from firewalls to intrusion prevention systems. We know that for many organizations with limited IT resources and budget that unified threat management (UTM) devices that combine enterprise firewall and intrusion prevention systems, as well as secure web and email gateway functionality, in a single appliance are a popular choice.

Here at Zix, we work with network security and UTMs due to our support for SMTP. We work with vendors such as:

- Barracuda Networks
- Checkpoint Technologies
- Cisco
- Dell Sonicwall
- Fortinet
- Juniper Networks
- Sophos
- Watchguard

Sender   **Mail Server or Service**   **UTM**   **Gateway Encryption**   **UTM**
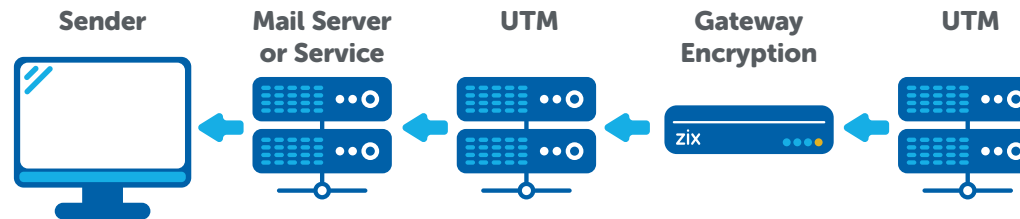
Secure Email Gateways

We know that most organizations have secure email gateways (SEGs) to protect from spam and email-based threats. Zix can provide a secure email gateway solution bundled with email encryption, but if you already have a SEG solution, Zix works with that too.

Zix solutions work with SEGs due to our SMTP interoperability. We work with vendors such as:

- Barracuda Networks
- Cisco
- Dell SonicWall

- ForcePoint
- Fortinet
- Mimecast
- Proofpoint
- Sophos
- Symantec
- Trend Micro
- Trustwave
- Watchguard

Sender → Mail Server or Service → SEG → Gateway Encryption → SEG
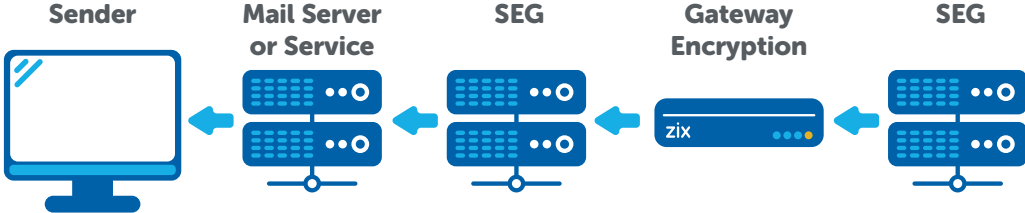
Security Information and Event Management

Many organizations use security incident and event management (SIEM) solutions to enhance their situational awareness by aggregating event data produced by security devices, network infrastructure, systems and applications.

Zix allows administrators to automatically export encrypted email data logs into a syslog format for integration with SIEM solutions such as:

- Alienvault
- EMC (RSA) Netwitness

- HPE Arcsight
- IBM QRadar
- Intel Security
- LogRhythm
- Micro Focus
- NetIQ
- Splunk
- Trustwave

Sender **Mail Server or Service** **Gateway Encryption**

Syslog Data
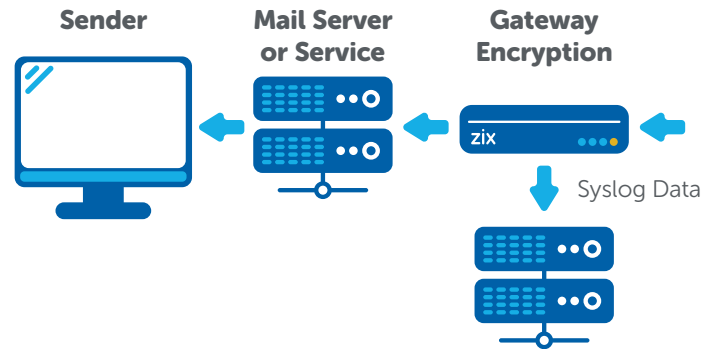
To learn more about our secure email capabilities and how we fit in your ecosystem, visit zixcorp.com or register for a demo here.

zix®

Phone 866-257-4949
sales@zixcorp.com
www.zixcorp.com