# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Voltage SecureMail for Office 365</td>
<td>1</td>
</tr>
<tr>
<td>The Email Security Considerations When Adopting Microsoft Office 365</td>
<td>2</td>
</tr>
<tr>
<td>The Voltage SecureMail End-to-End Email Encryption Solution with Office 365</td>
<td>2</td>
</tr>
<tr>
<td>IT Interoperability with O365: How Can Voltage SecureMail Integrate with the Office 365 Environment?</td>
<td>7</td>
</tr>
<tr>
<td>Voltage SecureMail Feature Compatibility</td>
<td>8</td>
</tr>
<tr>
<td>SecureMail Deployment Models with O365: How to deploy SecureMail with O365</td>
<td>8</td>
</tr>
<tr>
<td>Summary</td>
<td>10</td>
</tr>
</tbody>
</table>
Introduction

Microsoft Office 365 is a highly capable suite of cloud-based productivity tools that includes email, calendaring, scheduling, task management, desktop productivity, telephony, real-time communications, and collaboration tools. All these components are hosted “in the cloud” on Microsoft servers, allowing users to tailor the package for their specific requirements, easily manage future upgrades, mitigate costs, and minimize IT labor requirements and migration challenges.

The increased convenience brings increased concern about combining inherently insecure email systems with cloud-based platforms. In an age of constant data and email breaches, customers require an end-to-end email encryption solution to protect both internal and outbound emails containing sensitive data. Voltage SecureMail provides a scalable email encryption solution that delivers the additional data protection you need with Office 365.

Voltage SecureMail for Office 365

Voltage SecureMail adds best-in-class e-mail encryption protection to Office 365 for corporations that want to implement end-to-end protection to their most sensitive information flowing across the business. Voltage SecureMail desktop email encryption plug-ins and native mobile client applications make it simple and easy for users to encrypt emails on their devices before transmission over private and public networks. This protects sensitive email content and makes it unreadable until it reaches the intended recipient. IT administrators use management tools to protect emails among internal Office 365 users and with external customers, partners, and users.

The Voltage SecureMail solution architecture supports on-premises, cloud, or hybrid cloud configurations to work with your existing Microsoft Exchange and Office 365 deployments. Email administrators can integrate Voltage SecureMail with existing email gateways, Active Directory (AD), SharePoint storage, email archive, and eDiscovery systems to efficiently add email encryption to your Office 365 environment.

Voltage SecureMail also enables companies to adopt best cloud security practices with a clear separation of duties and information. This allows companies to maintain complete access control over encrypted emails in the Office 365 cloud to meet regulatory compliance requirements and protect sensitive data from unauthorized 3rd party access.

This document outlines the Voltage SecureMail end-to-end email encryption benefits and deployment models to maintain uniform email encryption protection while migrating to Office 365. This document also assists Messaging Security Architects, Information Security Architects, Information Security Directors and IT staff design, set up, and configure the Voltage SecureMail solution with Office 365.
The Email Security Considerations When Adopting Microsoft Office 365

Email continues to be an invaluable business tool. It is also one of the most vulnerable communication channels with the potential for exposing sensitive business, customer, and personal data. Today’s IT email security solutions must guard against insider threats and unintended data loss due to human error. The following are critical email security questions that need to be considered to properly configure Microsoft Office 365 to meet your data security requirements.

- Where are cloud email messages and keys stored, and where are they visible?
- Who controls and manages the email encryption keys?
- How do you plan to encrypt internal and external emails?
- What devices will users be using to read and compose encrypted emails?
- Which cloud email deployment models does your business need to support? On-premises? Hybrid? Cloud?
- Have you deployed a centralized, company-wide Data Loss Prevention (DLP) solution?
- Do your email archive plans involve storage outside Office 365?

The built-in message encryption feature of Microsoft Office 365 can be added for an additional cost to certain Office 365 licenses and secures external email transport between the company to Office 365 and between Office 365 servers in the cloud with Transport Layer Security (TLS). However, internal emails on the corporate network remain unencrypted. Message Encryption requires an Office 365 administrator to configure and setup Exchange Transport Rules (ETR) for the user to trigger email encryption (there is no “send secure” button). Office 365 Message Encryption only provides gateway encryption, which is based on Microsoft DLP rules. As a result, the end user has to rely on Microsoft DLP rules to encrypt outgoing email.

The Voltage SecureMail End-to-End Email Encryption Solution with Office 365

Voltage SecureMail offers a number of user, administrator and business benefits with Office 365. It makes it easy for users to send encrypted email just like any other normal email. For administrators, the solution is simple to operate with minimal on-going maintenance and support, thus keeping your operating costs low.
The system can also be configured to automate email encryption to remove the dependency on users to encrypt emails containing sensitive data.

This section discusses the key features that makes Voltage SecureMail a natural complement to your Office 365 deployment.

**End-to-End Email Encryption**

Voltage SecureMail provides client endpoint message encryption capabilities to secure messages from when the message is sent until the message is opened by the intended recipient. Voltage SecureMail provides desktop email client plug-ins, web interface and native mobile device applications to encrypt and decrypt messages on the device, including all email replies. The encrypted email message and payload are sent and stored (i.e. “pushed”) to the recipient’s email system until the recipient is ready to read the message. Once the user is authenticated, the message is decrypted and presented to the user. This protects against TLS vulnerabilities and “man-in-the-middle” security threats as the email traverses the network to the recipients email system. Voltage SecureMail end-to-end encryption provides complete protection for Office 365 messages inside and outside the company.

**Voltage SecureMail Client Endpoints**

For Outlook desktop users, the Voltage SecureMail Encryption Client offers a simple, easy to use Outlook client plug-in that installs a “Send Secure” button on the desktop client. To send an encrypted email, the sender composes and attaches files to the email and clicks the “Send Secure” Outlook button instead of the regular “Send” button. There is no prerequisite to exchange certifications in advance to sending encrypted email. If the recipient has also installed the SecureMail Outlook plug-in, incoming messages will be automatically decrypted and presented to the recipient in the clear.

For mobile users, native Voltage SecureMail iOS and Android mobile client applications are available to automatically decrypt and read emails once the SecureMail user is authenticated. It is also used to compose and send encrypted emails. Voltage SecureMail email replies will be automatically encrypted to protect the entire email thread.

For client-less users such as users of Outlook Web Access (OWA), Voltage SecureMail offers the Zero Download Messenger (ZDM), which enables web users to easily read and reply (with the appropriate software license) to Voltage SecureMail messages in their web email systems without special client plug-in, or new software program downloads.
Figure 1 below illustrates the end-to-end email encryption flow with Office 365. In this configuration, Voltage SecureMail is deployed on the customer premises.

The following section describes the data flow with Office 365:

**Step 1** – Sender has installed the Voltage SecureMail Encryption Client. Email is encrypted at the sender desktop PC and sent to the hosted Microsoft Exchange Server (or Office 365).

**Step 2** – The hosted Microsoft Exchange Server (or Office 365) delivers the encrypted email to the recipient.

**Step 3** – The recipient authenticates with the Voltage SecureMail Server. The ZDM and Android mobile client transmit the encrypted email to the Voltage SecureMail Server for decryption. The iOS mobile client requests a decryption key for local decryption.

**Step 4** – The ZDM, iOS and Android mobile clients receive the decrypted email. The email message remains encrypted on the Office 365 (or Microsoft Exchange) server.

**Customer-Controlled Message Access and Key Management**

Cloud security best practices call for separation of duties and information. In the example of the built-in add-on message encryption feature of Microsoft Office 365, messages and message encryption keys
are stored in the Office 365 cloud and the keys are managed under a separate Azure RMS subscription. Companies that do not want cloud vendors to access their encrypted emails stored in the cloud can prevent unauthorized access by deploying Voltage SecureMail to encrypt the email messages stored in the cloud.

With Voltage SecureMail configured with Office 365, encrypted email messages are stored (or “pushed”) to the recipient’s email system so the email contents are not stored on a Voltage SecureMail server. Voltage SecureMail encryption are managed in the Voltage SecureMail Key Server on the company premises, or in the Voltage SecureMail Cloud outside the Office 365 environment. This allows the company to control the key storage and mitigate risk of unauthorized cloud administrator access to encrypted emails.

**Simple and Low Cost Email Encryption Operations**

Voltage SecureMail is built on Identity-Based Encryption (IBE) which offers a stateless key management solution that uses the recipient’s email address to generate the encryption key. Unlike other encryption techniques that use PKI, encryption keys do not need to be exchanged in advance with the recipient. Instead, the IBE (private) key is mathematically calculated when needed so there is no action required by the recipient. This greatly reduces the key management, IT administration effort, and costs associated with other email encryption solutions. It also increases the use of email encryption leading to a more secure and effective email solution.

**Flexible Deployment Models**

Many companies have Microsoft Exchange installed on their company premises and plan to move their users to Office 365. However, they may not be ready to move all at once. To allow the companies to move to Office 365 at their own pace, companies need an email encryption solution that will support both on-premises, hybrid, and cloud hosted Exchange deployment models.

Voltage SecureMail supports three flexible deployment models: on premise, hybrid, and in the cloud. This flexible architecture enables companies to design a Voltage SecureMail solution to support and secure their unique Exchange, hosted Exchange and/or Office 365 cloud email deployment. Organizations can dictate the migration path and pace to Office 365 while maintaining a consistent email encryption solution across their Exchange user community.

Voltage SecureMail server and gateways can be deployed on-premises or hosted by the customer to store IBE keys and encrypt emails before sending them to Office 365 (or hosted Exchange servers).
Additionally, Voltage SecureMail can be provided as a 100% hosted Software as a Service (SaaS) through the Voltage SecureMail Cloud offering. Voltage SecureMail Cloud allows a company to move email encryption infrastructure to the cloud including the Voltage SecureMail email encryption services for Office 365.

**File Level Encryption Options**
Voltage SecureMail offers a convenient file encryption feature called SecureFile. Voltage SecureMail Encryption Client users who want file security and user access control can adopt SecureFile to encrypt the file and define a list of users authorized to open and view the file in the clear. This helps companies utilize public cloud file sharing services like Microsoft OneDrive while securing their unstructured data files of almost any type. The SecureFile desktop plug-in adds an easy-to-use “encrypt” button to Microsoft Word, Excel and PowerPoint. SecureFile can also be implemented as a batch encryption process, or integrated with collaboration portals.

The standard Voltage SecureMail product already encrypts attachments in messages. But for very large attachments that could be blocked even by Office 365, we provide an alternative large file attachment delivery. The Voltage SecureMail Large Attachment Module maximizes deliverability of large attachments by avoiding file size restrictions. Attachments exceeding the size limit are automatically removed from the message, encrypted as SecureFile, and replaced in the message for a link the recipient can use to download it. These 2 features reduce the risk of employees using insecure means to exchange files.

**Inbound/Outbound Security Messaging**
Companies strive to deploy a company wide data governance and management strategy. Any solution must guard against data loss due to email misdelivery of sensitive data. With Voltage SecureMail, messaging security features can be integrated adding Data Loss Prevention (DLP) policy software to scan outbound emails, and AntiVirus/Anti-Spam software to filter inbound email.

An enterprise DLP solution is a key solution component to identify and classify data that needs to be protected. Voltage SecureMail integrates with 3rd party products to provide a best-in-class data classification and policy-based email encryption solution to automatically protect against unintended sensitive data leaks.

The Voltage SecureMail solution architecture supports enterprise DLP product integrations to protect data across all data storage depositories on-premises and in the cloud. This system wide approach makes it simple to manage and govern data protection uniformly across the company and Office 365, and avoids the creation of DLP policy silos from disparate tools and applications.
IT Interoperability with O365: How Can Voltage SecureMail Integrate with the Office 365 Environment?

Voltage SecureMail is compatible with Office 365 to seamlessly integrate email encryption in the Office 365 and email administration environment.

Office 365 Feature Compatibility
Voltage SecureMail is compatible with other IT functions to efficiently scale the solution and meet compliance requirements like eDiscovery, archiving, DLP and authentication.

The table below briefly describes the compatibility of Voltage SecureMail with specific functions in Office 365.

<table>
<thead>
<tr>
<th>Office 365 Feature</th>
<th>Voltage SecureMail Compatible?</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IN-PLACE EDISCOVERY</strong></td>
<td>✗</td>
<td>Voltage SecureMail eDiscovery Accelerator tool can decrypt messages in the Office 365 In-Place eDiscovery PST files.</td>
</tr>
<tr>
<td><strong>DATA LOSS PREVENTION (DLP)</strong></td>
<td>✗</td>
<td>Office 365 DLP rules and connectors can be configured to detect sensitive data (like social security numbers) and route emails to Voltage SecureMail server or gateway (using the FlagSecure tag) for email encryption. See the example below.</td>
</tr>
<tr>
<td><strong>ACTIVE DIRECTORY (AD) AUTHENTICATION</strong></td>
<td>✗</td>
<td>On-premises AD services and Office 365 can be used for Voltage SecureMail authentication. Compliant with message retention, eDiscovery, and hold requirements.</td>
</tr>
<tr>
<td><strong>ROUTING EMAIL TO SMART HOSTS</strong></td>
<td>✗</td>
<td>Office 365 message routing can be directed to the Voltage SecureMail Gateway for email encryption and decryption.</td>
</tr>
<tr>
<td><strong>ARCHIVING</strong></td>
<td>✗</td>
<td>Voltage SecureMail can decrypt Office 365 email archives.</td>
</tr>
<tr>
<td><strong>SHAREPOINT ONLINE</strong></td>
<td>✗</td>
<td>Voltage SecureMail and SecureFile are compatible with SharePoint in Office 365.</td>
</tr>
<tr>
<td><strong>OUTLOOK WEB ACCESS/APP (OWA)</strong></td>
<td>✗</td>
<td>Using Voltage SecureMail, encrypted email received in OWA can be decrypted using the Voltage SecureMail Zero Download Messenger (ZDM) web interface.</td>
</tr>
<tr>
<td><strong>OUTLOOK CACHED/ NONCACHED MODE</strong></td>
<td>✗</td>
<td>Voltage SecureMail supports both Outlook desktop message storage modes.</td>
</tr>
</tbody>
</table>

Table1. Voltage SecureMail function compatibility with Office 365.
Voltage SecureMail Feature Compatibility

Voltage SecureMail offers additional features that can enhance the functionality and usability with Office 365.

<table>
<thead>
<tr>
<th>Voltage SecureMail Feature</th>
<th>Is Office 365 Compatible?</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>VOLTAGE SECUREMAIL MOBILE</td>
<td>x</td>
<td>Voltage SecureMail Mobile apps allow you to read and compose encrypted emails with Office 365.</td>
</tr>
<tr>
<td>VOLTAGE SECUREMAIL ENCRYPTION CLIENT</td>
<td>x</td>
<td>Voltage SecureMail Encryption Clients work with Outlook clients configured with Office 365. Check supported versions of Windows and Outlook.</td>
</tr>
<tr>
<td>SAFELIST/SERVER POLICIES</td>
<td>x</td>
<td>A Voltage SecureMail has both server policies and client-based &quot;safelist&quot; that enable email to specific addresses or domains to be automatically encrypted or decrypted based on pre-set rules. Work with Office 365.</td>
</tr>
<tr>
<td>VOLTAGE SECUREMAIL LARGE ATTACHMENT DELIVERY (LAD)</td>
<td>x</td>
<td>Large file attachments that exceed Office 365 limits can be delivered via a download link in the Voltage SecureMail ZDM web tool.</td>
</tr>
<tr>
<td>SECUREFILE</td>
<td>x</td>
<td>Almost any files encrypted with SecureFile can be shared with Office 365.</td>
</tr>
<tr>
<td>DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING AND CONFORMANCE (DMARC)</td>
<td>x</td>
<td>Reduces IT administration effort to maintain and manage SecureMail Cloud sending trusted encrypted emails on behalf of the company’s email domain. Works independent of Office 365.</td>
</tr>
</tbody>
</table>

Table 2. Voltage SecureMail feature compatibility with Office 365.

SecureMail Deployment Models with O365: How to deploy SecureMail with O365?

Businesses may have on-premises Exchange solutions that have yet to be migrated to the Office 365 cloud. Therefore, businesses need an email encryption solution that will protect their on-premises email deployments and enable them to migrate from on-premises to the cloud as they desire.

Voltage SecureMail can be deployed to align with your IT and email system topology design and offer the email encryption controls needed with Office 365.

Voltage SecureMail on-premises with Office 365

The Voltage SecureMail on-premises server can be configured with current Microsoft Exchange on-premises servers, or Microsoft Hosted Exchange or Office 365.
Benefits:

- Customer manages a consistent email encryption solution regardless of email system location
- Customer controlled and managed email encryption key server

Below the Voltage SecureMail gateway resides on the customer premises and encrypts Office 365 emails sent to an external user. This configuration allows the sender to encrypt specific emails automatically with the Voltage SecureMail gateway. Emails to be encrypted can be identified by either a subject line trigger, by adding an Xheader, or by setting up rules based on an email ID or domain(s). Incoming email can also be automatically decrypted at the Voltage SecureMail gateway server.

The following section describes the email encryption data flow:

**Step 1** – An outbound email is composed and sent to Office 365 (hosted Microsoft Exchange server) for delivery. The email can be flagged for encryption using a subject line prefix, adding an x-header, or applying Office 365 DLP policies.

**Step 2** – Office 365 (hosted Microsoft Exchange Server) detects the email flagged for encryption and routes them to the Voltage SecureMail gateway server.

**Step 3** – The Voltage SecureMail gateway server encrypts the email and routes it to the Mail Transfer Agent (MTA) for delivery. The MTA can be part of the Voltage SecureMail Server or the Microsoft Exchange Server, or it can be any supported MTA.

**Step 4** – The MTA delivers the encrypted email to the recipient.

**Step 5** – The recipient authenticates with the Voltage SecureMail Server. The ZDM or Android mobile client transmits the encrypted email to the Voltage SecureMail Server which returns the decrypted email to the recipient. The iOS mobile client requests a decryption key for local decryption.
Step 6 – The ZDM or Android mobile client receives the decrypted email. The iOS mobile client receives the decryption key and decrypts the email.

Voltage SecureMail Cloud with Office 365

In addition to Microsoft Exchange on-premises and Hosted Exchange, SecureMail Cloud can be deployed with Office 365.

Benefits:
- Rapid email and encryption solution deployment
- Separate email encryption keys host from Office 365

Voltage SecureMail Cloud will encrypt and decrypt all Office 365 messages including replies. Voltage SecureMail manages the keys so customer maintain control over message decryption.

Summary

Voltage SecureMail is a natural complement to Office 365 to provide desktop and mobile email security controls to protect email content and attachments in the cloud. It extends email security to the client endpoints to encrypt emails before they are sent to the cloud ensuring end-to-end encryption. This helps ensure that organizations maintain complete control over sensitive data exchanged via email.

In addition, SecureMail architecture is flexible enough to support a smooth Microsoft Exchange migration to Office 365 and to integrate with best-in-class enterprise DLP solutions to deliver data classification
and policy-based email encryption to protect sensitive data stored on-premises and in the cloud. This enables companies to automate email encryption and centralize data protection administration across the company. With Voltage SecureMail, the email encryption solution puts you in control of your email and data protection in the cloud.

Appendix: Voltage SecureMail and Office 365 Message Encryption Comparison

Below is a comparison of Office 365 Message Encryption with Voltage SecureMail.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Office 365 Message Encryption</th>
<th>Details</th>
<th>Voltage SecureMail</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>GATEWAY RULES BASED ENCRYPTION</td>
<td>x</td>
<td>Gateway rules scan the email and encrypt it if the rules match.</td>
<td>x</td>
<td>Gateway rules or third party DLP like Digital Guardian scan the email and encrypt it if the rules match.</td>
</tr>
<tr>
<td>END-TO-END ENCRYPTION</td>
<td>NA</td>
<td>Email is encrypted on the Office 365 email gateway.</td>
<td>x</td>
<td>Email is encrypted on the sender’s desktop or mobile device.</td>
</tr>
<tr>
<td>ON-DEMAND ENCRYPTION</td>
<td>NA</td>
<td>The sender has to rely on DLP rules setup in Office 365 to trigger message encryption.</td>
<td>x</td>
<td>Encryption is not dependent on format or content recognition by DLP or gateway rules. The sender can click on “Send Secure” within Outlook to encrypt the email.</td>
</tr>
<tr>
<td>DATA PRIVACY &amp; CONFIDENTIALITY (EXTERNAL)</td>
<td>NA</td>
<td>Email is encrypted by Office 365, so the cloud provider can see the contents of the email.</td>
<td>x</td>
<td>Email is encrypted before it reaches Office 365, so the cloud service provider cannot see the contents of the email.</td>
</tr>
<tr>
<td>DATA PRIVACY &amp; CONFIDENTIALITY (INTERNAL)</td>
<td>NA</td>
<td>Copies of the email are retained by and are available on the email server.</td>
<td>x</td>
<td>No copies of the email are retained by Voltage SecureMail.</td>
</tr>
<tr>
<td>CONTROL OVER KEY SERVER</td>
<td>NA</td>
<td>Organizations have to rely on Office 365 for key generation.</td>
<td>x</td>
<td>Voltage SecureMail gives organizations control over the key server.</td>
</tr>
</tbody>
</table>

Table3. Voltage SecureMail and Office 365 Message Encryption comparison

Learn More At
www.microfocus.com/securemail