PROOFPOINT FOR OFFICE 365: ENABLES ADVANCED SECURITY AND COMPLIANCE FOR YOUR ENTERPRISE

UNDERSTAND THE SOLUTION BY ROLE: COMPLIANCE

What are the compliance challenges of Microsoft® Office 365™?

Microsoft® Office 365™ Compliance Capabilities
Microsoft® Office 365™ includes multiple capabilities to enable organizations to monitor, enforce and demonstrate compliance with regulatory and internal practices. These include:

- Independent verification of compliance with requirements such as ISO 27001, FISMA, and other U.S. and European Union regulations.
- Predefined policy templates for specific types of sensitive data as defined by a range of regulations, such as PCI-DSS, GLBA, or regional regulations for PII and PHI.
- Customizable DLP policy templates that can be applied to detect sensitive information at multiple places in an email message.
- Policy Tips to inform and educate end users when they are handling sensitive information.

Data loss prevention policies in Office 365 are implemented as packages of transport rules, and can be managed through the Exchange™ Management Shell, the Exchange™ Administration Center, or via an XML editor.

Microsoft® Office 365™ Compliance Challenges Overview
Microsoft® Office 365™ includes a basic set of data privacy tools, but these lack the options and configurability that most organizations are already employing for their on-premise email infrastructure. With a limited number of hard-to-customize predefined data loss prevention (DLP) policies, inconsistent policy enforcement across devices, and incomplete critical capabilities for email encryption, organizations are faced with choosing between the cost savings and other benefits of Office 365 and compromising on the controls needed to achieve their accepted level of risk.

In addition, Microsoft stores Office 365 customer data in a number of different countries based on the location of the customer. Microsoft can move customer data without notice and will not guarantee exactly where a customer’s data will be stored. Microsoft notes that it will not provide notice when customer data is transferred to a new country and that “the requirements of providing the services may mean that some data is moved to or accessed by Microsoft personnel or subcontractors outside the primary storage region.”

What capabilities does Office 365 have for safeguarding data?
Office 365 Data Protection Capabilities
Microsoft has implemented data loss prevention (DLP) in Office 365, Exchange™ Online and Exchange™ 2013 based on Exchange™ Transport Rules. By using Policy Tip notification messages, Outlook® users can be alerted to possible violations of corporate policies when sending email that could contain sensitive or confidential information. Microsoft has provided a number of definitions that can be used in its standard offering, but allows administrators to develop and publish custom definitions as well.

As of today, DLP Policy Tips used with Exchange™ Online can be used with Outlook® 2013, OWA or OWA for Devices. These DLP policies work for emails sent from other clients, but the Policy Tips feature works only with these platforms. Advanced capabilities like file fingerprinting are not available, and Office 365 email encryption capabilities are missing key features, including end user revocation of messages that may have been sent to an unintended recipient.

Office 365 Data Protection Challenges
Some organizations maintain several on-premises and cloud-based messaging, collaboration, or storage platforms, and thus require an archiving and compliance solution that will support all of them. Microsoft’s archiving solutions do not currently support all of the platforms that an organization might have in place, such as GroupWise®, Notes/Domino, Google Apps™, Box or Dropbox, among many others. For example, while Microsoft offers online archiving for Exchange™, it does not do so for SharePoint®, requiring the use of a third party solution for organizations that need to archive their SharePoint content.

For many organizations, this will be an important consideration. Because an eDiscovery effort, for example, can be made more complicated and more expensive if an organization must extract content from multiple archiving systems—such as one for Office 365, one for SharePoint content, or one for files stored in the cloud—having one, corporate-wide archiving solution for all content will speed eDiscovery, litigation holds and other activities, as well as drive down their cost.

Protecting data on mobile devices is an area of particular challenge for Microsoft® Office 365™. BlackBerry® Enterprise Server (BES) is not supported by Microsoft in Office 365, although BlackBerry Business Cloud Services supports Office 365xxi. Despite declining support for BES in some organizations, this is a serious problem for organizations that still have many BlackBerry users.

Moreover, Office 365 will wipe only those mobile devices that are managed using ActiveSync, and Office on Demand, a key feature of Office 365 that permits temporary Office client to be installed on any Windows 7/8 PC, is not supported on the iPad, the most commonly deployed tablet computer in the workplace.

Finally, Office 365 will wipe only ActiveSync devices. This can be a serious limitation for the large number of organizations that still support BlackBerry devices and do not want to do so via ActiveSync. Plus, while all versions of Office 365 support the BlackBerry Internet Service, not all versions support BlackBerry Business Cloud Services. Although BlackBerry supports ActiveSync, there have been some reported problems. An alternative for many organizations will be to deploy BlackBerry Enterprise Services, which
will offer support for not only BlackBerry devices, but also iOS and Android devices, but this will add to the cost of Office 365.

**How does Office 365 meet the requirements for SEC/FINRA?**

**Office 365 SEC/FINRA Capabilities**
Microsoft® Office 365™ uses a framework-based approach to manage compliance-related controls, which enables Microsoft to plan, deliver, operate, and manage a customer’s compliance requirements. Microsoft Online Services undergoes multiple third-party compliance audits annually. Office 365 has been certified with ISO27001, an internationally recognized standard in security practices.

**Office 365 SEC/FINRA Challenges**
Office 365 provides a solid foundation for regulatory compliance, but global financial services organizations face a myriad of unique and specific regulatory challenges, which typically requires the use of third party supervisory tools or archiving solutions. For example, within the requirements of SEC 17a-4, organizations are required to maintain information within immutable storage, which is not a supported architectural element of Office 365. For broker-dealer firms governed by FINRA, supervisory reviews are required of broker communications such as email, instant messaging, and social media. These communications are subject to frequent regulatory audit and Office 365 does not offer the necessary features to meet these requirements.

**How easy is it to add third-party compliance capabilities to Office 365?**

**Extending Office 365 Compliance**
Third-party cloud-based solutions for monitoring and enforcing data privacy are a natural fit for Microsoft Office 365, if they combine flexible integration options with the tools and capabilities that Office 365 lacks.

Some organizations maintain several on-premises and cloud-based messaging, collaboration or storage platforms, and so will require an archiving and compliance solution that will support all of them. Microsoft’s archiving solutions do not currently support all of the platforms that an organization might have in place, such as GroupWise, Notes/Domino, Google Apps, Box or Dropbox, among many others. For example, while Microsoft offers online archiving for Exchange, it does not do so for SharePoint, requiring the use of a third party solution for organizations that need to archive their SharePoint content.

For many organizations, this will be an important consideration. Because an eDiscovery effort, for example, can be made more complicated and more expensive if an organization must extract content from multiple archiving systems – such as one for Office 365, one for SharePoint content or one for files stored in the cloud – having one, corporate-wide archiving solution for all content will speed eDiscovery, litigation holds and other activities, as well as drive down their cost.
Proofpoint & Extending Office 365
Proofpoint solutions for Office 365 make it easy for organizations to continue meeting their compliance and data privacy goals as they move to Office 365, while also realizing the material and operational cost savings that are a key benefit of adopting a cloud-based infrastructure.

Will Office 365 compliance capabilities meet my needs?

Office 365 Compliance Capabilities
Some third-party archiving solutions offer more control and transparency about where customer data resides, which may alleviate decision makers’ concerns. This is particularly true for non-US customers that may not want their data accessed under the PATRIOT Act, by the IRS or by other US government agencies.

Microsoft stores Office 365 customer data in a number of different countries based on the location of the customer. Moreover, Microsoft can move customer data without notice and will not guarantee exactly where a customer’s data will be stored.

Microsoft notes that it will not provide notice when customer data is transferred to a new country and that “the requirements of providing the services may mean that some data is moved to or accessed by Microsoft personnel or subcontractors outside the primary storage region.”

Office 365 Compliance Challenges
Microsoft Office 365 includes a basic set of data privacy tools, but these lack the options and configurability that most organizations are already employing for their on-premise email infrastructure. With a limited number of hard-to-customize predefined DLP policies, inconsistent policy enforcement across devices, and missing critical capabilities for email encryption, organizations are faced with choosing between the cost savings and other benefits of Office 365 and compromising on the controls needed to achieve their accepted level of risk.

How does Office 365 meet the requirements for data retention?

Office 365 Data Retention Challenges
For many organizations, the data retention tools provided by Microsoft® Office 365™ are insufficient to meet their needs. A financial services organization, for example, won’t be able to sufficiently meet FINRA or SEC requirements, as Office 365 doesn’t provide email supervision capabilities. In addition, the data stored in Microsoft’s infrastructure does not benefit from “write once, read many” storage (WORM) which ensures data immutability.

Office 365 also includes no native supervision features that allow monitoring or sampling of communications. This is an important capability for highly regulated firms, such as broker-dealers, that must sample communications per FINRA Regulatory Notice 07-59.