Office 365 & Related
Cloud Solutions

Andrew Lally, Director of Technology
Feb. 19th, 2020
At KTL Solutions, it’s not just about the technology, but rather improving the process. We do more than just implement or upgrade systems. **WE ADD VALUE TO YOUR BUSINESS.**

- KTL Solutions has been building systems since 1999 and have since grown to encompass all technologies such as ERP, CRM, Development, Managed Services, Cloud Services, and Business Intelligence.
- Microsoft Direct CSP
- Microsoft Gold Partner
- Authorized partner for the Commercial, GCC and GCC-H Office 365 Environments
- Authorized NFP, Edu and Government
Agenda

• Mobile Productivity
  • Office 365
  • MS Teams

• Data Security
  • User Identification / Authorization
  • Data Location
  • Data Labeling
Mobile Productivity

Office  |  Travelling  |  Home
SharePoint and OneDrive

• OneDrive
  • Personal files you don’t plan to share
  • Shared files that exist prior to creating a team

• SharePoint
  • When you are working as a team
  • Files that should outlive an employee
  • Corporate intranet or communication sites
  • Supports pages and lists
OneDrive Client

- OneDrive client for iOS, Android, Windows and macOS
- Used to sync both OneDrive and SharePoint libraries to your device
- Integrates with Office applications to support collaborative editing
- Provides a native windows file explorer experience
- Save space with On-Demand file download
  - Only the metadata exists locally to support file browsing
  - File content is downloaded when the file is accessed
Office Apps

• Support for Windows, macOS, iOS and Android
• Edit documents that are synced through OneDrive sync client
• Edit documents directly from OneDrive or SharePoint
X1050 MARKETING COLLATERAL TIMELINES

This is a working reference document for use by the project team to help plan, review, and respond to feedback. There are areas where you can enter changes, annotations, or questions. It is not necessary to use track changes.

Note: Please don’t update local copies of this document. Remember, we can all work in the document at the same time when it’s posted to SharePoint, so there’s no reason to have to work in additional copies.
Exchange Online / Outlook

- Exchange Online provides access to your email from anywhere with an internet connection
- Outlook provides a familiar experience across devices
- Outlook Web Access provides access from any browser
Microsoft Planner
You have late tasks!
Hi Megan, You have a task due in Microsoft Pl...

Microsoft Planner
You have tasks due today!
Hi Megan, You have a task due in Microsoft Pl...

Microsoft Planner
You have upcoming tasks due.
Hi Megan, You have a task due in Microsoft Pl...

Microsoft Azure
Your Azure AD Identity Protection Weekly Dig...
See your report. Your Azure AD Identity Prote...
Microsoft Teams

- Hub for teamwork and communication
- Chat based collaboration
- Schedule and host meetings
  - PSTN conference line available as a per user add-on
- Screen sharing
- Integrations with SharePoint, OneDrive and other 3rd party applications
- Cross platform functionality
  - Android, iOS, Windows, macOS and Web
- Chat is archived through advanced retention policies
Chat Based Communication
Teams & Channels

![Microsoft Teams interface with channels and messages]

**Teams**

- Your teams
- Digital Initiative Public Relations
- General
- Mark 8 Project Team
- General
- Design
- Digital Assets Web
  - Research and Development
  - Sales and Marketing
  - General
  - Monthly Reports
- Retail
  - General
  - NC460 Sales

**Channels**

- **Design**
  - Posts
  - Files
  - Usability Priorities
  - Wiki
  - Excellent meeting, everyone. Please follow up with some of the items that we discussed when they are ready. Thanks😊
  - 4 replies from you, Alex, and Johanna
  - Reply

- **Usability Testing**
  - Hello, we’ve finished our first round of usability testing on the X1050. In general, things went very well. There are a few issues to overcome in the next few weeks prior to launch, but the dev team is moving forward rapidly. Our user testing has also identified some really compelling opportunities for additional features that may be included after launch. You can find more details in the attached documentation.
  - [XT1050 Usability test 2.3.docx]
  - 5 replies from you, Alex, Miriam, and 2 others
  - Reply

- **General**
  - Megan Bowen
  - 12/11/19 7:33 AM
  - Great teamwork

**Help**

- Join or create a team

**Search or type a command**
SharePoint Integration
Inline File Editing

X1050 MARKETING COLLATERAL TIMELINES

This is a working reference document for use by the project team. Please add or reply to comments where you have changes, queries, or action items. Not necessary to use track changes.

Note: Please don't update local copies of this document. Remember, we can all work in the document at the same time when it's posted to SharePoint, so there's no reason to have to work in additional copies.
Calendar Management
Data Security
Prevent data loss through security
Who or What Has Access to The Data?

• Employees
• Partner Organizations
• Service Providers
• Guests
• 3rd Party Applications
Online Identity

• Uniquely identify a person or application to an online identity through some type of challenge
• Commonly done through just a username and password combination
• What level of assurance is provided
Risk of Password Reuse

• 51% of people reported reusing their work password with other services (https://www.yubico.com/2019/01/yubico-releases-the-2019-state-of-password-and-authentication-security-behaviors-report/)

• Group that accessed Mark Zuckerberg’s Twitter and Pintrest accounts claimed the password came from accounts leaked in a previous LinkedIn breach (https://techcrunch.com/2016/06/06/zuckerbergs-twitter-pinterest-linkedin-accounts-hacked/)

• https://haveibeenpwned.com/ is a great resource to check if your account has been included in known data breaches
Phishing Risk

• Users receive legitimate looking emails that contain malicious links
• Links redirect to fake O365 login pages prompting the user to enter their username and password
• Newer attacks redirect users to application consent request for malicious applications
• Freely available frameworks for attackers to download and use
• Can be mitigated using advanced spam filtering & Multi-Factor Authentication
What is o365-attack-toolkit

o365-attack-toolkit allows operators to perform an OAuth phishing attack and later on use the Microsoft Graph API to extract interesting information.

Some of the implemented features are:

- Extraction of keyworded e-mails from Outlook.
- Creation of Outlook Rules.
- Extraction of files from OneDrive/Sharepoint.
- Injection of macros on Word documents.

Architecture
Multi-Factor Authentication (MFA)

• Should be enabled at a minimum for all privileged accounts
• STRONGLY recommended for all accounts
• Should be any two of the following
  • Something you know (password)
  • Something you are (fingerprint, face or other biometric identifier)
  • Something you have (ID Badge, cryptographic key, OTP)
• Increases user identity assurance
Azure MFA

• Included with O365
• Simple self-service provisioning at user logon
• Meets the “something you have” requirement of the MFA process
• Can be enforced for guest users as well
DUO MFA

- Simple self-service provisioning at user logon
- Meets the “something you have” requirement of the MFA process
- Integrates with common VPN providers
- Support for Windows logon process
Delegated Application Access

• Added security by not sharing your credentials
• Fine grained control by limited application access to only what is necessary
• Must approved delegated permissions prior to any additional permissions being granted
Delegated Application Access Risks

- Allows apps to access data on behalf of users
- By default all users can allow apps to access their data on their behalf
- Maintains access after passwords resets
- Easy to make a request seem legitimate
- Strong passwords and MFA do nothing to mitigate this risk
Permissions requested

Contoso Test App
zawad.co

This app would like to:

☑️ Read and write your files
☑️ Read your calendar
☑️ Sign you in and read your profile

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

[Cancel] [Accept]
Reduce the risk of malicious apps

- Use a separate account for admin/escalated functions
- Disable the ability for non-admin users to authorize applications
- Review app permissions and company prior to consenting to their use
- Periodically review the applications that have been authorized
- [https://myapps.microsoft.com](https://myapps.microsoft.com)
Permissions requested

Contoso Test App
zawad.co

This app would like to:

✓ Read and write your files
✓ Read your calendar
✓ Sign you in and read your profile

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

[Cancel] [Accept]

Need admin approval

Contoso Test App
zawad.co

Contoso Test App needs permission to access resources in your organization that only an admin can grant. Please ask an admin to grant permission to this app before you can use it.

Have an admin account? Sign in with that account

Return to the application without granting consent
Beyond MFA

- Atypical travel
  - New locations
  - Impossible travel speeds
- Sign-in properties
- IP Address Reputation
- Threat Intelligence
  - Crowd sourced data analysis to detect known attack patterns
  - Machine learning models to detect anomalies in user access
Where Is The Data?

- Corporate File Servers
- Cloud Storage
  - SharePoint Online, OneDrive, Box, DropBox
- Email Servers
- Devices
  - Corporate devices, Personal devices (BYOD)
Joe receives an email containing documents. He saves and opens them on his local computer to review.
Joe uploads the document to a team site to share
Susan sees the new file and downloads it to her machine to review
Sam sees the document as well but is out of the office. He downloads the file to his phone
Mobile Device Management (MDM)

• Cross platform support (iOS, macOS, Windows, Android)
• Ensure data is secured
• For BYOD segment work data from personal data to ensure they never get mixed
• Ensure only approved applications and devices are used to work with data
• Control the flow of data between work and personal
MDM – Company Policies

- Require PIN/Passcode to unlock the device
- Encrypt device storage
- Block access to public app stores allowing only corporate authorized apps
- Detect and block rooted or vulnerable out of date phones
- Push required work settings (WIFI, VPN, etc.)
- Supports wiping devices to protect data in the event it is lost or stolen
- Automatically configure corporate applications
MDM – Work Profiles

- Allows for securing company data in BYOD friendly way
- Apple and Android both support work segmented and encrypted storage
- Limit data access to approved applications
- Limit the ability to move data in and out of work encrypted storage
- Supports wiping only work data in the event the device is lost, stolen or the employee is terminated
- Require PIN to access work applications
Joe needs to share a file with Steve who works for a different company
How Does This Secure Data Sent To Steve?

- Steve must authenticate prior to being able open the document
- Steve’s access can be revoked no matter where he moves the document
- Your access and permissions stay with the file no matter where it goes
- Steve can’t share the file with any unapproved users
Unified Labeling (Azure AIP)

• Use labels to tag/classify data
• Apply rights management policies based on classification
• Apply document encryption policies based on classification
• Automatically apply document markings
• Revoke user access no matter where the document is at
• Supports Data Loss Prevention efforts
Data Classification Labels

• Applied manually through labels while documents are being edited
• Optionally can be automatically applied or suggested based on detected content in documents.
Apply Labels Directly in Office Apps
Prevent Data Loss

- Use labels to inform users on how to handle documents
  - Headers, Footers, Watermarks, Descriptions
- Use labels to block emails containing sensitive data
- Use labels and data classifications to alert admins and block file sharing
- Use labels to revoke access for documents outside your environment
- Use document encryption to protect documents in 3rd party systems
Contoso Confidential
Testing the General label for the Block message

To: admin@contoso.com

Subject: Testing the General label for the Block message

Microsoft Azure Information Protection

Email Blocked

You are about to send content classified as General to one or more untrusted recipients:
admin@contoso.com

Your organization policy does not allow this action.
Consider removing these recipients, or replace the content.

OK
Testing the General label for the Justify message

Your organization policy requires justification for you to send content classified as General to untrusted recipients.

- I confirm the recipients are approved for sharing this content
- My manager approved sharing of this content
- Other, as explained

[Blank field for justification]

Confirm and Send  Cancel
Classify and protect - Azure Information Protection

Not set

<table>
<thead>
<tr>
<th>Personal</th>
<th>General</th>
<th>Internal</th>
<th>Confidential - Finance</th>
<th>Confidential - PII</th>
<th>Highly Confidential</th>
</tr>
</thead>
</table>

Delete Label

Protect with custom permissions

Select permissions: Viewer - View Only

Select users, groups, or organizations: alaily@ktlsolutions.com

Expire access: 1/10/2020

Apply

Close
Data Integrity and Resiliency

- Microsoft provides data integrity and resiliency through replication
  - Copies of data is stored in no less than two datacenters at a time
- Microsoft does not provide traditional data backup
  - SkyKick
  - Backupify
  - Veeam