softchoice

Securing your University's Cloud Footprint While Getting More from What You Already Own

Microsoft security overview

Agenda

1. Introduction
2. Cool security features – MFA, Conditional Access, Cloud App Security, and Azure ATP
3. MFA Deep Dive
4. Conditional Access Deep Dive
5. Overview of CAS and AATP
6. Cloud success story

Your Presenters

Terence Snijtsheuvel

Solutions Architect

Terence.Snijtsheuvel@softchoice.com

www.linkedin.com/in/tsnijtsheuvel

Trevor Lysyk

Professional Services Architect

Trevor.Lysyk@softchoice.com

www.linkedin.com/in/trevorlysyk

Wade Sellers

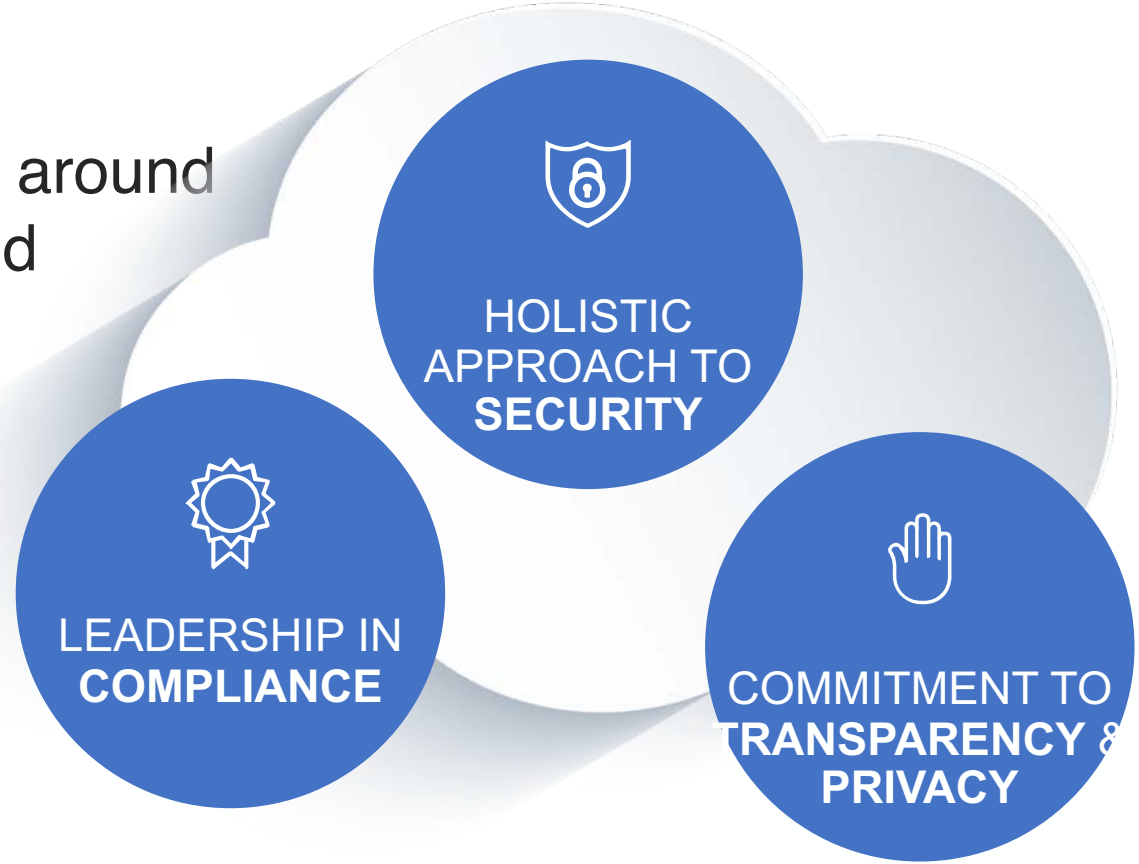
IT manager

wadesellers@capilanou.ca

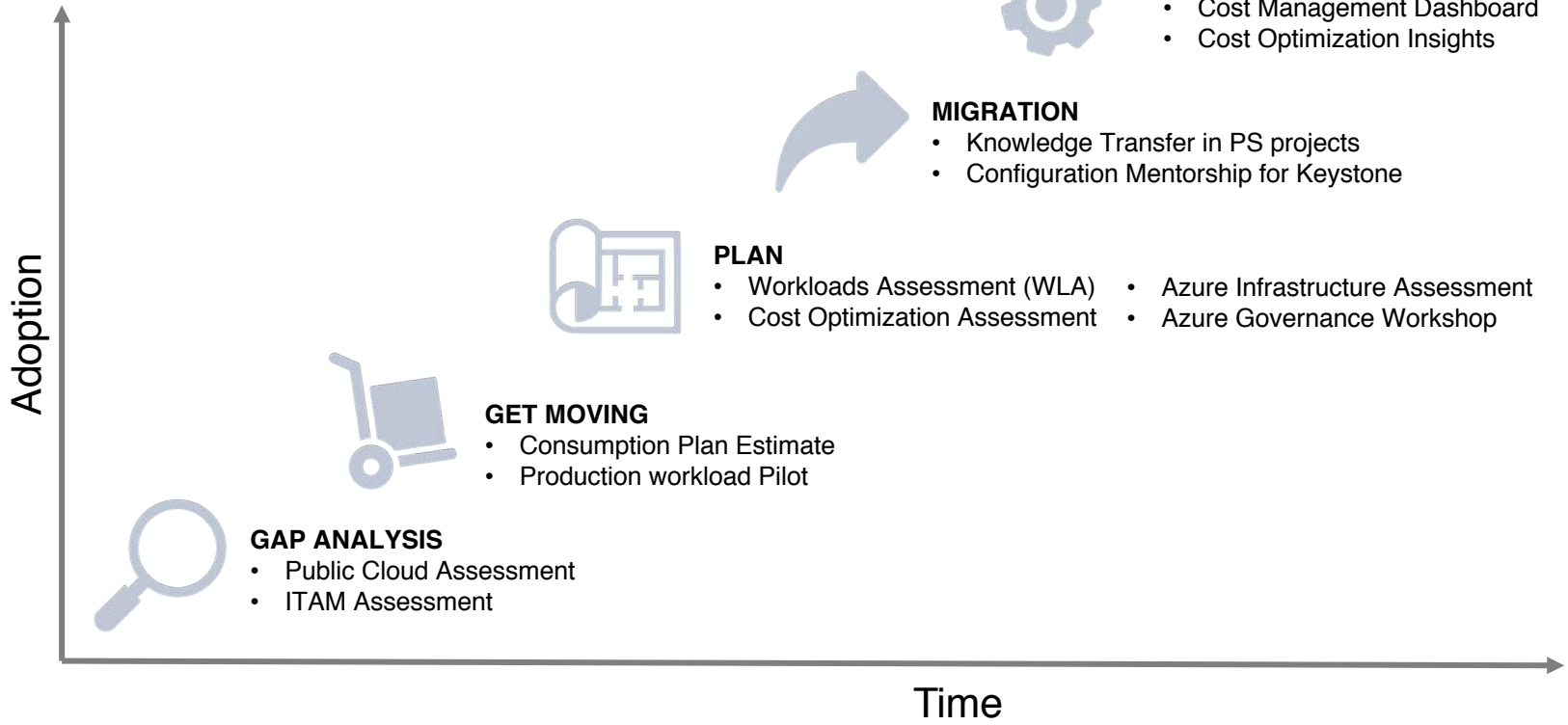
www.linkedin.com/in/wadesellers

Today's Objective

To provide information around 2019 Microsoft updated security capabilities



The Stages Of Adoption



OPTIMIZE
- Keystone Essentials/Complete for Azure
- Cost Management Dashboard
- Cost Optimization Insights

MIGRATION
- Knowledge Transfer in PS projects
- Configuration Mentorship for Keystone

PLAN
- Workloads Assessment (WLA)
- Cost Optimization Assessment
- Azure Infrastructure Assessment
- Azure Governance Workshop

GET MOVING
- Consumption Plan Estimate
- Production workload Pilot

GAP ANALYSIS
- Public Cloud Assessment
- ITAM Assessment

Governance Modeling

Deployment identifier

Why it's there

Business priority

Availability

Deployment	Owner	Purpose	Steward	Priority	Net Benefit	Operations
Active Directory	IT	Security	CIO	Critical	Productivity of end users	24x7
Web Site	Marketing	Public information and branding	CFO	Critical	Demand Generation	24x7
CRM	Sales	Manage our Customers	Sales VP	Normal	Client Relationships	9x5

...

Who pays the bill

Who makes decisions

Business value

What is the **Number 1** culprit in security failures in most organizations?

softchoice

Windows XP box that was forgotten about?

Server room being left pried open?

That TCP/3389 external firewall rule that is still enabled?

softchoice

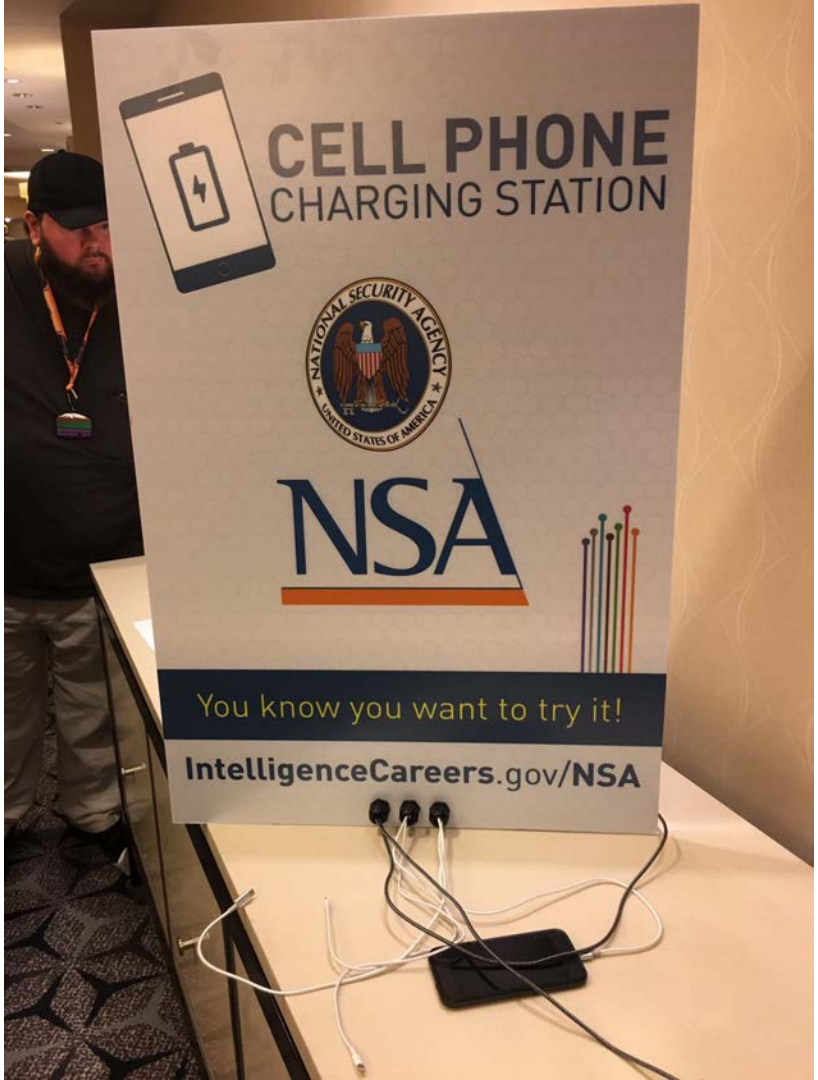
Ok if you guessed

TCP/3389 external firewall rule that is still enabled
(Remote Desktop open to the internet)

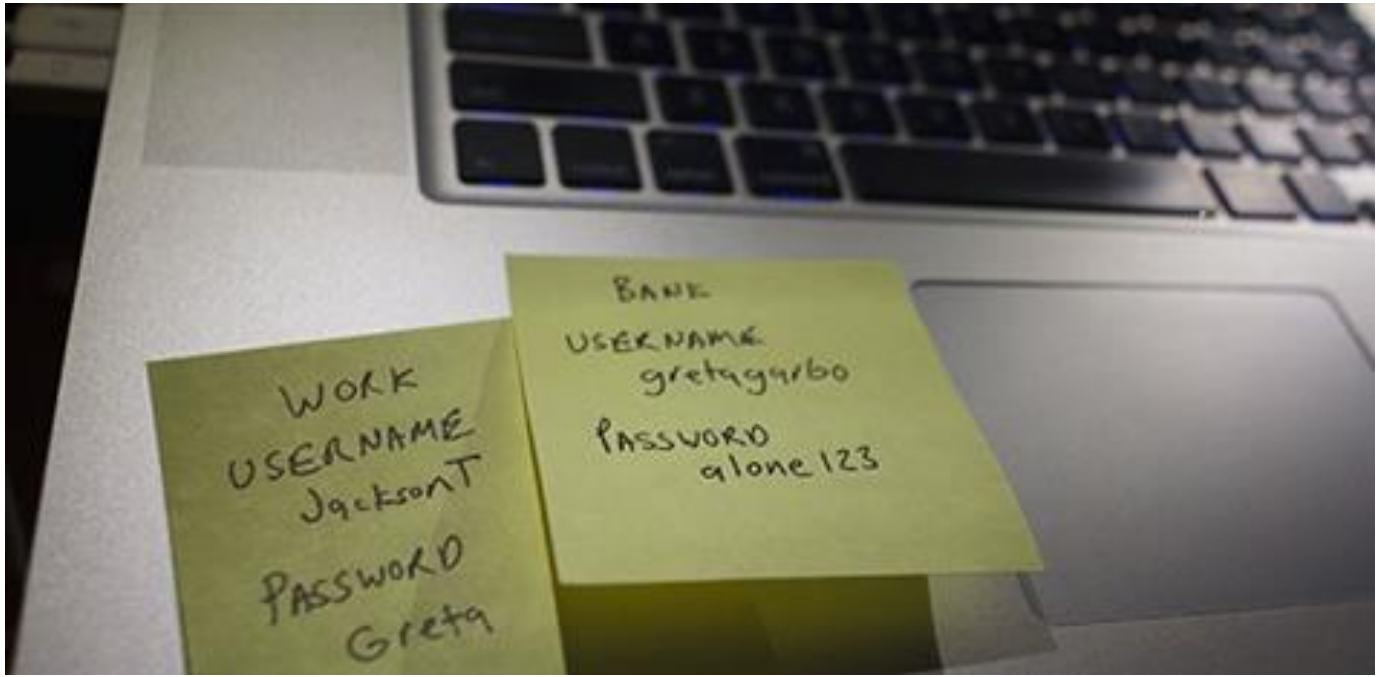
Good guess but not quite*

**Try this on an Azure virtual machine, you will within an hour get brute forced with hundreds of thousands of login attempts an hour!*

softchoice


CELL PHONE
CHARGING STATION
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
NSA
You know you want to try it!
IntelligenceCareers.gov/NSA

softchoice


WORK
USERNAME
JacksonT
PASSWORD
Greta
BANK
USERNAME
gretagarbo
PASSWORD
alone123

softchoice

If you guessed poor user practices – you would be correct

Phishing, social engineering, poor passwords, passwords stuck under keyboards…

softchoice

Now – what if you could enable features you likely already own in the cloud

So, if your users do many of the terrible things, they will still do no matter how many times IT sends out those phishing email tests and alike

You just don’t have to care, or worry (as much anyway)

As their terrible password is far from the last line of defence

And bonus! You are paying for these features already

You just have to turn them on ☺

softchoice

What all do you already own?

Lot's of services to maintain and secure…

Microsoft 365 A3 vs. Microsoft 365 A5

Microsoft 365 A3

Office 365 A3
w/ rights to Office Professional Plus

- Advanced Security Management
- Skype Meeting Broadcast
- Bookings (*Coming soon*)

+

Windows 10 Enterprise A3

+

EMS A3

- Azure Active Directory Premium P1
- Azure Information Protection P1
- Intune for Education
- Advanced Threat Analytics

+

Minecraft: Education Edition

- Minecraft: Education Edition

+

Windows CALs
Productivity CALs

- All customers get Enterprise CALs

Productivity Server Licenses

- Includes Productivity Server Licenses

Microsoft 365 A5

Office 365 A5
w/ rights to Office Professional Plus

- Advanced Security Management
- Skype Meeting Broadcast
- Bookings (*Coming soon*)
- ***Advanced Threat Protection***
- ***Threat Intelligence Dashboard***
- ***Advanced eDiscovery***
- ***PowerBI Pro***
- ***Cloud PBX***
- ***PSTN Conferencing***

+

Windows 10 Enterprise A5

- ***Windows Defender ATP***

+

EMS A5

- ***Azure Active Directory Premium P2***
- ***Azure Information Protection P2***
- ***Cloud App Security***
- Intune for Education
- Advanced Threat Analytics

+

Minecraft: Education Edition

- Minecraft: Education Edition

+

Windows CALs
Productivity CALs

- All customers get Enterprise CALs

Productivity Server Licenses

- Includes Productivity Server Licenses

Security Features of Interest

Good news! You own all of the pieces to do just that!

Microsoft 365 A3 vs. Microsoft 365 A5

Microsoft 365 A3		Microsoft 365 A5	
Office 365 A3 *w/ rights to Office Professional Plus*	• Advanced Security Management • Skype Meeting Broadcast • Bookings (*Coming soon*)	**Office 365 A5** *w/ rights to Office Professional Plus*	• Advanced Security Management • Skype Meeting Broadcast • Bookings (*Coming soon*) • ***Advanced Threat Protection*** • ***Threat Intelligence Dashboard*** • ***Advanced eDiscovery*** • ***PowerBI Pro*** • ***Cloud PBX*** • ***PSTN Conferencing***
+		+	
Windows 10 Enterprise A3		**Windows 10 Enterprise A5**	
+		+	
EMS A3	• Azure Active Directory Premium P1 • Azure Information Protection P1 • Intune for Education • Advanced Threat Analytics	**EMS A5**	• ***Windows Defender ATP*** • ***Azure Active Directory Premium P2*** • ***Azure Information Protection P2*** • ***Cloud App Security*** • Intune for Education • Advanced Threat Analytics
+		+	
Minecraft: Education Edition	• Minecraft: Education Edition	**Minecraft: Education Edition**	• Minecraft: Education Edition
+		+	
Windows CALs	• All customers get Enterprise CALs	**Windows CALs**	• All customers get Enterprise CALs
Productivity CALs		**Productivity CALs**	
Productivity Server Licenses	• Includes Productivity Server Licenses	**Productivity Server Licenses**	• Includes Productivity Server Licenses

softchoice

Multi-Factor Authentication

Multi-Factor Authentication

- Think of when you call a bank
  - Do you just give your name and account number and get access to your money?
- Same ideology for accessing Office 365
  - A push notification to your phone or smart watch
  - Text message
  - Phone call
  - Token

To get MFA going for Office 365

1. Enable Modern Authentication in Office 365
   - Two PowerShell commands
2. Install the Microsoft Authenticator on your device
   - iOS and Android support
3. Enable MFA on your user account
4. Log in as the user, and enroll your device
5. MFA is now setup for this account!

What works and doesn't with MFA?

- Office 2013 SP1 or newer (16/19)
  - Office 2010 does not support Modern Auth
- MFA works natively with:
  - Outlook App (iOS and Android)
  - iOS Mail App (iOS 11 and higher)
- MFA does not work with:
  - Android Mail App (all brands)

softchoice

But with any good thing…

- Comes the problem – Personal devices
  - For this to work a mobile device is generally required
  - Employee's can refuse to use their personal device for this purpose, and it cannot be forced on them
  - Device subsidies or corporate owned devices defeat the savings
  - Tokens can be used – also not a perfect solution
    - Easily lost, poor user experience, and not cheap in their own right

- Can an organization have secure access to the cloud without MFA?
  - Yes, yes you can!

softchoice

softchoice

Conditional Access

Requirements for Conditional Access

- Domain and Forest FL at 2012 or higher
- AADC configured for Hybrid AD Join
  or
- Intune agent installed on each device
- Works for both Federated (ADFS) and Managed Tenants
- Computer Objects sync'd into the cloud
- Windows 10 1703 and greater is *preferred*

How to setup Conditional Access?

1. Create a new Conditional Access Rule
2. Select the cloud services you want to protect
3. Select what type of devices the rule is being enforced against (i.e. Desktops or Mobile devices)
4. Select the users or groups in scope for the rule
5. Select the condition for access (i.e. Hybrid AD Joined Computer or Intune Compliant)
6. Enable the rule
7. **You are now protected!**

softchoice

So – that’s it?

A user never knows?

softchoice

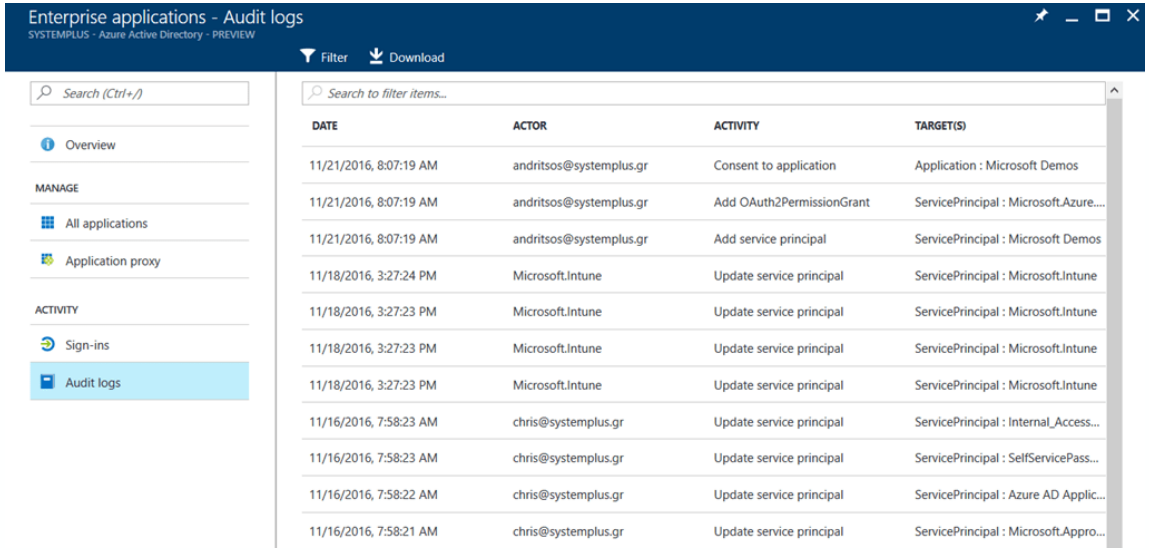
Well Almost - Notes on Conditional Access

- Supports Internet Explorer and Edge Natively
- Chrome is supported with the Microsoft Account extension
- Firefox, Opera, Safari etc – not supported
- Intune agent conflicts with SCCM agent
  - Thus why Hybrid AD Join is the preferred method

softchoice

How do you know something is wrong?

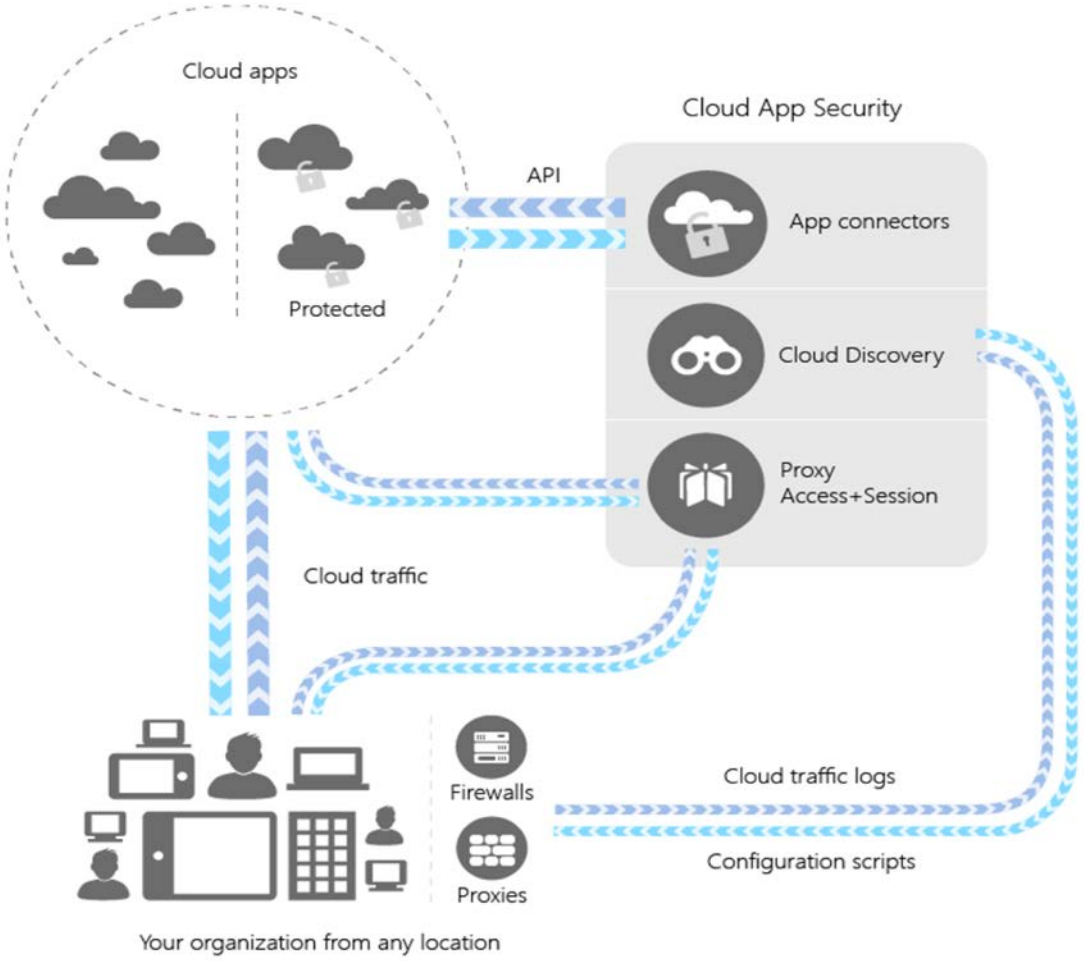
- Have you ever looked at your sign-in or audit logs?



softchoice

Too much noise!

- Thousands and thousands of entries
  - How can you get it down to problems or issues?
- A5 license holders are in luck!
  - Cloud App Security parses your logs and *for the most part* helps you see through the noise
  - Some assembly is required of course


Cloud apps
Protected
API
Cloud App Security
App connectors
Cloud Discovery
Proxy
Access+Session
Cloud traffic
Firewalls
Proxies
Cloud traffic logs
Configuration scripts
Your organization from any location

softchoice

How to deploy Cloud App Security

- Enable Cloud App Security
- Enable Azure Information Protection
  - This is required for using CAS policies for data retention
- Connect Cloud App Security to cloud apps
  - Office 365, Azure, AWS, Dropbox, Box, G-Suite, Okta, Salesforce, and ServiceNow are supported
- Upload Firewall traffic logs for analysis

Cloud App Security

Files

QUERIES: Select a query...
APP: Select apps...
OWNER: Select users...
ACCESS LEVEL: Select access level...
FILE TYPE: Select type...
MATCHED POLICY: Select policy...
Save as | Advanced

1 - 20 of 1,000+ files

New policy from search

File name	Owner	App	Collaborators	Policies	Last modified
European customer data.docx	Patrick Cottle	Box - US		1 policy match	Mar 28, 2019
Invoices from Partners	Patrick Cottle	Box - US		—	Mar 28, 2019
Project Titanium	Admin	Box - US		—	Mar 28, 2019
Plates	Adeline Cruz	Microsoft SharePoint ...	3 collaborators	1 policy match	Mar 27, 2019
Test	Adeline Cruz	Microsoft OneDrive fo...		—	Mar 27, 2019
Documents	Adeline Cruz	Microsoft OneDrive fo...	5 collaborators	—	Mar 27, 2019
Employee_SSN.txt	Frederick Hoag	Microsoft OneDrive fo...	1 collaborator	—	Mar 27, 2019
Customer data	Frederick Hoag	Microsoft OneDrive fo...	1 collaborator	—	Mar 27, 2019
European customer data.d...	Frederick Hoag	Box - US		1 policy match	Mar 15, 2019

Path: —

URL: https://app.box.com/files/0/f/0/1/f_422357869679

Azure Advanced Threat Protection (ATP)

- Protect on-prem Active Directory
  - Understand when a threat has occurred inside your network

1. Active the Azure ATP Tenant
2. Install the agent on ALL domain controllers
3. Setup sensor options
4. Hope you don’t get any alerts like these…

Azure Advanced Threat Protection | contoso-corp | Timeline
PREVIEW

Microsoft

4:04 PM Today

Honeytoken activity Updated

OPEN

The following activities were performed by Bob Minion:

- Logged in to 2 computers via Contoso-DC.
- Authenticated from 2 computers using Kerberos when accessing 5 resources against Contoso-DC.
- Authenticated from ITARGOET-T470S using NTLM against corporate resources via Contoso-DC.

Started at 3:08 PM Jan 22, 2018

3:23 PM Jan 22, 2018

Remote execution attempt detected

OPEN

The following remote execution attempts were performed on Contoso-DC from ALICE-DESKTOP:

- Attempted remote execution of one or more WMI methods by AdminUser.

3:06 PM Jan 22, 2018

Suspicious service creation

OPEN

AdminUser created 10 services in order to execute potentially malicious commands on Contoso-DC.

3:03 PM Jan 22, 2018

Brute force attack using LDAP simple bind

OPEN

200 password guess attempts were made on 2 accounts from ALICE-DESKTOP. 2 account passwords were successfully guessed.

2:59 PM Jan 22, 2018

Reconnaissance using account enumeration

OPEN

Suspicious account enumeration activity using Kerberos protocol, originating from ALICE-DESKTOP, was detected. The attacker performed a total of 101 guess attempts for account names. 2 guess attempts matched existing account names in Active Directory.

12:38 PM Jan 21, 2018

Malicious replication of directory services

OPEN

Malicious replication requests were attempted by Alice Liddel, from ALICE-DESKTOP against Contoso-DC.

11:59 AM Jan 21, 2018

Reconnaissance using DNS

OPEN

Suspicious DNS activity was observed, originating from ALICE-DESKTOP (which is not a DNS server) against Contoso-DC.

softchoice

Questions?

softchoice

Thank you for time!

softchoice