Tracking changes in Hybrid Identity environments with both Active Directory and Azure Active Directory

Presenters:

**Sander Berkouwer**  
Senior Consultant at SCCT  
10-fold Microsoft MVP  
Active Directory aficionado

**Russell McDermott**  
Systems Engineer  
Netwrix
Agenda

• Introduction to Hybrid Identity
  – Active Directory and Azure AD
  – What is involved with Hybrid Identity?

• Why you need monitoring
  – Active Directory is the cornerstone
  – Azure AD is all the hype
    • But... it’s a service

• What does Netwrix offer?
AN INTRODUCTION TO HYBRID IDENTITY

How Active Directory and Azure AD can work together to bring you the magic of Single Sign On on any device, anytime from anywhere
Hybrid Identity

• Expanding Active Directory Domain Services into the cloud
  – Active Directory has been your Single Sign-On (SSO) solution for years
  – Active Directory uses legacy protocols like Kerberos and NTLM

• Azure Active Directory is Microsoft’s cloud-based identity solution
  – Azure AD is Microsoft’s Identity Management as a Service solution
    • Offering Single Sign-On (SSO) to over 2800 apps
    – Azure AD only offers open interconnection standards
      • Like WS-Federation, SAML, OAuth2, OpenID Connect
    – Azure AD is for not just for admins
Benefits of Hybrid Identity

• One identity to rule them all
  – Single Sign-On (SSO)
    • Both on-premises and in the cloud
    • Leveraging Active Directory Federation Services (AD FS)
  – Same Sign-On (SSO)
    • Two identities, appearing as one

• Easy Multi-Factor Authentication

• Easy collaboration with partners without AD Trusts
  – Relying Party Trusts (RPTs) are scalable, flexible and secure
How to setup Hybrid Identity

• First you need to identify your organization
  – There are 13million organizations with +1B users in Azure AD

• Then, you need to specify your domain name and other info
  – Create a TXT or MX DNS record temporarily

• Then, specify a sign-in method
  – Active Directory Federation Services
  – Password Hash Sync
  – Pas-through Authentication

• Then, you’ll need to synchronize your users
  – Between 3 mandatory attributes and 151 standard attributes synced
Tools to setup Hybrid Identity

• For synchronization
  – Azure AD Connect
  – Forefront Identity Manager
  – Microsoft Identity Manager
  – 3rd party solutions

• For federation (optional)
  – AD FS
  – Ping Federate

#### Pie Chart

- Azure AD Connect: 100%
- Deprecated Microsoft Sync Tools: 7.6%
- FIM / MIM: 1.9%
- Other: 0.0%
Risks of Hybrid Identity

• Oversight and negligence
  – Lingering (privileged) accounts
  – Complex issuing and revocation of privileges
  – Complex issuing and revocation of access
  – Expiring certificates and other certificate trust issues

• Attacks
  – Undetected token deflection attacks
  – Leaked on-premises credentials, reused in the cloud
  – DoS attacks using your publicly available federation endpoints
  – MiTM attacks leveraging downgraded encryption algorithms
  – Vulnerabilities in web standards, leveraged by attackers

• Fines
  – For not meeting regulations like GDPR with breaches of PII data as a result
Common risk mitigation strategies

• Every piece of access is governed by group memberships
  – Azure AD as slave to Active Directory
    • Risk of token bloat
    • Not taking advantage of attribute-based functionality
      – Dynamic group memberships for licensing
      – Dynamic group memberships for applications
      – Etc.

• AD FS solutions not published to the Internet
  – Office 365 unusable on iPads and other portable devices outside the office
  – Not a recommended practice from Microsoft because of MEX
WE NEED PROPER MONITORING

There are two types of organizations; Those that have been hacked, and those that don’t yet know they’ve been hacked.
Monitoring of Active Directory

• Active Directory is the cornerstone of almost every infrastructure
  – Active Directory has been around for two decades (NT5 Beta)

• Domain Controllers are Castles of Identity
  – Some organizations still run them as physical hosts

• Auditing is alive and well
  – Many solutions to choose from
  – Solutions like Netwrix, SPLUNK, ArcSight and STEALTHAudit.
  – Solutions like Microsoft’s own Advanced Threat Analytics
Monitoring of Azure Active Directory

- Azure AD is all the hype!
  - Office 365 uses Azure AD as its identity platform
  - Azure AD allows for Single Sign-On (SSO) access
    - to 2800+ readily integratable apps
    - to your own apps using Azure App Proxy

- Some organizations are cloud-only.
  - A minority today, but increasing fast!

- But ... Azure AD is a service
  - Microsoft runs it and takes care of auditing
  - Auditing is exposed through the Graph API for a maximum of 180 days
  - Not every vendor has a solution out there today...
Monitoring Hybrid Identity

- Monitoring both Active Directory and Azure Active Directory
  - One Single Pane of Glass
  - Up to date Enterprise Overview

- Reporting
  - On privilege use
  - On anomalies and vulnerabilities across Hybrid Identity
  - On objects being migrated, managed, extended without blind spots

- Notifications

- Machine Learning (ML)
What Microsoft offers

• Azure AD Connect Health
  – Monitors Azure AD Connect, AD FS and AD DS
  – Reports on outages
  – Part of Azure AD Premium
  – Initially designed to aid admins in restoring the functionality of Azure AD Connect, as its architecture makes it a single point of failure

• Advanced Threat Analytics
  – Monitors Active Directory Domain Services
  – Initially designed to detect anomalies like golden ticket attacks in Enterprise Active Directory environments
  – Part of Microsoft EMS E5
WHAT DOES NETWRIX OFFER?

A Single Pane of Glass to monitor, analyze and report on both Active Directory and Azure AD.
Netwrix Auditor
Demonstration
Netwrix Auditor Applications

- Netwrix Auditor for Active Directory
- Netwrix Auditor for Azure AD
- Netwrix Auditor for Exchange
- Netwrix Auditor for Office 365
- Netwrix Auditor for Windows File Servers
- Netwrix Auditor for EMC
- Netwrix Auditor for NetApp
- Netwrix Auditor for SharePoint
- Netwrix Auditor for Oracle Database
- Netwrix Auditor for SQL Server
- Netwrix Auditor for Windows Server
- Netwrix Auditor for VMware
Netwrix Customers

Financial

ING, CREDIT SUISSE, fiserv, Allianz, Amica, Berkshire Hathaway Inc., KPMG, John Hancock, Z, FXCM, L, Standard Chartered, BARINGS, UNITED BANK

Healthcare & Pharmaceutical

MAGNACARE, VERTEX, Blue Cross of Idaho, Massachusetts General Hospital, WebMD, American Medical Association, R1, Dignity Health, Yale-New Haven Hospital, Mallinckrodt Pharmaceuticals, VALEANT

Federal, State, Local, Government

U.S. DOT, MAINE, Columbia University, West Point, BNA, University of Cambridge, NASA, NASA, NASA

Industrial/Technology/Other

Crevos, HYUNDAI, CISCO, IBM, L'ORÉAL, CGI, NBC Universal, THOMSON REUTERS, HP, YP, IGATE, PCC, HOUSTON AIRPORT SYSTEM

HITACHI, BLACK & DECKER, PEPSICO, PETROBRAS, Whirlpool, UNITED NATIONS, Verizon, NALGONDE SHAH, Flowers Foods, Bell, Virgin Atlantic
Industry Awards and Recognition

All awards: www.netwrix.com/awards
Concluding

Hybrid Identity
  Active Directory Domain Services
  Azure Active Directory
  Azure AD Connect

Monitoring
  Solutions from Microsoft
    Azure AD Connect Health
    Advanced Threat Analytics
  Netwrix Auditor 9.5
Next Steps

**Free Trial**: setup in your own test environment:
- On-premises: [netwrix.com/freetrial](http://netwrix.com/freetrial)
- Virtual: [netwrix.com/go/appliance](http://netwrix.com/go/appliance)
- Cloud: [netwrix.com/go/cloud](http://netwrix.com/go/cloud)

**Test Drive**: run a virtual POC in a Netwrix-hosted test lab [netwrix.com/testdrive](http://netwrix.com/testdrive)

**Webinars**: join our upcoming webinars and watch the recorded sessions [netwrix.com/webinars](http://netwrix.com/webinars)
Thank You!

Presenters:

**Sander Berkouwer**  
Senior Consultant at SCCT  
10-fold Microsoft MVP  
Active Directory aficionado

**Russell McDermott**  
Systems Engineer  
Netwrix