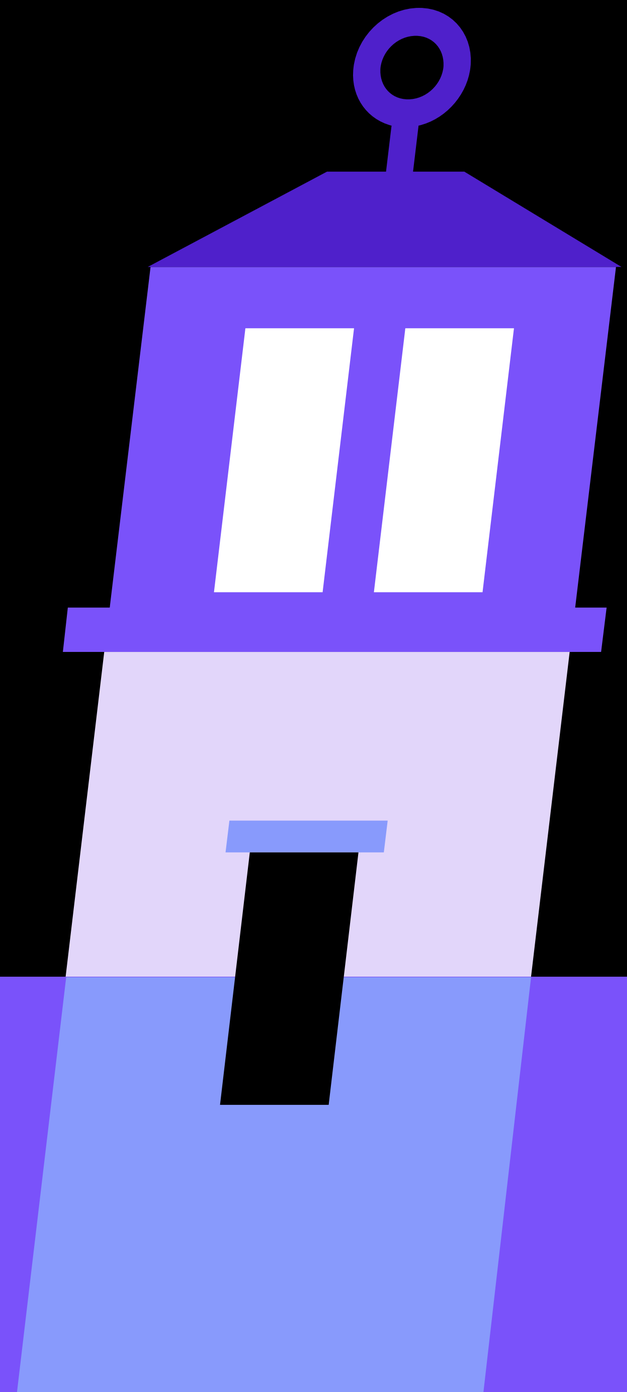
HYBRID
IDENTITY
PROTECTION

conf25

CHARLESTON



Active Directory Roadmap

Linda Taylor
Principal Software Engineer

Cliff Fisher
Senior Program Manager

Microsoft

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Linda Taylor

Microsoft

Principal Software Engineer

24 years in Active Directory @ Microsoft

Worked with AD since Windows 2000 (including NT 4.0)

Oxford Brookes University intern ->

CSS Support Engineer (EE) ->

Software Engineer

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Cliff Fisher

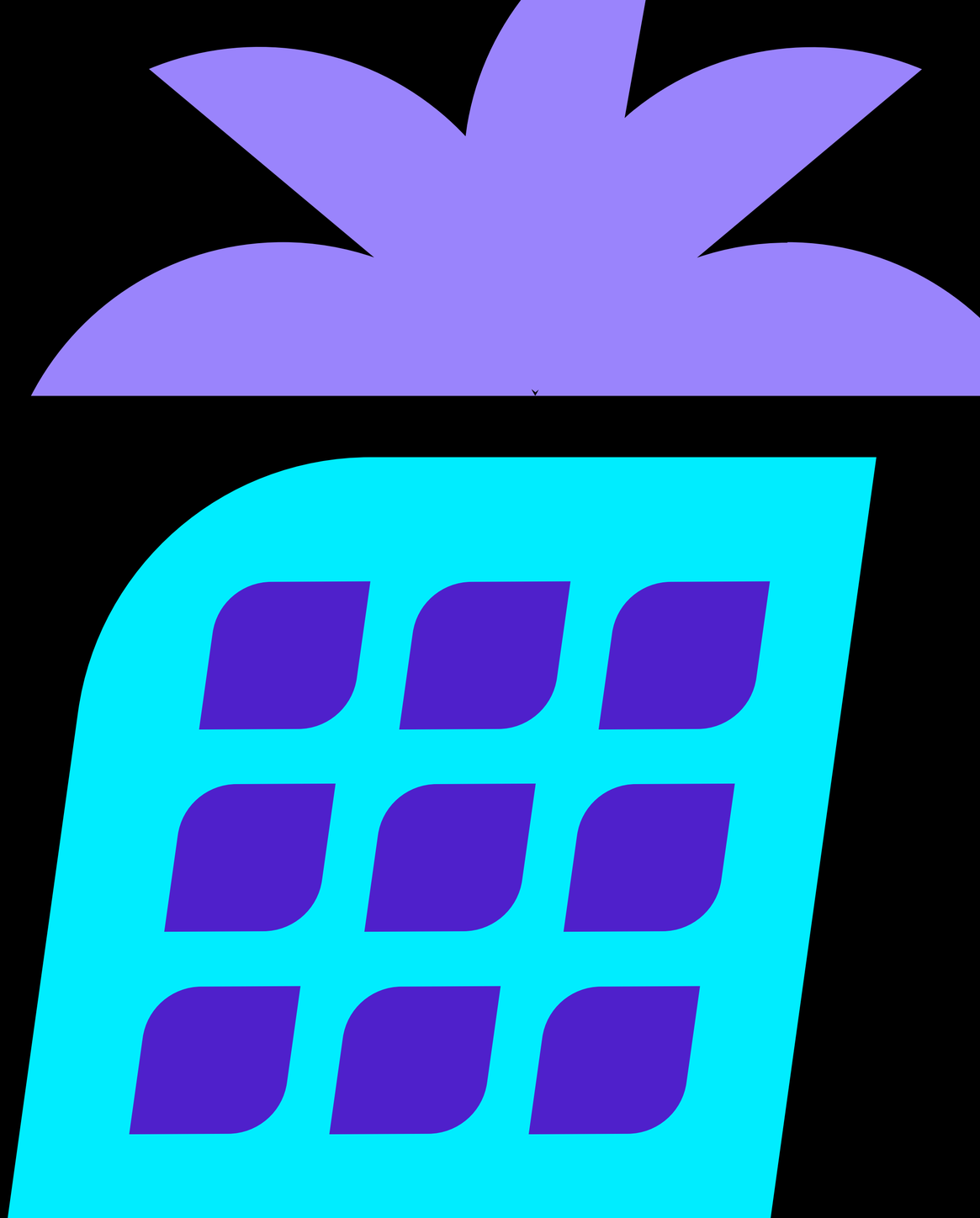
Microsoft

Senior Technical Program Manager

Nearly 20 years' experience with Active Directory administration, support, escalations, debugging, and TPM for Fortune 500 companies in the healthcare, travel, and banking industries

Agenda

- Today’s Active Directory Landscape
- What’s New? What's Next?
- How you can help!

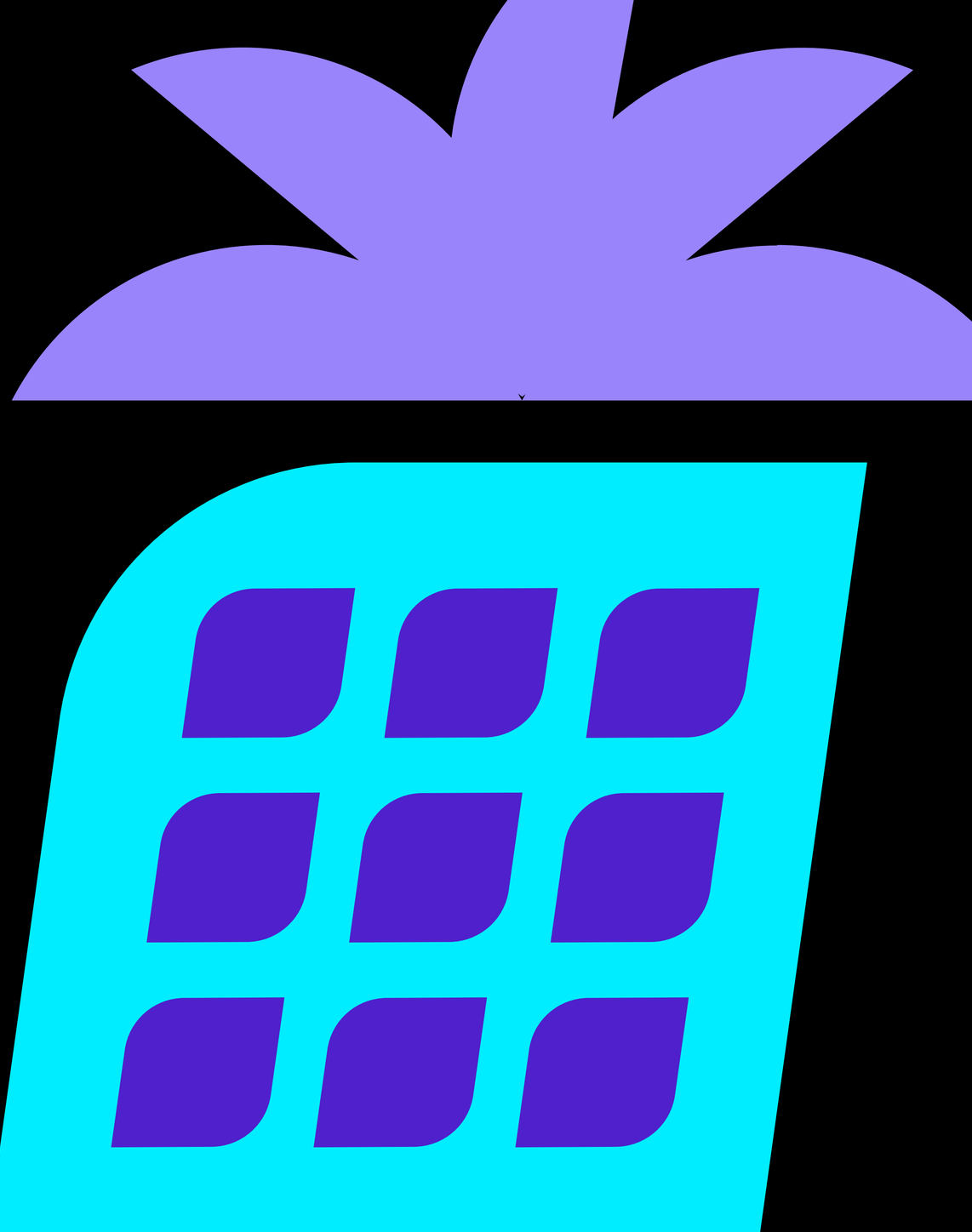


HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Agenda

Today’s Active Directory Landscape

- AD Security Trends
- Patch Tuesday Insights
- Issue Evolution
- Our Priorities & Community Poll Insights



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

25 Years of Active Directory

Origins

Directory service roots at 3Com, later transferred to Microsoft. Integration attempts with LAN Manager and Cairo project

Launch

Official launch with Windows 2000 Server, introducing centralized identity management

Hybrid Identity Is Born

Emergence of Azure AD for hybrid and cloud-native identity management

Windows Server 2025

Investments in security, scalability, and cloud enablement

1980's-1995 | 1996 | 2000 | 2003-2012 | 2014 | 2016 -2022 | 2024+

Exchange 4.0

Exchange Directory Service team lays foundation for Active Directory

Growth & Maturity

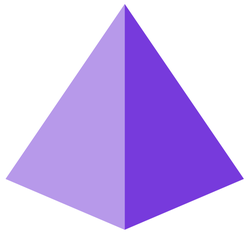
AD becomes enterprise identity backbone with Group Policy Objects (GPOs); introduction of AD Recycle Bin, Fine-Grained Password Policies, Dynamic Access Control, ADFS

Security Focus

Focus on security, sustained engineering

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Active Directory Today?



*“Microsoft is **committed** to keeping **Active Directory** **protected** and **productive** in modern enterprise environments by investing in its **security** and **supportability** while also supporting our customers' transitions to **cloud-based** identity solutions.”*

Active Directory Technologies

AD Mgmt Tools

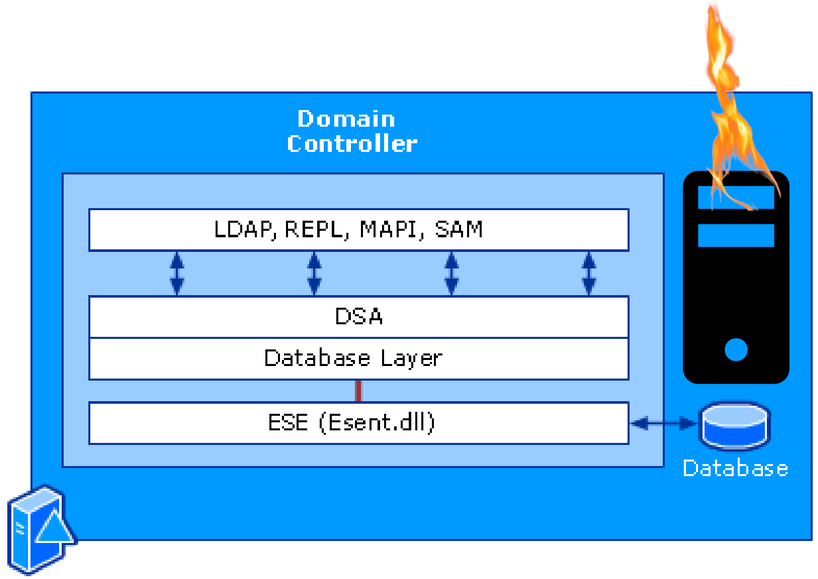
DC Locator

Domain Join

LAPS

AD CS

AD FS



Authentication

Crypto

Access Control

LSASS stuff

DFSR

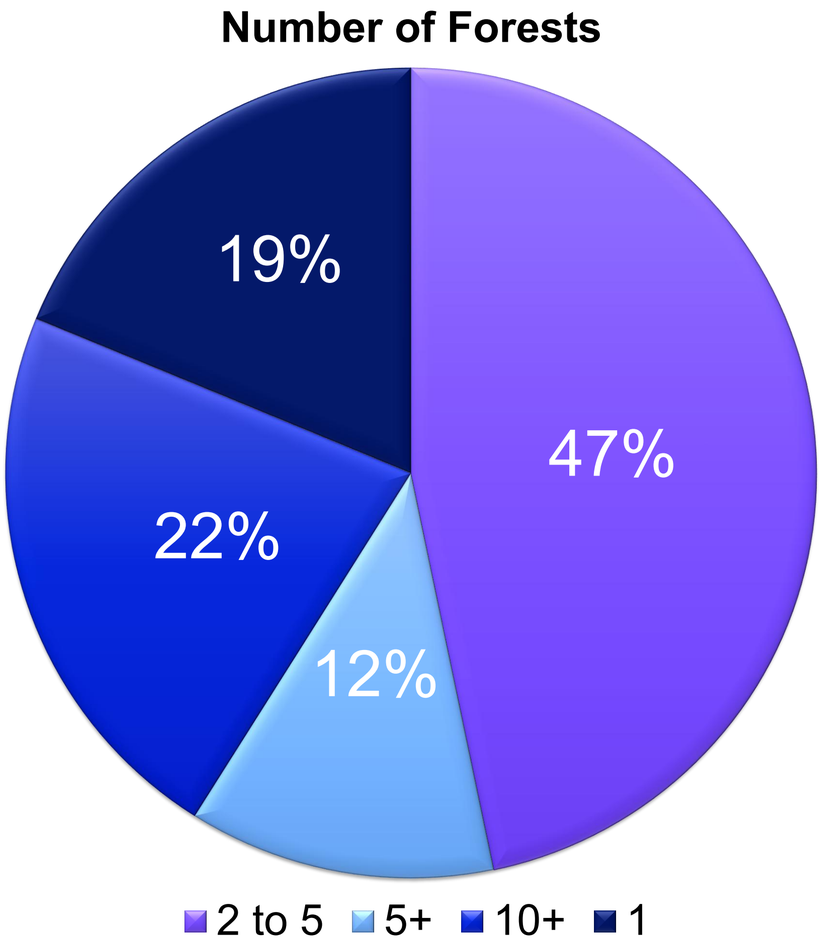
DNS

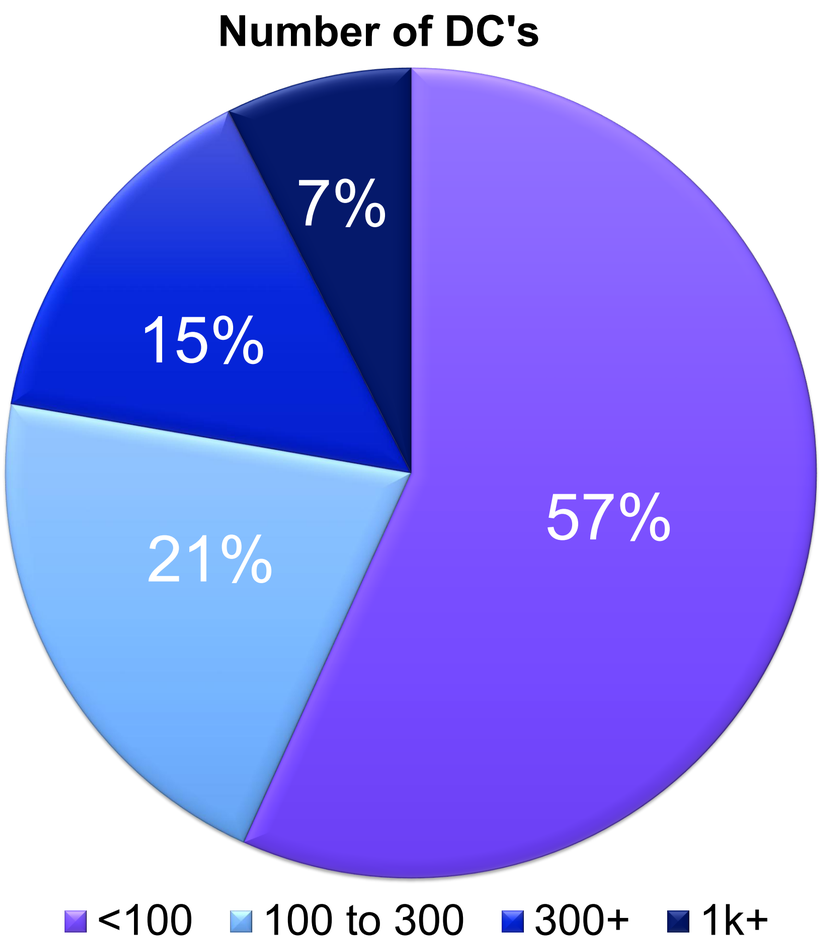
Group Policy

User profiles

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

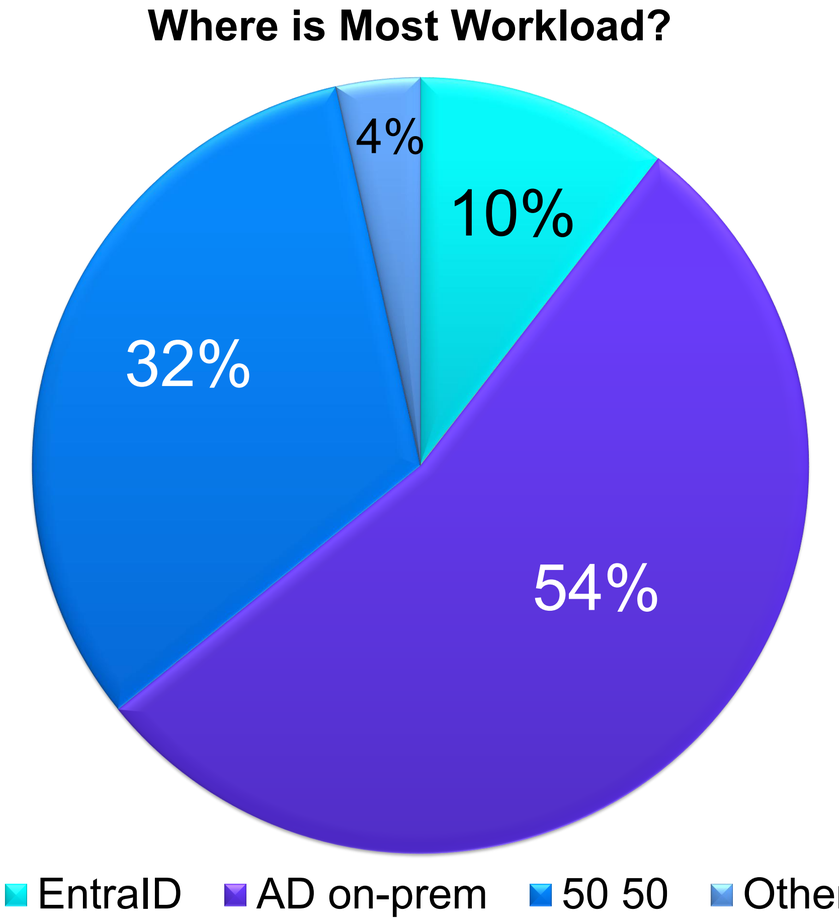
AD Poll: Deployment Diversity

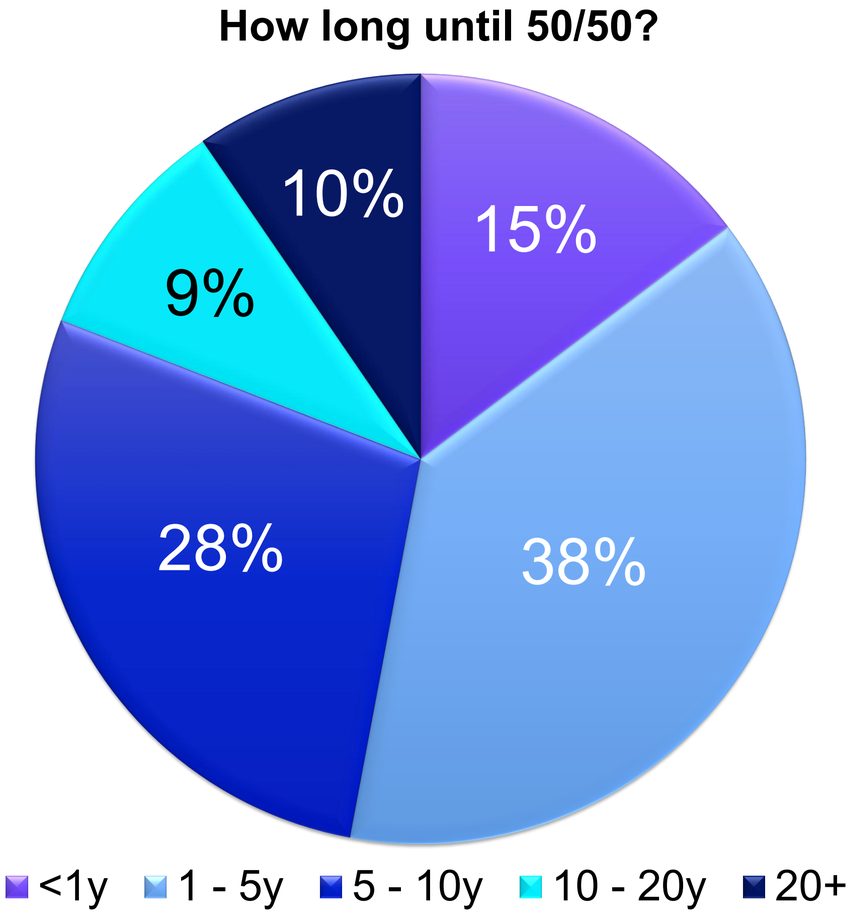




https://www.linkedin.com/pulse/active-directory-community-poll-results-linda-taylor-g23ke

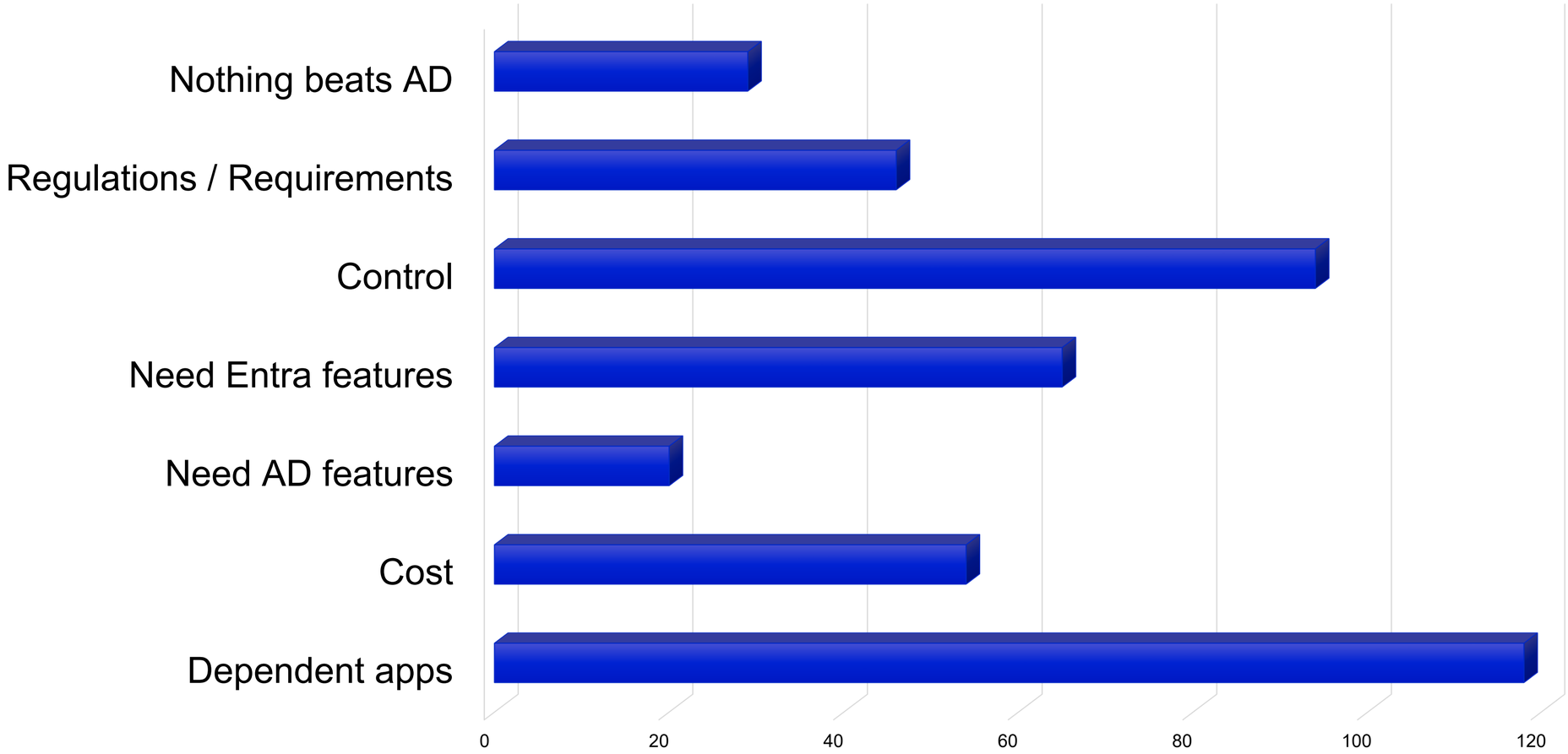
AD Poll: AD Landscape





https://www.linkedin.com/pulse/active-directory-community-poll-results-linda-taylor-g23ke

AD Poll: Cloud Migration Blockers



https://www.linkedin.com/pulse/active-directory-community-poll-results-linda-taylor-g23ke

Where Does Our Work Come From?

Security Vulnerabilities

Customer Requests

Partner Requests

Watson / Telemetry Bugs

Feedback Hub

The Randomizer

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

What Are Our Priorities?

Fix Security Issues

Fix Customer Issues

Don’t Create More Issues

AD By the Numbers

(2024-present)

Incoming MSRC Cases

Evaluated

190+

Fixed in at least one OS version

180+

Total security updates shipped

1200+

Non-Security Work

Bugs Squished

410+

DCRs Shipped

10+

Security

Supportability

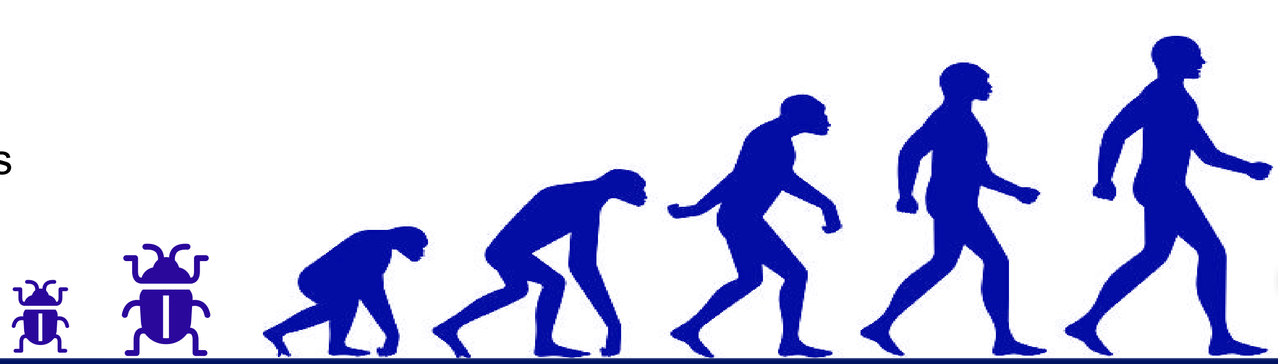
Cloud Growth

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Evolution of AD Security Vulnerabilities

Early AD Vulnerabilities

Null dereference bugs
Low impact fix
Low quantity



Modern AD Vulnerabilities

Complex
Design changes
High impact fix
High friction

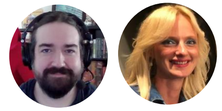
2000

2025

Security Evolves

More complex bugs
Increased quantity
MSRC bug bar evolved

Case study – Domain Join Hardening



Vulnerability reported

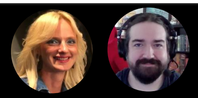
2022

Issue 1 reported

- Account pre-staging + reuse is popular
- Accounts other than DA need to be exempt

Issue 2 reported

- Smart Card Domain joins fail to reuse accounts with GPO



Oct 2022 | Nov 2022 | Mar 2023 | July 2023 | Sept 2023 | Aug 2024

Evaluate

- Investigate
- Design
- Implement
- Test
- Document

CVE-2022-38042 ships

- Vulnerability fixed using client-side logic
- Emergency legacy registry key

Update#1

- Expanded default exemption to all Admins
- Design + implement new GPO

Update#2

- Smart card fix
- All evaluation logic moved to DC

Final Update

- Remove Legacy Reg key
- Fix GPO issue across one-way trusts

KB5020276—Netjoin: Domain join hardening changes - Microsoft Support

Releasing vs Servicing Windows

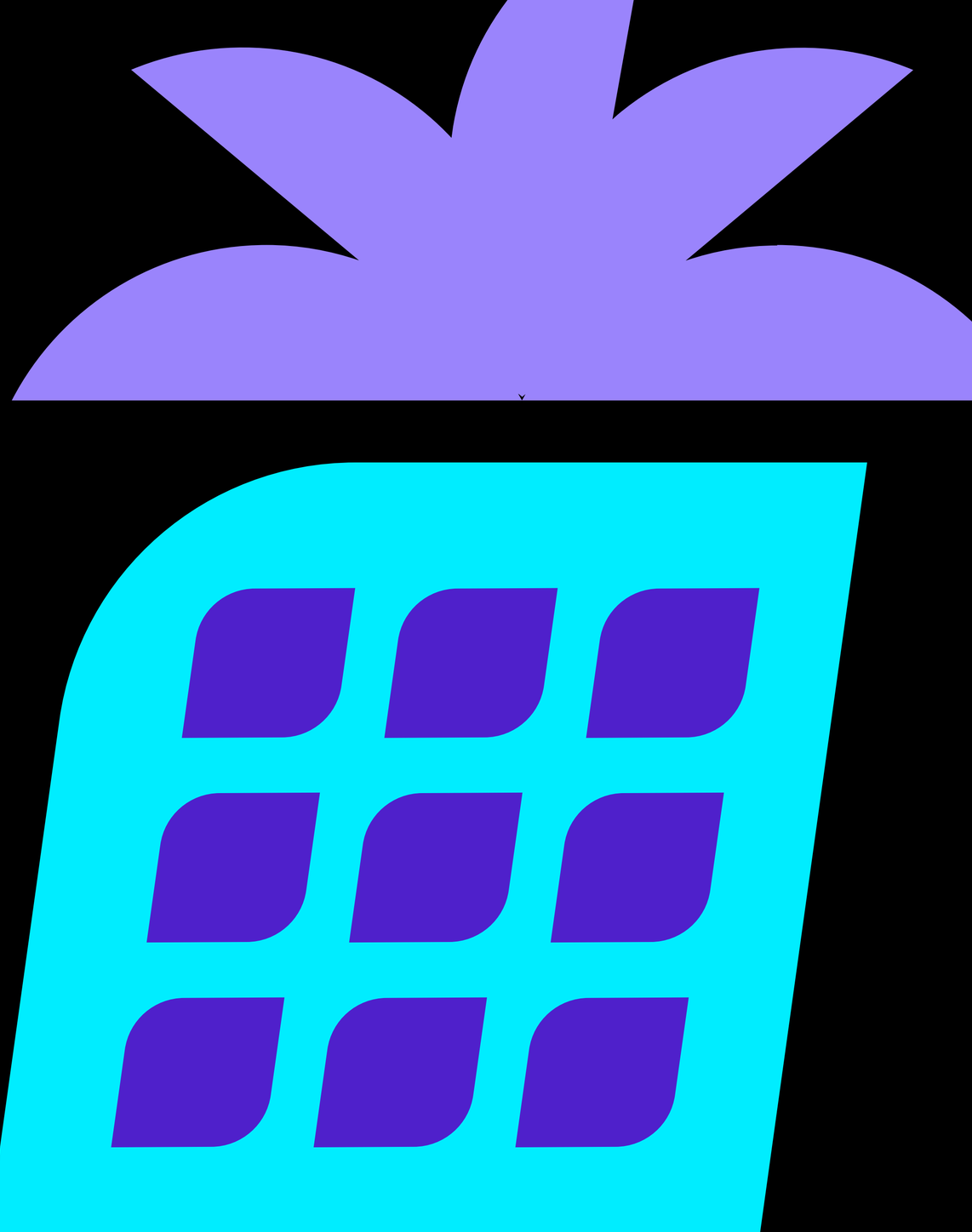
Releasing to New Users

Servicing to Existing Users

Agenda

What’s New? What’s Next?

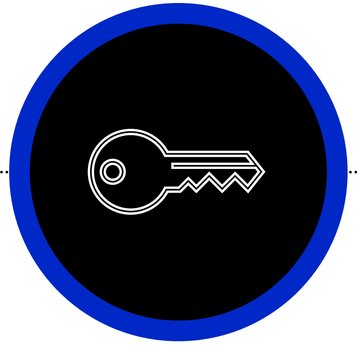
- Explore upcoming AD security enhancements
  - What to enable
  - What to retire
  - Why it matters



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

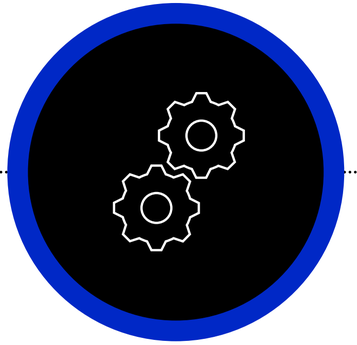
Investment Focus for Active Directory

Security

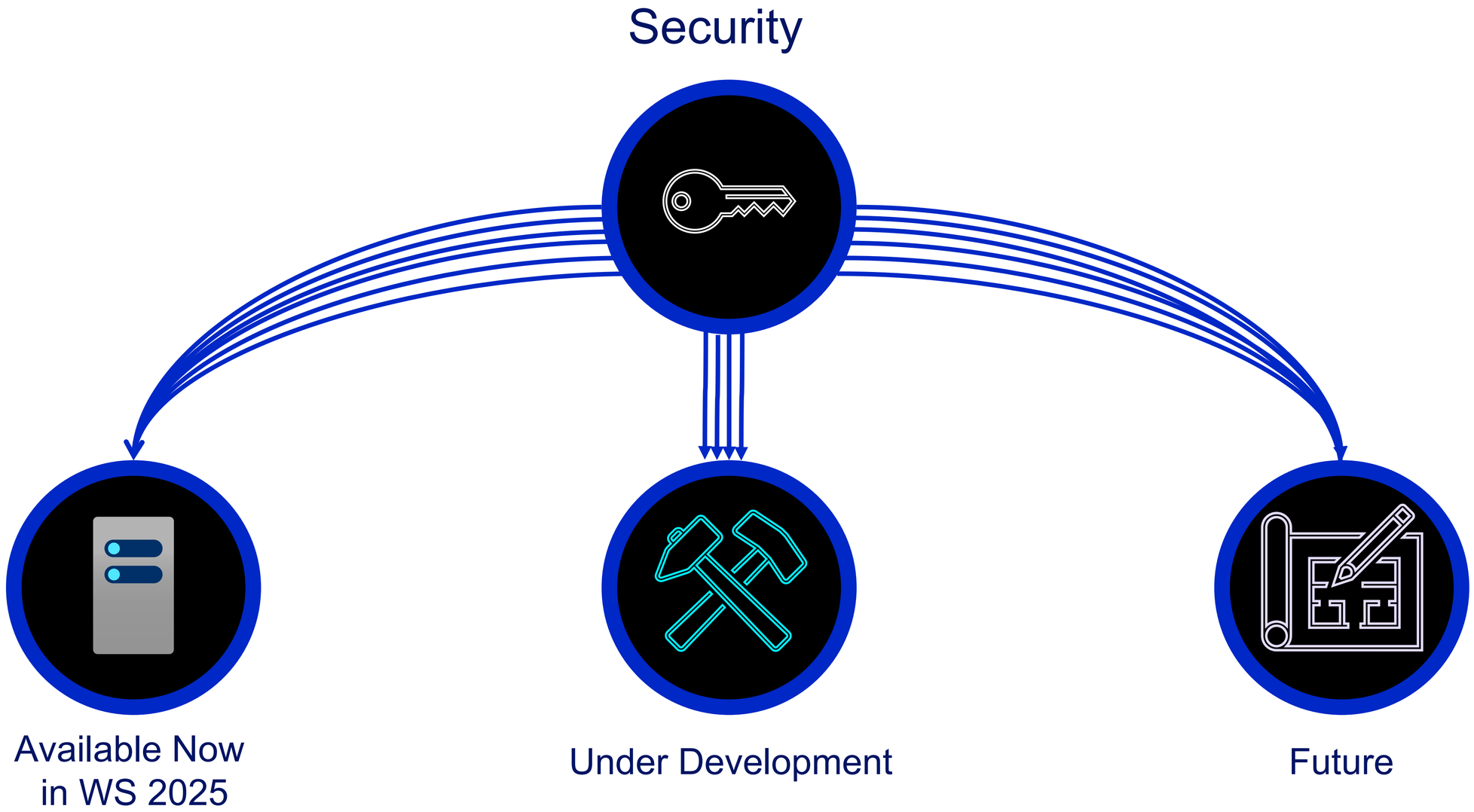


Cloud Enablement

Supportability



Deep Dive: Security Focused AD features

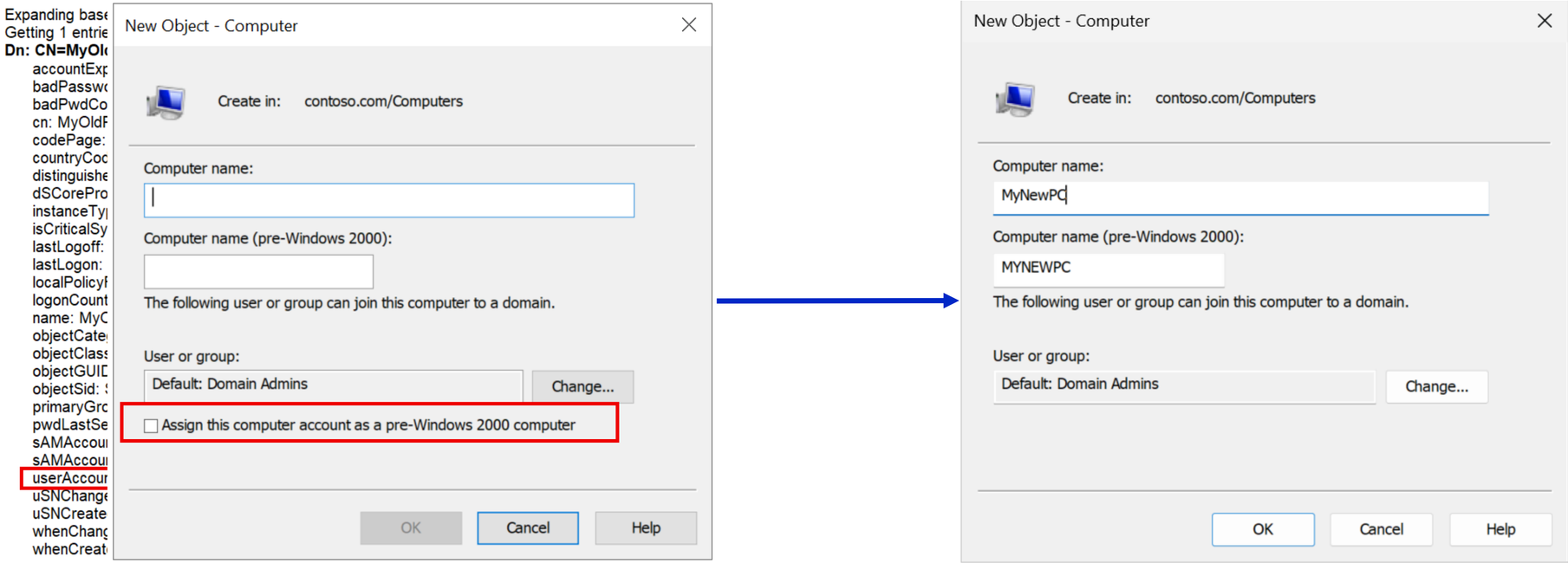


HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Available Now: Server 2025

Available Now
In WS 2025

- Improved default machine account passwords for accounts created on WS2025 DC
- Goodbye to “pre-Windows 2000 computer” box



[What's new in Windows Server 2025 | Microsoft Learn]

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

LDAP Security Improvements

Available Now
In WS 2025

- LDAP signing is enforced by default
- LDAP channel binding is set to when supported
- Confidential attributes require encrypted connection
- LDAP client encryption preferred by default

Table 3: CBT events

Event	Description	Trigger
3074	The following client performed an LDAP bind over SSL/TLS and would have failed the channel binding token validation if the directory server was configured to enforce validation of Channel Binding Tokens.	Triggered in any of the following circumstances: ▪ When a client attempts to bind with an improperly formatted Channel Binding Token (CBT) Minimum logging level: **2**
3075	The following client performed an LDAP bind over SSL/TLS and did not provide Channel Binding Information. When this directory server is configured to enforce validation of Channel Binding Tokens, this bind operation will be rejected.	Triggered in any of the following circumstances: ▪ When a client that is capable of channel binding does not send a CBT ▪ A client is capable of channel binding if the EPA feature is installed or available in the OS and not disabled through the registry setting **SuppressExtendedProtection**. To learn more, see KB5021989. Minimum logging level: **2**

Domain controller: Allow vulnerable Netlogon secure channel connections	Not Defined
Domain controller: LDAP server channel binding token requirements	Not Defined
Domain controller: LDAP server signing requirements	None
Domain controller: LDAP server signing requirements Enforcement	Not Defined
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Account Lockout Policy expansion

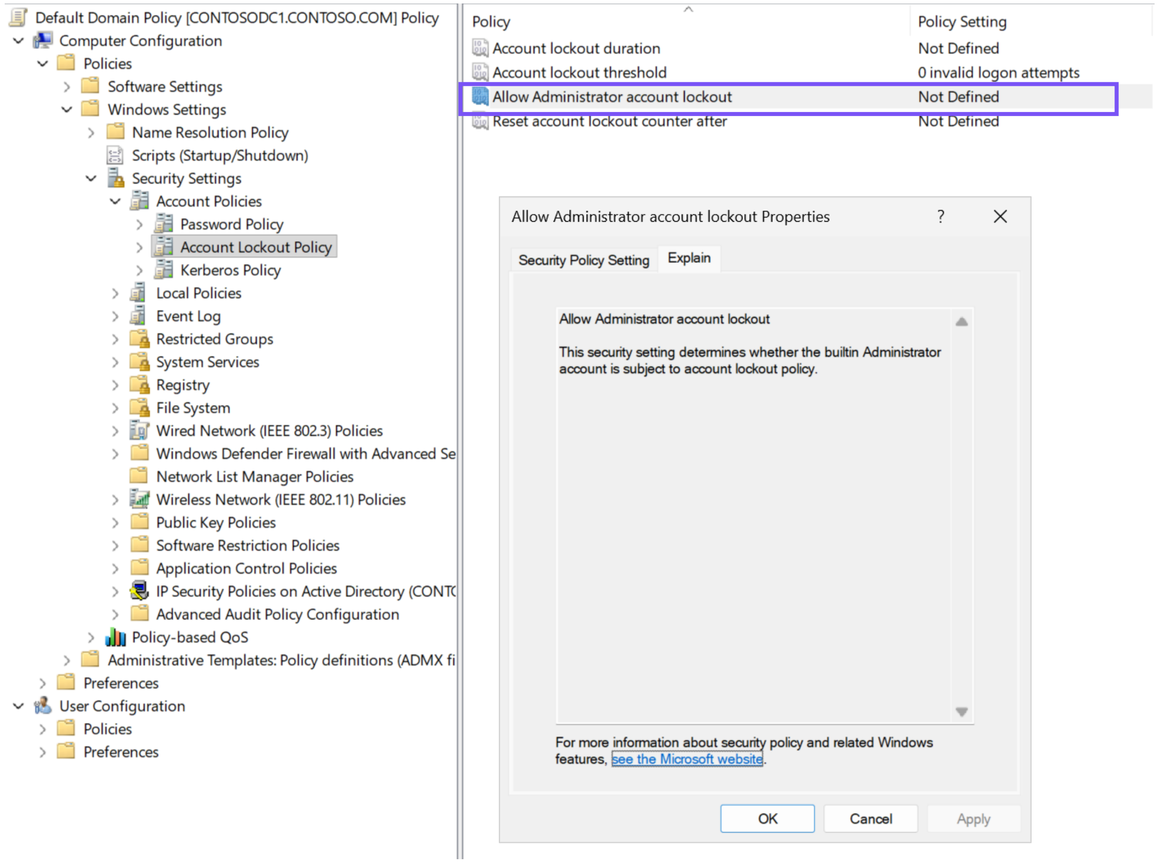
Available Now
In WS 2025

Built-In Administrator accounts can be locked out for NETWORK logons (such as RDP)

Defaults:

- **10** login failures
- Within **10** minutes
- Locks the account for **10** minutes

- Admin passwords — complexity required by default
- Local account lockout enabled by default for both workstations and server SKUs
- Event IDs: 4740 (DC), 4625 (Client)



KB5020282—Account lockout available for built-in local administrators - Microsoft Support

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

DMSA

Available Now
In WS 2025

- **Delegated Managed Service Accounts**
- Seamlessly supersede service accounts
- New account “retains” permissions of the defuncted SA
- Simple deployment with PowerShell
- Only accessible by KDC to retrieve keys
- No cred/identity changes required on service

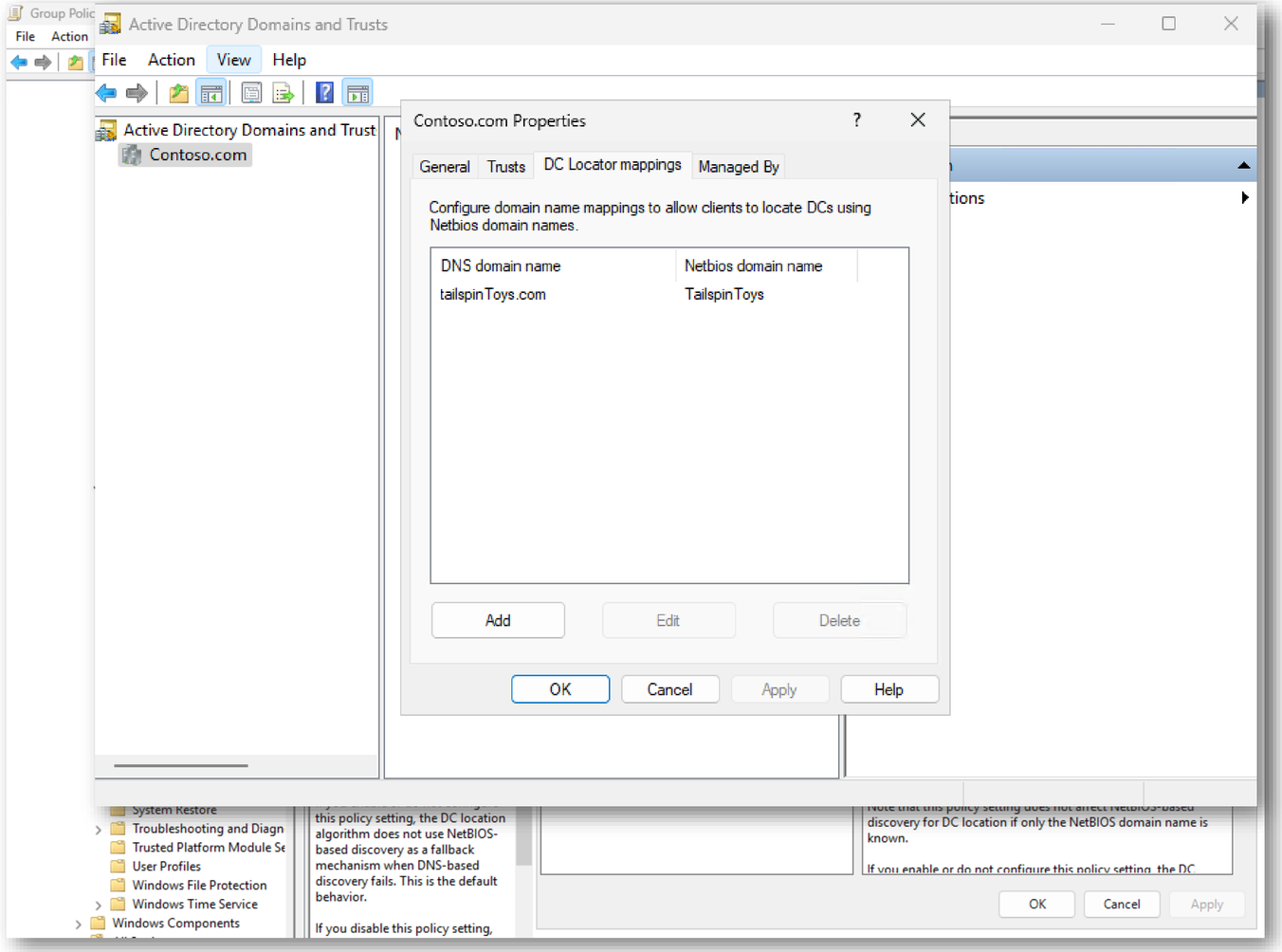
- **BadSuccessor (CVE-2025-53779)**: We now validate both accounts
  - Also mitigated by enforcement of CreateChild permission hardening
  - Released on WS2025 in August

dmsa@microsoft.com

DC Locator Improvements

Available Now
In WS 2025

- Administrators can configure mappings of NETBIOS names to DNS names through GPO
- No more MAILSLOTS



[The beginning of the end of Remote Mailslots - Microsoft Community Hub]

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Improved Trust Security

Available Now
In WS 2025

Name	Type	Description
Domain Admins	Security Group ...	Designated administrators of the domain
Domain Computers	Security Group ...	All workstations and servers joined to the domain
Domain Controllers	Security Group ...	All domain controllers in the domain
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators of the enterprise
Enterprise Key Admins	Security Group ...	Members of this group can perform administrative actions on key objects within the for...
Enterprise Read-only Domain Controllers	Security Group ...	Members of this group are Read-Only Domain Controllers in the enterprise
External Trust Accounts	Security Group ...	All external trust accounts in the domain.
Forest Trust Accounts	Security Group ...	All forest trust accounts in the forest.
Group Policy Creator Owners	Security Group ...	Members in this group can modify group policy for the domain

- Unique PrimaryGroupId for external and forest trust accounts respectively
- Effective on all trusts (even existing ones) when PDC role is on WS 2025 DC

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

LSARPC Improvements

Available Now
In WS 2025

```
NTSTATUS
LsarOpenPolicy3(
    [in,unique,string] PLSAPR_SERVER_NAME              SystemName,
    [in] PLSAPR_OBJECT_ATTRIBUTES                      ObjectAttributes,
    [in] ACCESS_MASK                                   DesiredAccess,
    [in] ULONG                                         InVersion,
    [in] [switch_is(InVersion)] LSAPR_REVISION_INFO*   InRevisionInfo,
    [out] ULONG*                                       OutVersion,
    [out] [switch_is(*OutVersion)] LSAPR_REVISION_INFO* OutRevisionInfo,
    [out] LSAPR_HANDLE*                                PolicyHandle
    );
```

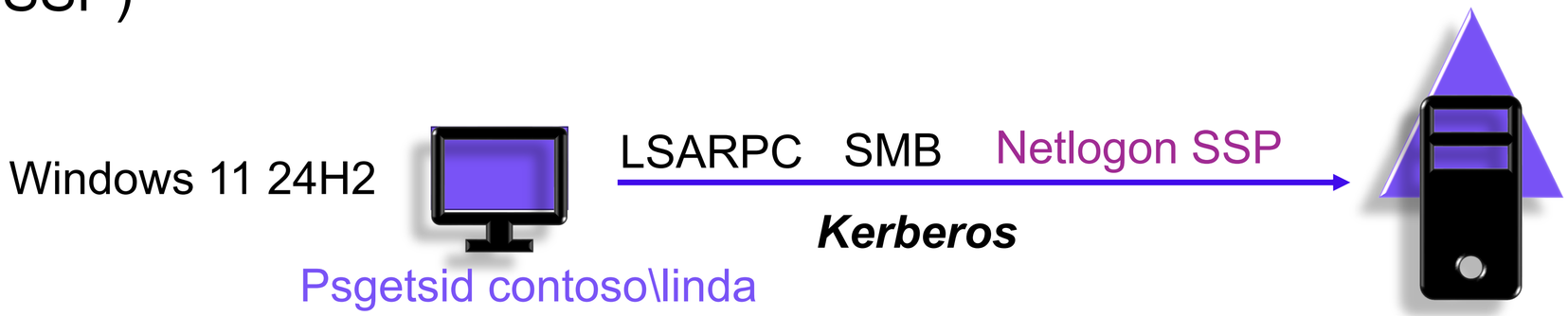
```
typedef struct _LSAPR_REVISION_INFO_V1{
    ULONG Revision;
    ULONG SupportedFeatures;
} LSAPR_REVISION_INFO_V1, *PLSAPR_REVISION_INFO_V1;
```

Value	Meaning
0x00000002	Upon receipt by the client, this value, when set, indicates that the **client can use authentication other than the RPC_C_AUTHN_NETLOGON security provider** when it calls **LsarLookupNames4** and **LsarLookupSids3** ([MS-LSAT] sections 3.1.4.5 and 3.1.4.9). It also indicates that the server supports the method **LsarOpenPolicyWithCreds** (section 3.1.4.4.10).<20>

Improved SID/Name Translation

Available Now
In WS 2025

Sid / Name lookups now use ***Kerberos*** authentication and encryption (was Netlogon SSP)




```
NTSTATUS
LsarOpenPolicyWithCreds(
    [in] handle_t                                    BindingHandle,
    [in] PLSAPR_OBJECT_ATTRIBUTES                    ObjectAttributes,
    [in] ACCESS_MASK                                 DesiredAccess,
    [in] ULONG                                       InVersion,
    [in] [switch_is(InVersion)] LSAPR_REVISION_INFO* InRevisionInfo,
    [out] ULONG*                                     OutVersion,
    [out] [switch_is(*OutVersion)] LSAPR_REVISION_INFO* OutRevisionInfo,
    [out] LSAPR_HANDLE*                              PolicyHandle
    );
```

[MS-LSAD]: LsarOpenPolicyWithCreds (Opnum 135) | Microsoft Learn

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

LAPS

Available Now
In WS 2025

- **Automatic Account Management**
  - Enable/disable, rename, or randomize the local admin account
- **Passphrase Support**
  - Randomly generate passwords like CorrectHorseBatteryStaple
- **Readability Support**
  - Removes similar looking characters like I/l/1, O/Q/0/o
- **Image Rollback Protection**
  - Prevents torn password state in the event of a recovery
- **Password Recovery from AD Database Backup Media**
  - Includes DSRM passwords

The latest and greatest in the world of Windows LAPS - Microsoft Technical Takeoff

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

In Development



Under development

AD Partnerships

- Forest recovery / cybersecurity incident recovery improvements
- Support for various Defender features
- Support for various authentication and other OS security features (e.g., Local Admin protection)
  Administrator protection on Windows 11 | Microsoft Community Hub
- Hybrid security support

Active Directory

- LDAP auditing improvements
- LDAP security improvements
- ADCS improvements (including PQS)
- DMSA improvements

"Some information relates to pre-released product, which may be substantially modified before it's commercially released. Microsoft makes no warranties, express or implied, with respect to the information provided here."

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Planned: Investigating

Future

- **Top AD customer asks**

  - Native AD backup and restore
  - On-prem MFA
  - AD management and tools improvements
  - Improved cloud migration scenarios

Have an ask? - adfeedback@microsoft.com

"Some information relates to pre-released product, which may be substantially modified before it's commercially released. Microsoft makes no warranties, express or implied, with respect to the information provided here."

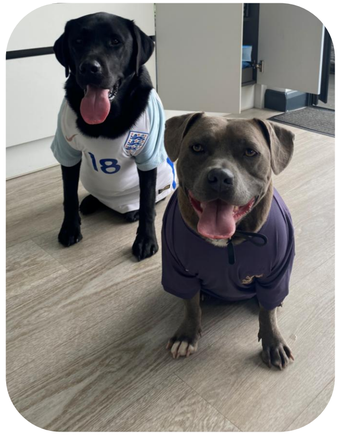
HYBRID IDENTITY PROTECTION conf25 CHARLESTON

AD Changes You Should Enable

Beware of the Create Child permission!

KB5008383—Active Directory permissions updates (CVE-2021-42291) - Microsoft Support

Strong cert mapping
KB5014754: Certificate-based authentication changes on Windows domain controllers - Microsoft Support



Newest DFL / FFL
Has goodies such as
32k pages
Recycle Bin
Protected users group
Auth silos


Legacy AD Features to Disable

mSDS-machineAccountQuota

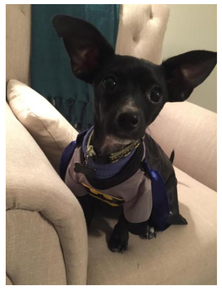
Active Directory domain join permissions in Windows Server | Microsoft Learn

NTLM

https://aka.ms/ntlm

External trusts

ADCS default templates



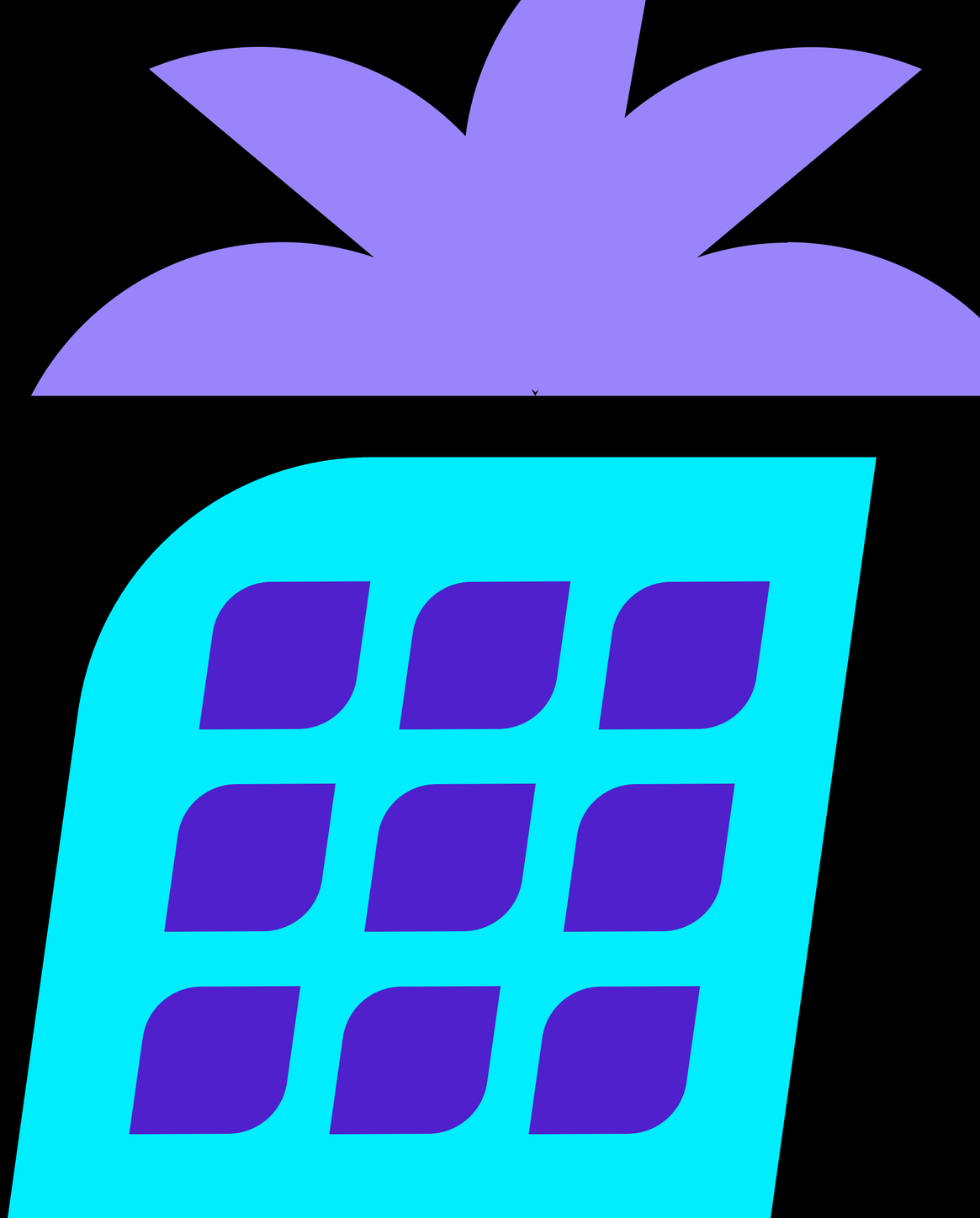
RC4

Documentation is in the works

Wrap up

How you can help!

- Key takeaway
- How to engage us!



HYBRID IDENTITY PROTECTION conf25 CHARLESTON

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Key Takeaway

*“Microsoft is committed to keeping **Active Directory protected** and **productive** in modern enterprise environments by investing in its security and supportability while also supporting our customers' transitions to cloud-based identity solutions.”*

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

How to Engage Us

ADFeedback
@microsoft.com

Feedback Hub

Support

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Questions?

HYBRID
IDENTITY
PROTECTION

conf25

CHARLESTON