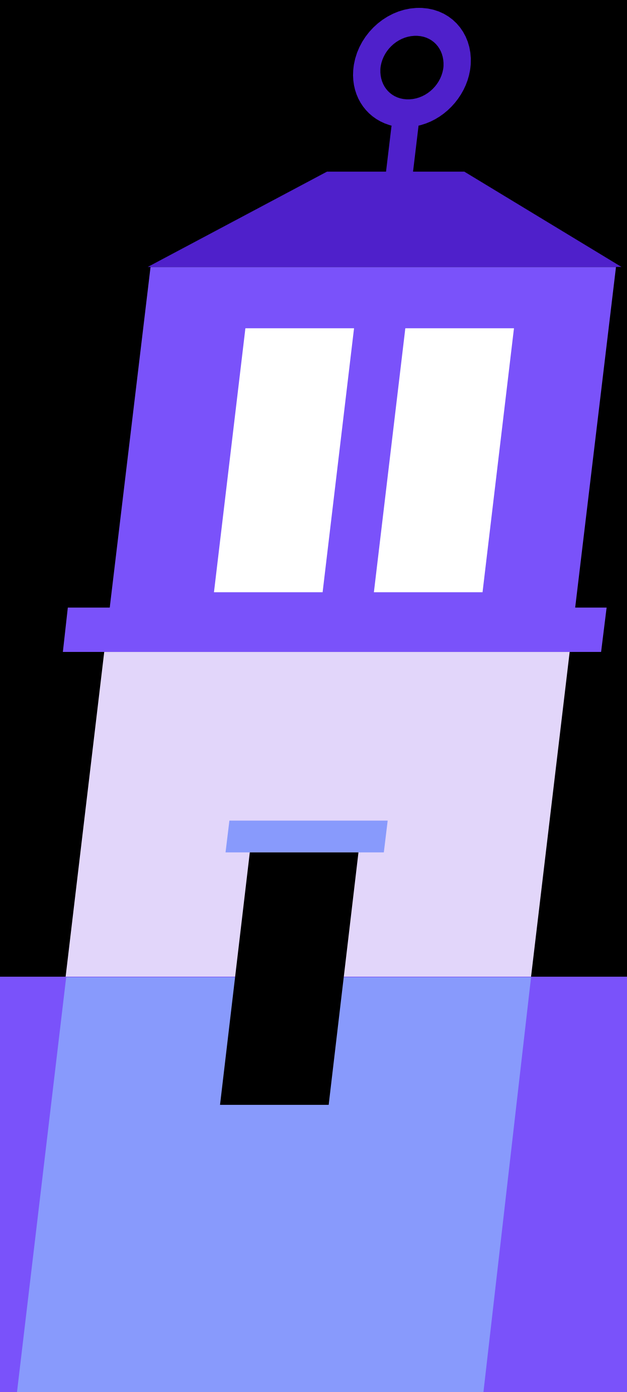
HYBRID IDENTITY PROTECTION conf25

CHARLESTON



Real-World ITDR for Hybrid Identity Environments

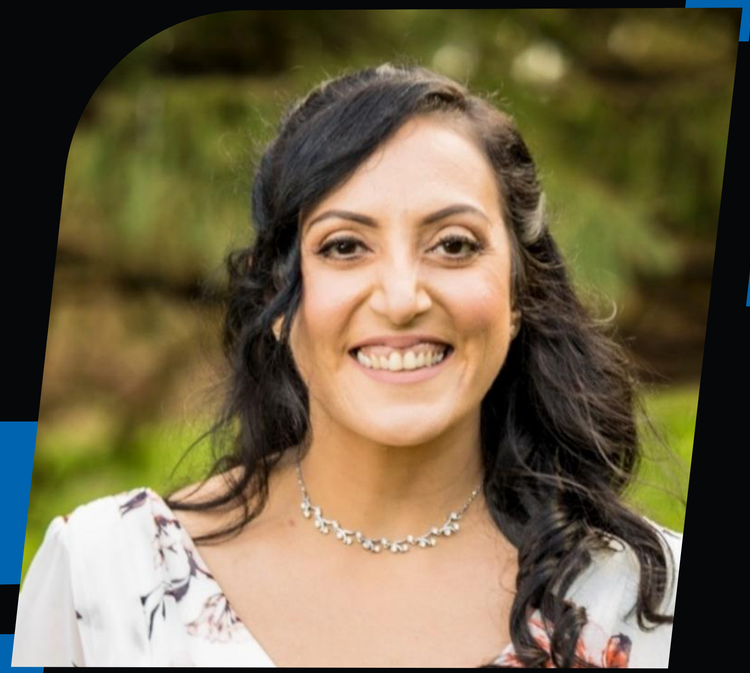
HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Jared Ross

Principal Product Architect, Entra ID, Microsoft

Jared Ross is a Product Architect at Microsoft focused on Identity Security and ITDR – enabling the evolution of the identity enabled SOC. Jared enjoys engaging deeply with customers and partners to build products that bridge technical and organizational divides. He previously led product areas across Azure from the early days of cloud. He lives in Seattle area and enjoys great sushi and his dog, Owen.

HYBRID IDENTITY PROTECTION conf25
CHARLESTON



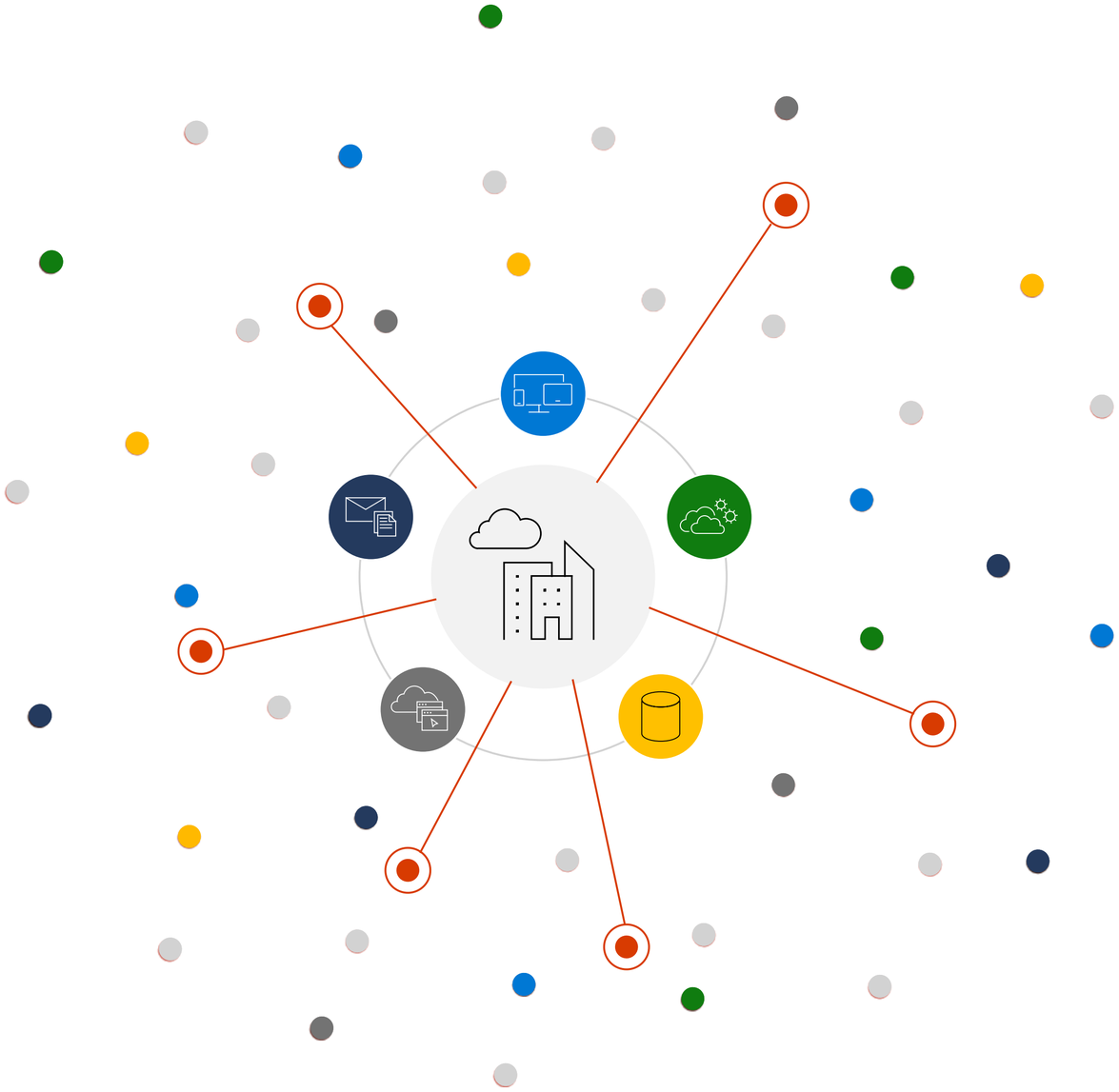
Sharon Chahal

Principal Product Manager, Entra ID

Sharon Chahal is a Principal Product Manager at Microsoft, in the MS Security Customer Experience Engineering team supporting Microsoft Entra. With over 25 years in the tech industry, she brings deep expertise in helping organizations design and architect secure identity solutions. Her passion for identity, security, and customer success drives her collaborative approach to problem-solving and innovation. Sharon brings deep expertise across IAM, Zero Trust, GenAI, and cybersecurity.

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Identities are the new security perimeter



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

The challenge of securing access continues to intensify

Median time for an attacker to access private data from phishing

1h12mins[1]

2023

60 seconds[2]

2024

Passwords attacks per second

2023

2024

Increased advanced attacks

+111%

increase in token theft in just one year

Speed

Scale

Sophistication

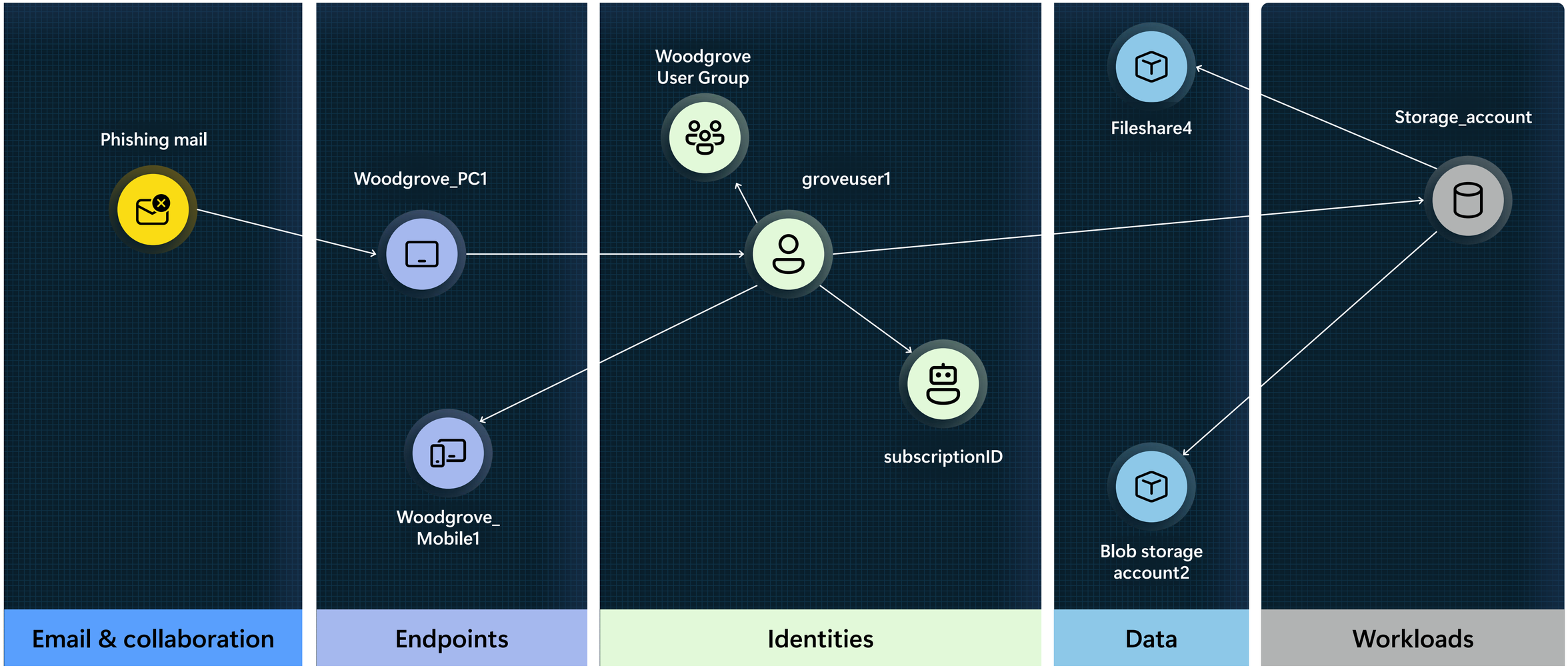
Over 300B identities across humans and machines

1 Microsoft Digital Defense Report 2023, 2024
2 Verizon Data Breach Investigations report, 2024

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

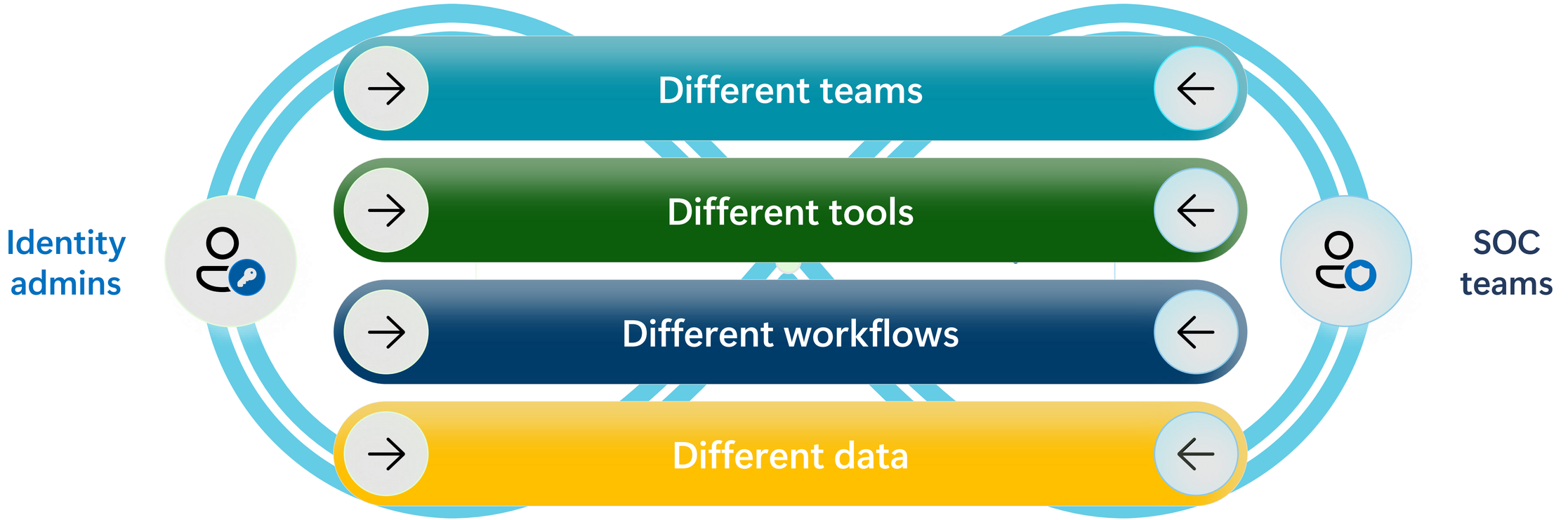
Attacker paths

surveying potential attack paths



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Modern identity security requires a partnership



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Identity admins

Foundational IAM and Modern Auth

Empowering AI for Security

Real-time adaptive access fueled by insights

Enhanced threat intelligence and response actions between identity and SOC teams

The future of protection

Extending protection to non-human identities, AI agents, and workloads

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Modern authentication starts with Microsoft Entra ID, the first layer to any identity security practice

Poor:
Password only

123456

admin

quertyuiop

P@ssword2024!

5%gHy*73xWcd#jQz89
cnpGo!17

Fair:
Password and...

- SMS
- Voice

Better:
Password and...

- Microsoft Authenticator push notifications
- Software Tokens OTP
- Hardware Tokens OTP

Better:
Passwordless

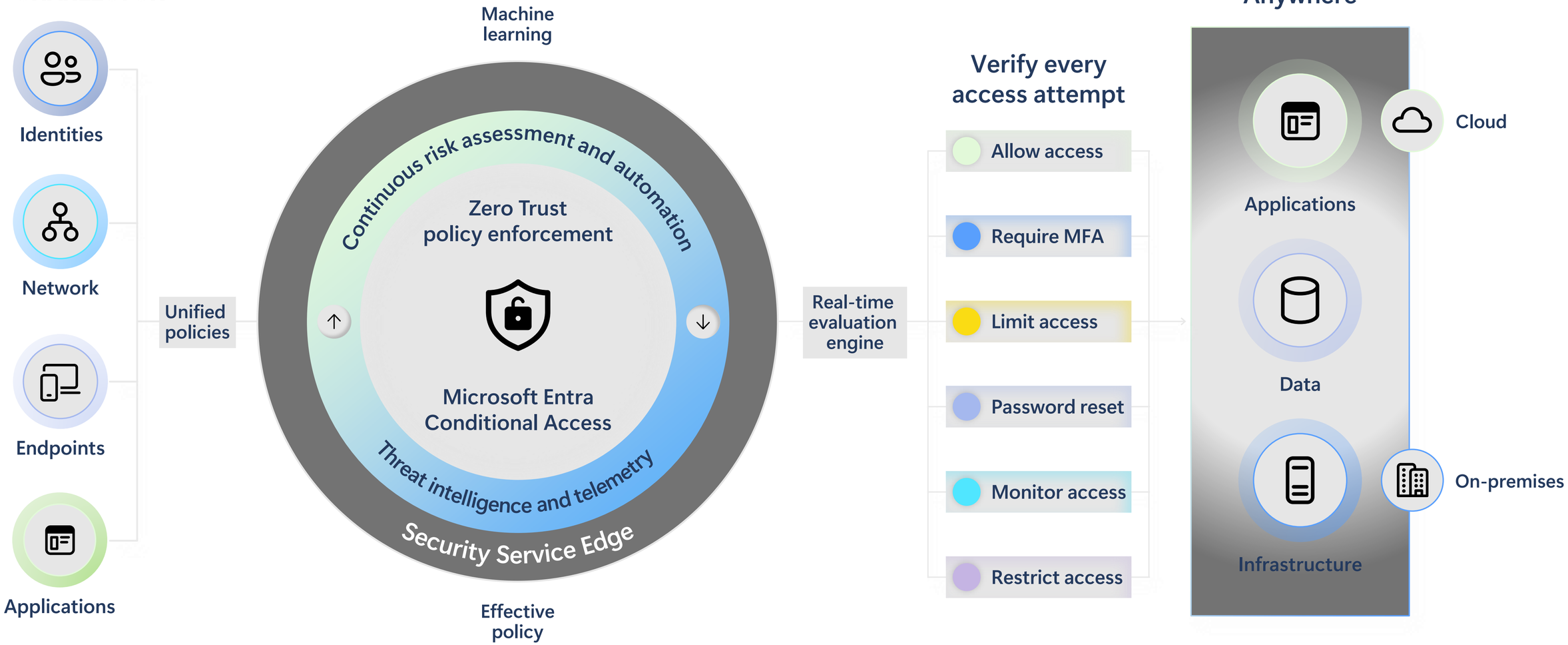
- Microsoft Authenticator phone sign-in

Best:
Phishing-resistant

- Windows Hello for Business
- FIDO2 security key
- Certificate-based authentication (multifactor)
- Passkey in Microsoft Authenticator (device-bound)
- Platform credential for macOS

Microsoft Entra ID supports a broad range of multifactor authentication options and external auth methods

Unify conditional access policies across your identity fabric



Build on threat-informed workflows in SIEM and XDR

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Conditional Access Policy optimization agent

Problem

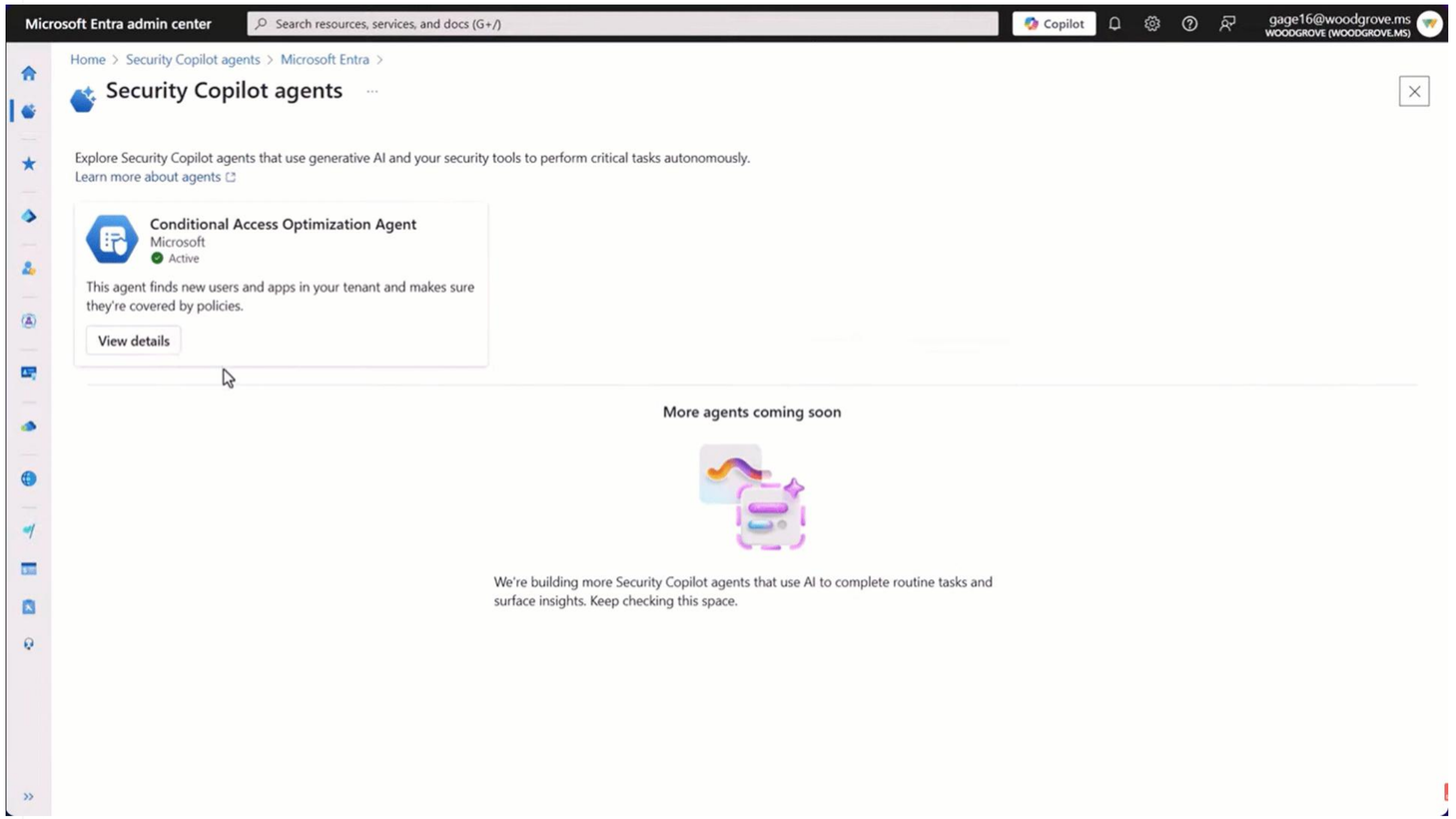
Admins struggle to identify security gaps because of the scale and complexity of their organization and resulting Conditional Access policy set

How the CA Agent helps

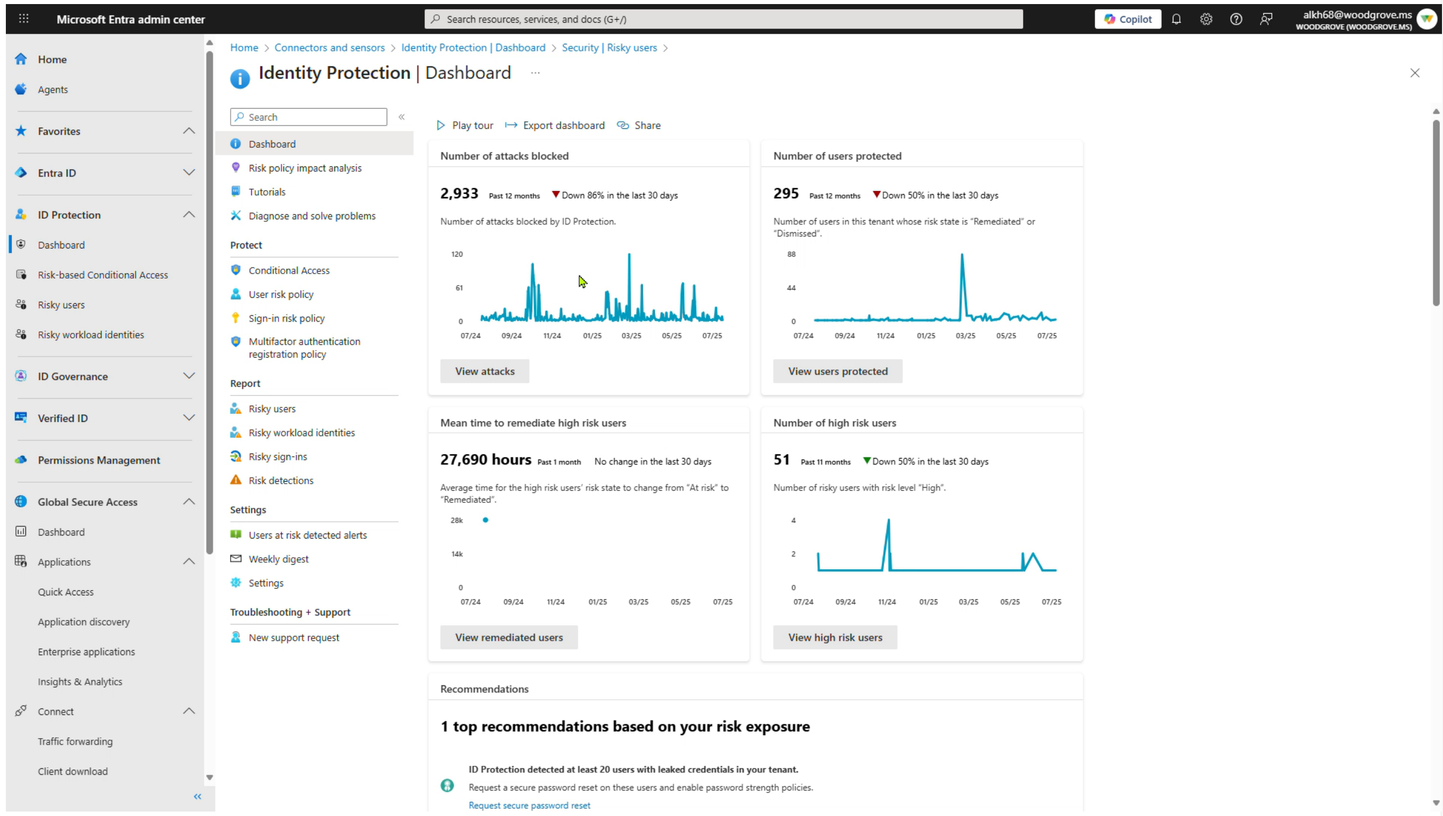
The CA optimization agent will automatically identify new objects (users/apps/devices) creation; analyze CA policies to identify gaps where new objects are not protected by CA

How the Agent increases efficiency

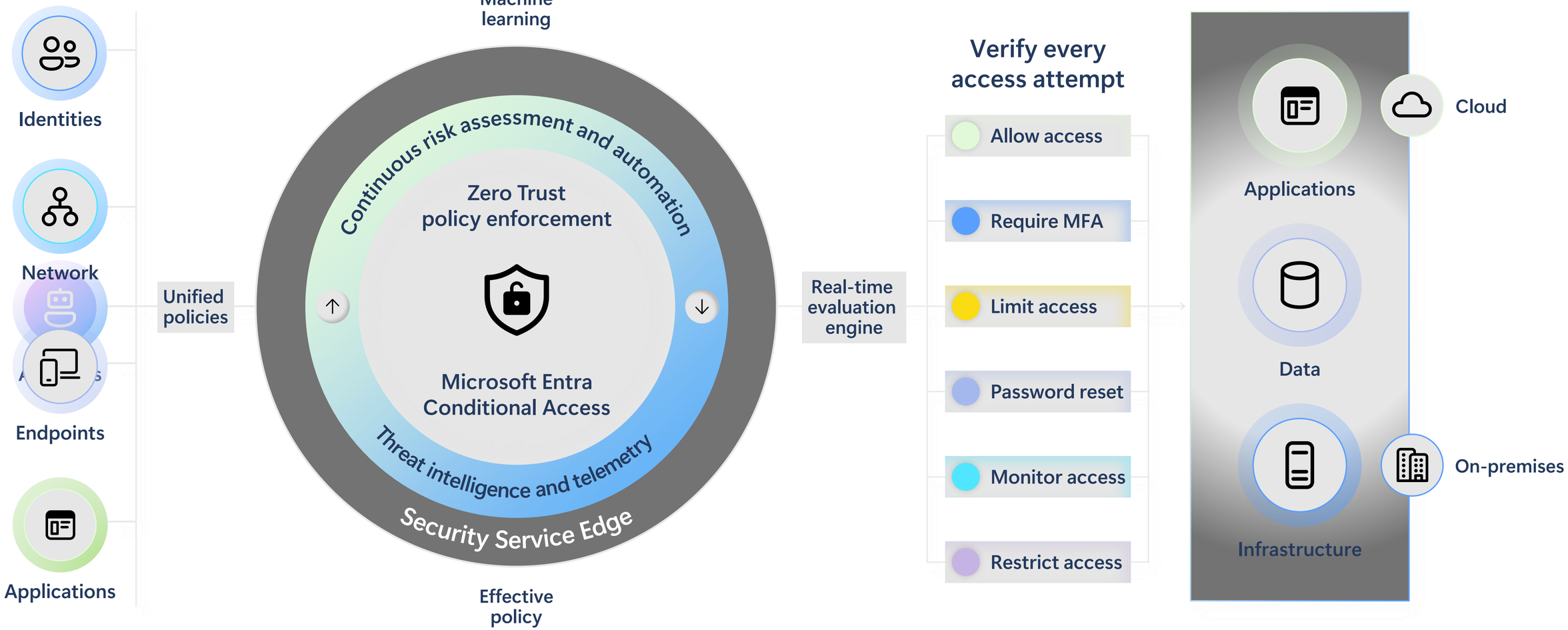
The CA optimization agent will recommend next steps to close gaps; provide a one-click action to apply the recommendation in report-only mode



Extending Security Copilot to make remediating users faster



Zero Trust policy engine for agentic AI



Build on threat-informed workflows in SIEM and XDR

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

SOC teams

Comprehensive coverage

Dedicated sensors and connectors provide protection across your unique identity fabric

Enriched visibility

Correlating identities and relevant data for greater visibility and insights

Security context

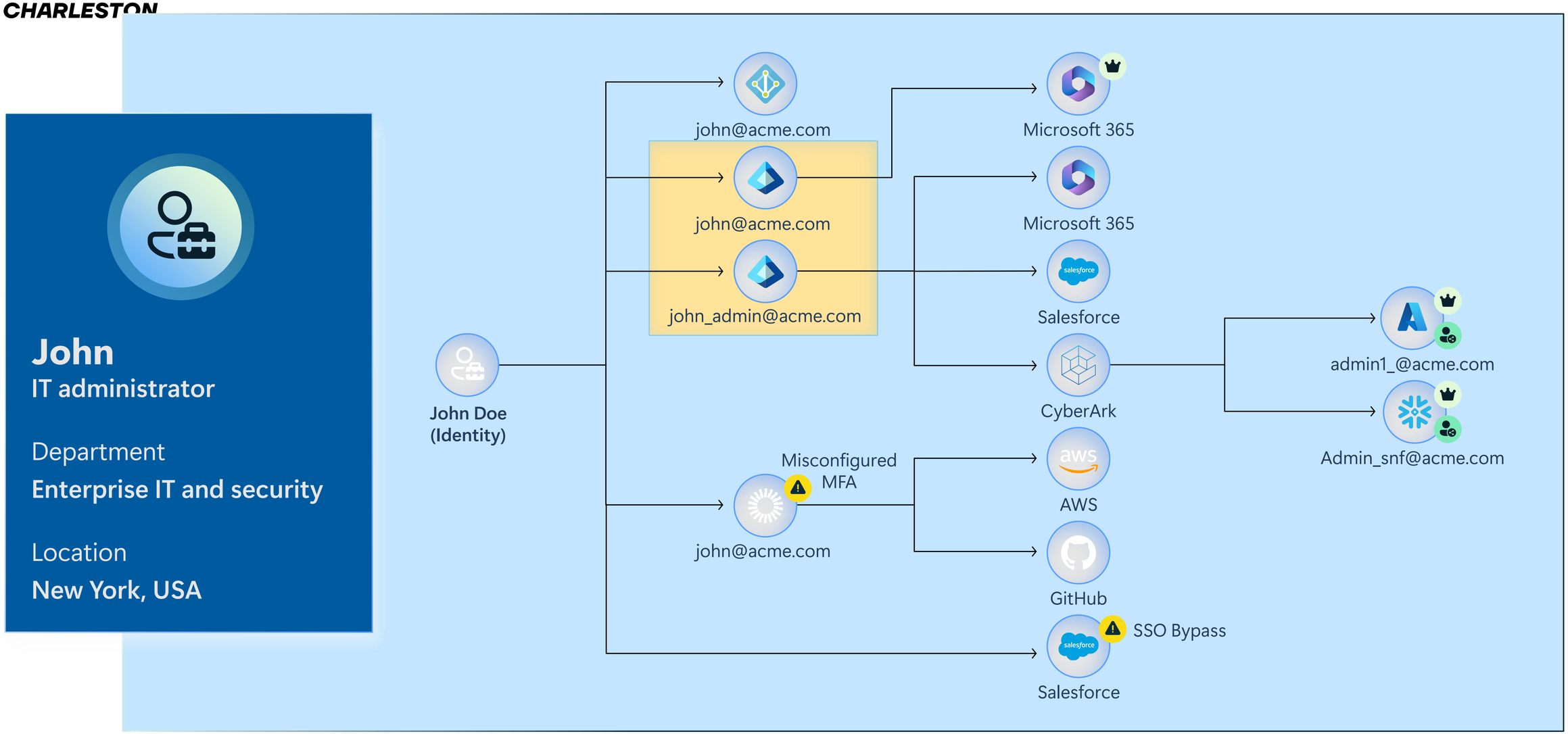
Identity posture, alerts and response actions in the context of SOC operations

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Comprehensive coverage
Dedicated sensors and connectors extend protections across your unique identity fabric

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Identity-centric security



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Enriched visibility into your unique identity fabric

Any identity:

Human

Non-human

Enriched with:

Other identity systems

Privileged access management

Identity governance administration

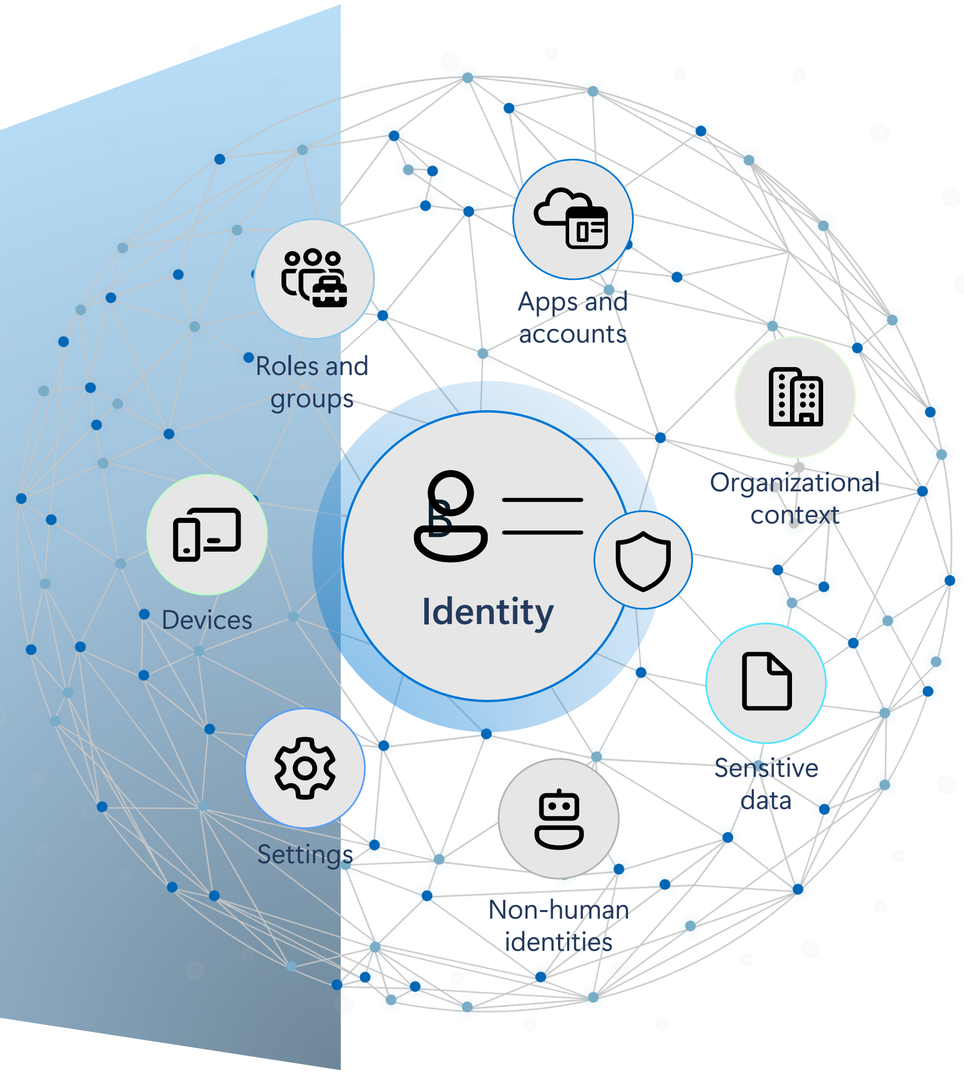
HR systems

Workday | Success Factors | API Management

Line of business applications

SAP | ECC | Oracle Database

Enterprise SaaS apps



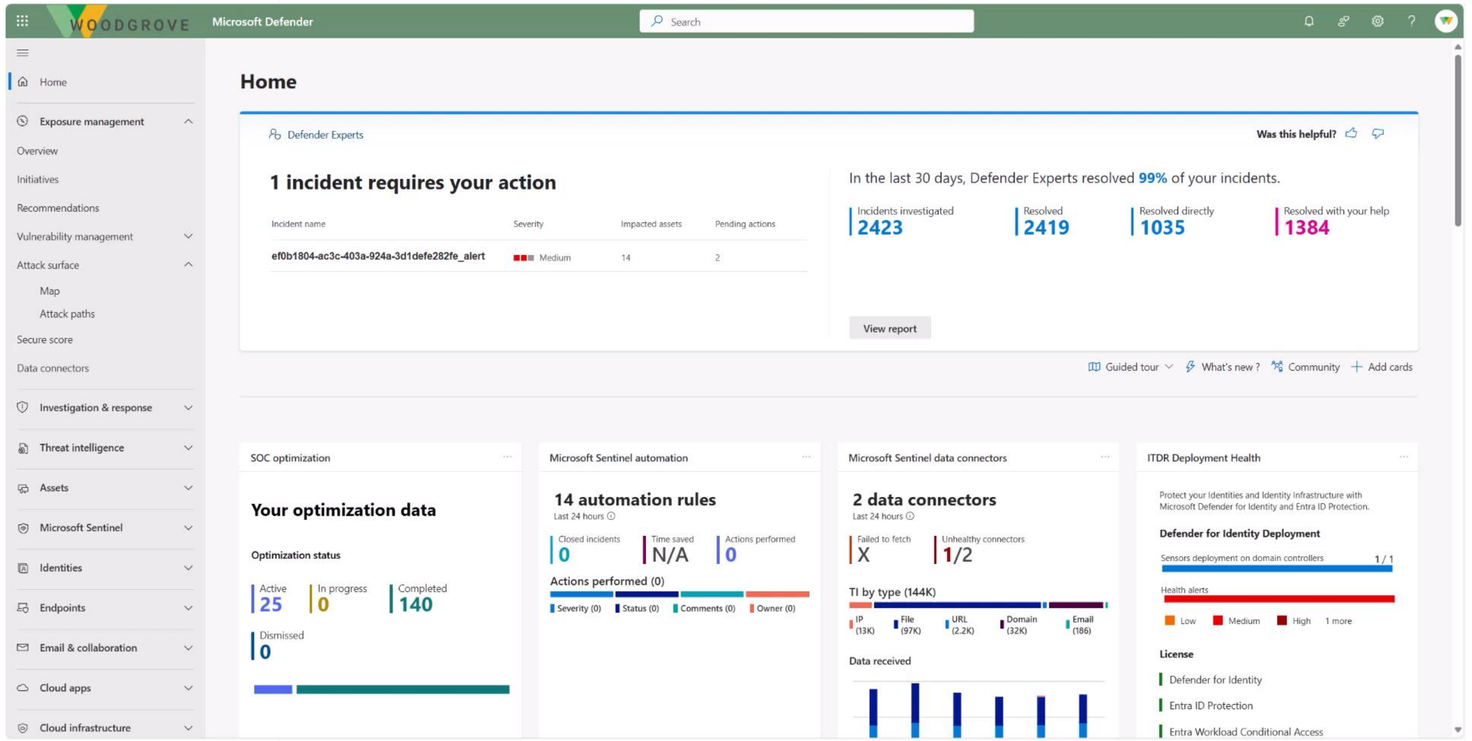
HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Holistic posture

Identity-specific posture recommendations (ISPM) consistently surfaced across experiences

Dedicated identity posture initiative groups ISPM's for more focused inspection

Cross-domain **attack path mapping** highlights potential vulnerabilities and lateral movement paths



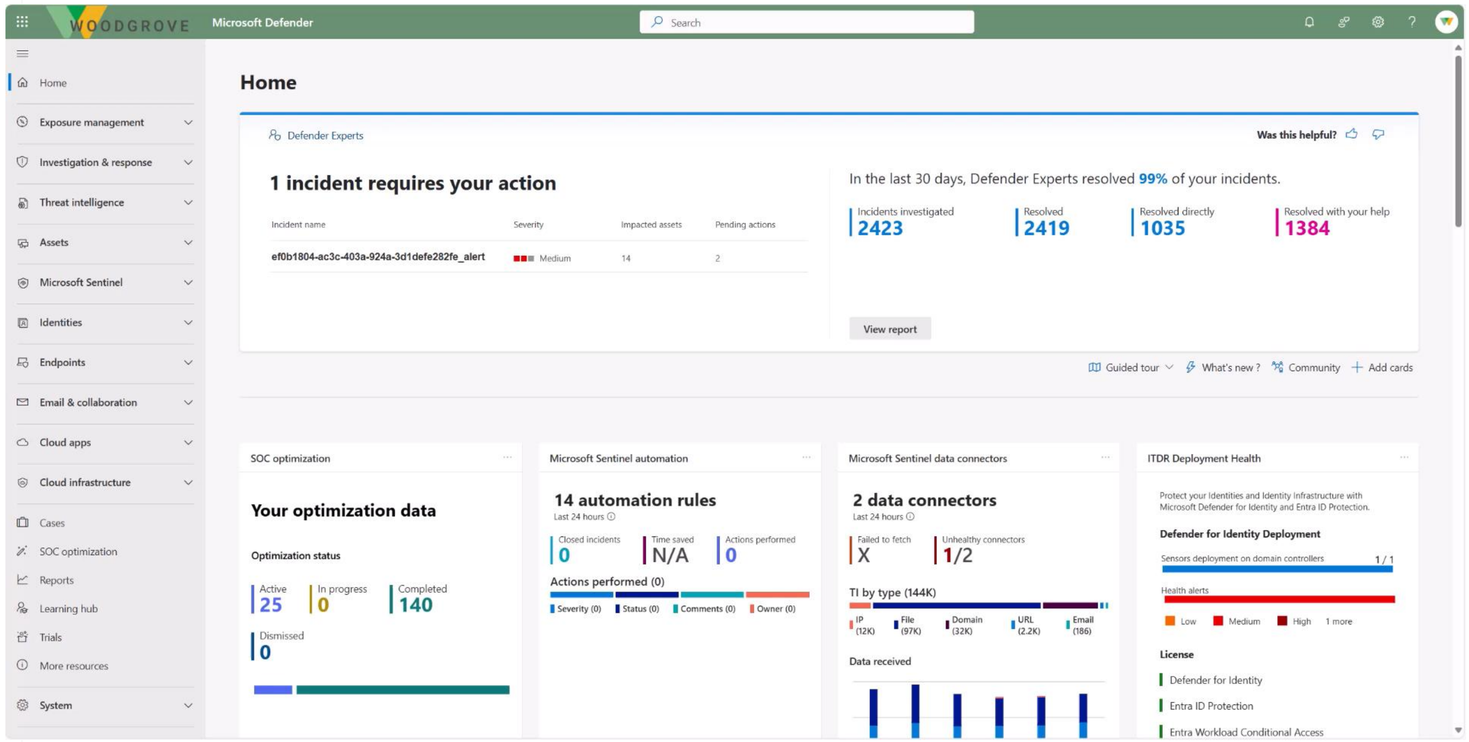
HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Incident-level visibility

Identity alerts are automatically correlated with data from across security domains to help the SOC easily understand **how the attacker went from compromise to target**

Cross-domain threat hunting experience allows users to **seamlessly query security data for deeper analysis into an attack or to spot underlying threats**

AI-powered insights and recommendations accelerate investigation and remediation



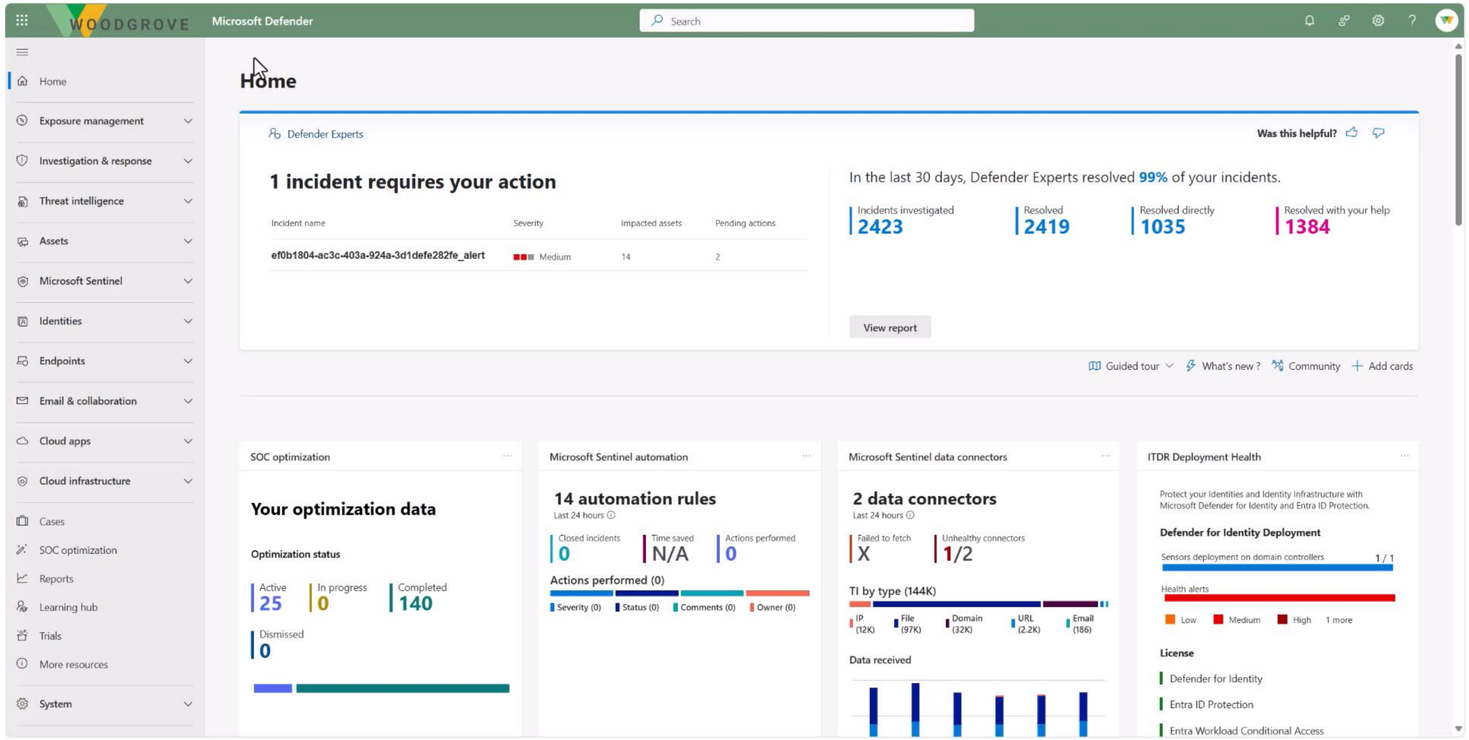
HYBRID IDENTITY PROTECTION conf25
CHARLESTON

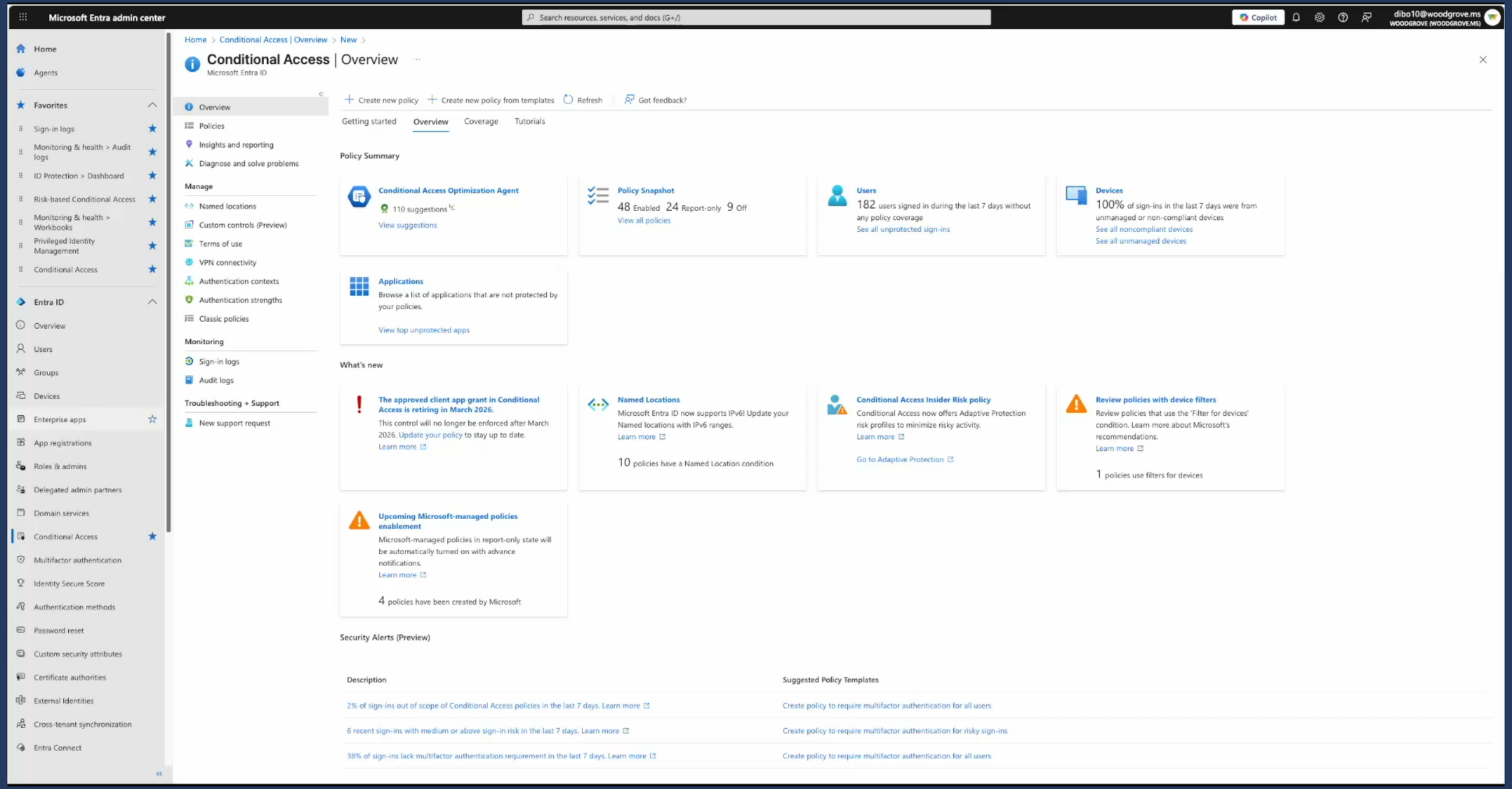
Automatic attack disruption

Built-in self-defense to automatically shutdown cyberattacks

Respond to identity threats **directly from the SOC experience.** Disable a user, mark a user as compromised or even rotate a password in a PAM solution.

Automatic attack disruption stops advanced multi-stage, multi-domain attacks by **identifying the compromised assets** and containing them in near real-time




Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
dibo10@woodgrove.ms
WOODGROVE (WOODGROVE.MS)
Home
Agents
Favorites
Sign-in logs
Monitoring & health > Audit logs
ID Protection > Dashboard
Risk-based Conditional Access
Monitoring & health > Workbooks
Privileged Identity Management
Conditional Access
Entra ID
Overview
Users
Groups
Devices
Enterprise apps
App registrations
Roles & admins
Delegated admin partners
Domain services
Conditional Access
Multifactor authentication
Identity Secure Score
Authentication methods
Password reset
Custom security attributes
Certificate authorities
External Identities
Cross-tenant synchronization
Entra Connect
Home > Conditional Access | Overview > New >
Conditional Access | Overview
Microsoft Entra ID
Overview
Policies
Insights and reporting
Diagnose and solve problems
Manage
Named locations
Custom controls (Preview)
Terms of use
VPN connectivity
Authentication contexts
Authentication strengths
Classic policies
Monitoring
Sign-in logs
Audit logs
Troubleshooting + Support
New support request
Create new policy
Create new policy from templates
Refresh
Got feedback?
Getting started
Overview
Coverage
Tutorials
Policy Summary
Conditional Access Optimization Agent
110 suggestions
View suggestions
Policy Snapshot
48 Enabled 24 Report-only 9 Off
View all policies
Users
182 users signed in during the last 7 days without any policy coverage
See all unprotected sign-ins
Devices
100% of sign-ins in the last 7 days were from unmanaged or non-compliant devices
See all noncompliant devices
See all unmanaged devices
Applications
Browse a list of applications that are not protected by your policies.
View top unprotected apps
What's new
The approved client app grant in Conditional Access is retiring in March 2026.
This control will no longer be enforced after March 2026. Update your policy to stay up to date.
Learn more
Named Locations
Microsoft Entra ID now supports IPv6! Update your Named locations with IPv6 ranges.
Learn more
10 policies have a Named Location condition
Conditional Access Insider Risk policy
Conditional Access now offers Adaptive Protection risk profiles to minimize risky activity.
Learn more
Go to Adaptive Protection
Review policies with device filters
Review policies that use the 'Filter for devices' condition. Learn more about Microsoft's recommendations.
Learn more
1 policies use filters for devices
Upcoming Microsoft-managed policies enablement
Microsoft-managed policies in report-only state will be automatically turned on with advance notifications.
Learn more
4 policies have been created by Microsoft
Security Alerts (Preview)
Description
Suggested Policy Templates
2% of sign-ins out of scope of Conditional Access policies in the last 7 days. Learn more
Create policy to require multifactor authentication for all users
6 recent sign-ins with medium or above sign-in risk in the last 7 days. Learn more
Create policy to require multifactor authentication for risky sign-ins
38% of sign-ins lack multifactor authentication requirement in the last 7 days. Learn more
Create policy to require multifactor authentication for all users

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Thank you!

HYBRID
IDENTITY
PROTECTION

conf25

CHARLESTON