

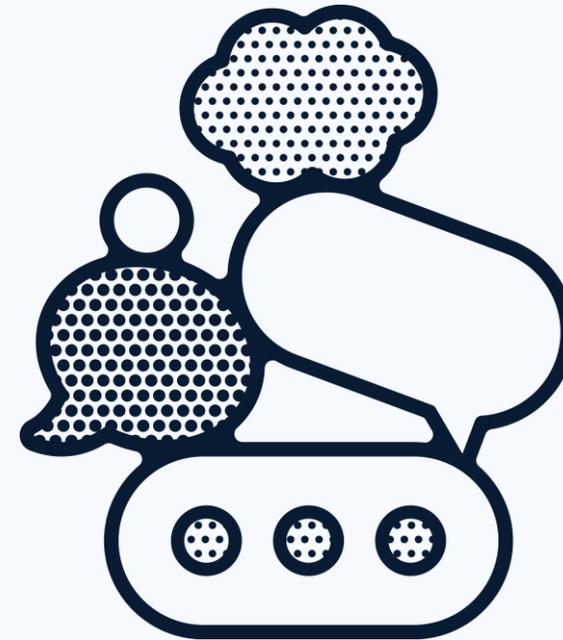
Attackers don't break in, they log in

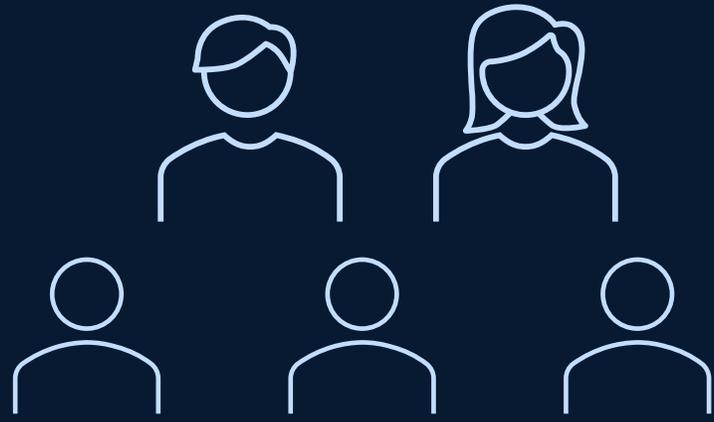
Webinar 22. Januari 2026

Gustav Jannerland, Bsure Sverige

Today's agenda

1. Highlights from Microsoft Digital Defense Report 2025
2. How attackers get in (spoiler: they log in)
3. Case example
4. Demo: Get an overview of identities and sign-ins in Entra ID





bsure.



Microsoft Digital Defense Report 2025

Lighting the path to a secure future

A Microsoft Threat Intelligence report

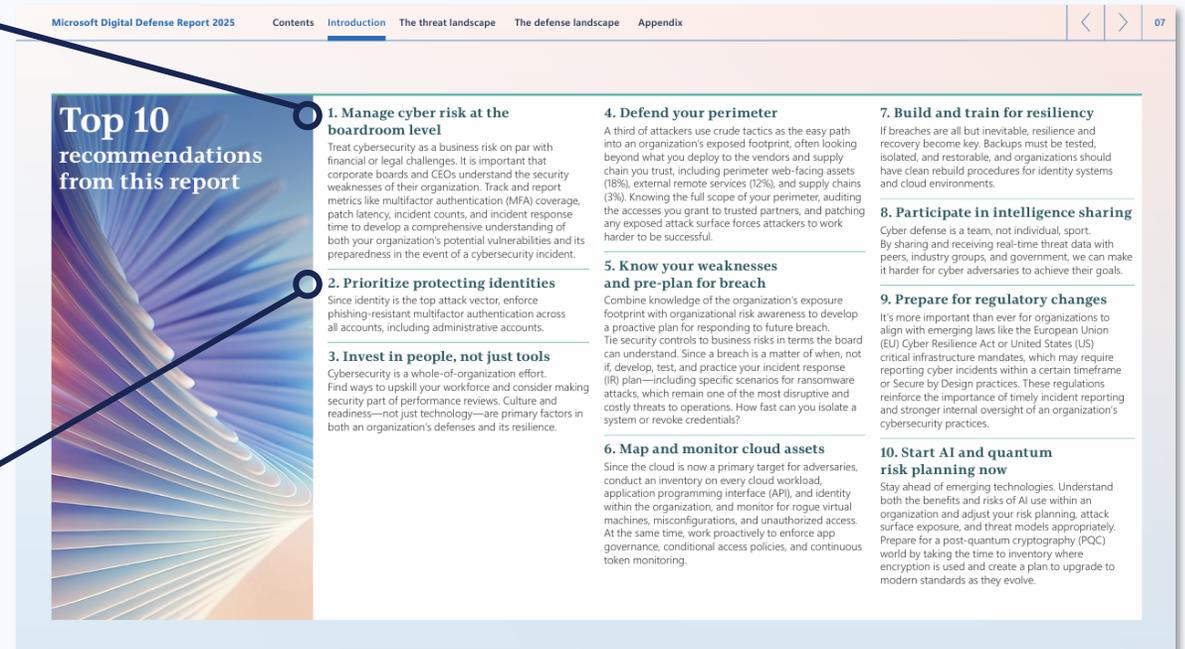
Top recommendations from the report

1. Manage cyber risk at the boardroom level

Treat cybersecurity as a **business risk** on par with financial or legal challenges. It is important that corporate boards and CEOs understand the security weaknesses of their organization.

2. Prioritize protecting identities

Since **identity is the top attack vector**, enforce phishing-resistant multifactor authentication across all accounts, including administrative accounts.



The screenshot displays the 'Top 10 recommendations from this report' section of the Microsoft Digital Defense Report 2025. The page has a navigation bar at the top with 'Contents', 'Introduction', 'The threat landscape', 'The defense landscape', and 'Appendix'. The main content area is titled 'Top 10 recommendations from this report' and lists ten key findings. Two recommendations are highlighted with callout boxes: '1. Manage cyber risk at the boardroom level' and '2. Prioritize protecting identities'. The first recommendation emphasizes treating cybersecurity as a business risk and understanding security weaknesses. The second recommendation focuses on identity as the top attack vector and enforcing phishing-resistant multifactor authentication. The remaining recommendations cover perimeter defense, knowing weaknesses, building resilience, intelligence sharing, regulatory changes, and AI/quantum risk planning.

Microsoft Digital Defense Report 2025 Contents Introduction The threat landscape The defense landscape Appendix

Top 10 recommendations from this report

- 1. Manage cyber risk at the boardroom level**

Treat cybersecurity as a business risk on par with financial or legal challenges. It is important that corporate boards and CEOs understand the security weaknesses of their organization. Track and report metrics like multifactor authentication (MFA) coverage, patch latency, incident counts, and incident response time to develop a comprehensive understanding of both your organization's potential vulnerabilities and its preparedness in the event of a cybersecurity incident.
- 2. Prioritize protecting identities**

Since identity is the top attack vector, enforce phishing-resistant multifactor authentication across all accounts, including administrative accounts.
- 3. Invest in people, not just tools**

Cybersecurity is a whole-of-organization effort. Find ways to upskill your workforce and consider making security part of performance reviews. Culture and readiness—not just technology—are primary factors in both an organization's defenses and its resilience.
- 4. Defend your perimeter**

A third of attackers use crude tactics as the easy path into an organization's exposed footprint, often looking beyond what you deploy to the vendors and supply chain you trust, including perimeter web-facing assets (18%), external remote services (12%), and supply chains (3%). Knowing the full scope of your perimeter, auditing the accesses you grant to trusted partners, and patching any exposed attack surface forces attackers to work harder to be successful.
- 5. Know your weaknesses and pre-plan for breach**

Combine knowledge of the organization's exposure footprint with organizational risk awareness to develop a proactive plan for responding to future breach. Tie security controls to business risks in terms the board can understand. Since a breach is a matter of when, not if, develop, test, and practice your incident response (IR) plan—including specific scenarios for ransomware attacks, which remain one of the most disruptive and costly threats to operations. How fast can you isolate a system or revoke credentials?
- 6. Map and monitor cloud assets**

Since the cloud is now a primary target for adversaries, conduct an inventory on every cloud workload, application programming interface (API), and identify within the organization, and monitor for rogue virtual machines, misconfigurations, and unauthorized access. At the same time, work proactively to enforce app governance, conditional access policies, and continuous token monitoring.
- 7. Build and train for resiliency**

If breaches are all but inevitable, resilience and recovery become key. Backups must be tested, isolated, and restorable, and organizations should have clear rebuild procedures for identity systems and cloud environments.
- 8. Participate in intelligence sharing**

Cyber defense is a team, not individual, sport. By sharing and receiving real-time threat data with peers, industry groups, and government, we can make it harder for cyber adversaries to achieve their goals.
- 9. Prepare for regulatory changes**

It's more important than ever for organizations to align with emerging laws like the European Union (EU) Cyber Resilience Act or United States (US) critical infrastructure mandates, which may require reporting cyber incidents within a certain timeframe or Secure by Design practices. These regulations reinforce the importance of timely incident reporting and stronger internal oversight of an organization's cybersecurity practices.
- 10. Start AI and quantum risk planning now**

Stay ahead of emerging technologies. Understand both the benefits and risks of AI use within an organization and adjust your risk planning, attack surface exposure, and threat models appropriately. Prepare for a post-quantum cryptography (PQC) world by taking the time to inventory where encryption is used and create a plan to upgrade to modern standards as they evolve.

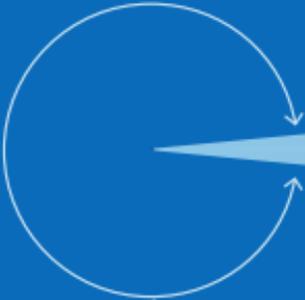
Microsoft Digital Defence Report

Identity, access, and the cybercrime economy

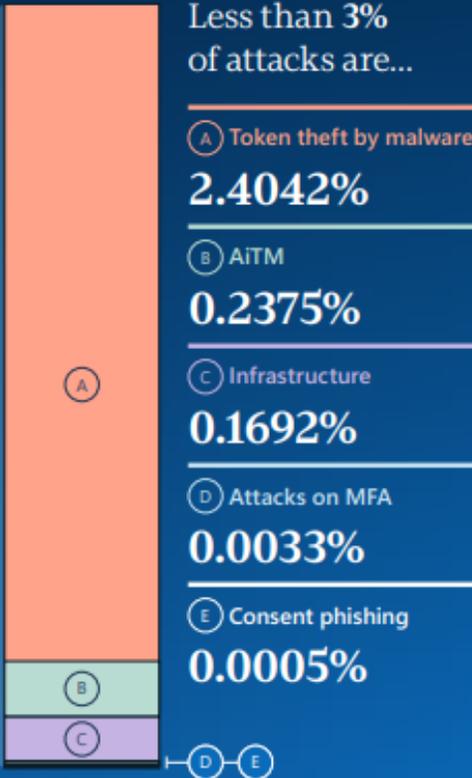
Identity attacks in perspective

Modern multifactor authentication still reduces the risk of identity compromise by more than **99%**.

While attacks against identity infrastructure (such as Microsoft Entra, Okta, Identity Provider (IdP), and hybrid components) are still limited in volume and are rare relative to other attacks, their variety is increasing. Novel attacks are continually being discovered, often targeting on-premises to cloud vertical attack paths.



More than **97%** of identity attacks are password spray or brute force attacks



Less than 3% of attacks are...

Source: Microsoft Defender XDR and Entra ID Protection alerts (April-June 2025)

Identity Categories in Microsoft 365



Identity Categories in Microsoft 365



Resource Mailboxes



Groups



Managed Identities



Contacts



SharePoint



Devices



Privileged Identities /
Directory Roles



External Identities (B2B/B2C)



Service Accounts – Service
Principals

**Each key is a potential
entry point for hackers**



40 %

...av de digitala identiteterna i Entra ID är inaktiva

2500 digitala identiteter

40% = 1000

20% = 500

10% = 250





Elisabeth Modig IT Driftchef i Västerköping

Ansvarstagande

Prestigelös

Vetgirig



Live Demo - Users

HA hallvard@bsuredemo.com

- bsure.
- Main Dashboard
- Users
 - Dashboard
 - Members
 - Guests
 - Data Quality
 - Properties
 - Sign-in Map
 - Sign-in Locations
 - Drilldown**
 - Microsoft Licences
 - Applications
 - Groups
 - Security
 - Devices
 - Customer Settings
 - Configuration
 - Book support
 - User Guides
 - Glossary
 - Documentation
 - Log Out

USERS – DRILLDOWN

User Guide
Filter Templates
Clear all slicers

Users

4 298

User Purpose

Alle

- Velg alt
- Guest
- Others
- Room
- Shared
- Unknown
- User

Created Date

06.02.2016 - 26.11.2025

Last Sign-in

01.03.2024 - 26.11.2025

User State

Active

Inactive

Sign-in Status

Never signed in

Signed In

Account

Disabled

Enabled

User Source

Cloud

On-premises

User Principal Name

Search

Focus Table

Evaluate potential d

User type details

User type	Users	%Users
Active Members	2 577	59,96%
Disabled Members	598	13,91%
Inactive Members	509	11,84%
Active Guests	404	9,40%
Inactive Guests	210	4,89%
Totalt	4 298	100,00%

Breakdown Table

Customize data with breakdown filter

Department	Users	%Users
Missing Data	1 149	26,73%
Finance	540	12,56%
Marketing	530	12,33%
Human Resources	525	12,21%
Operations	523	12,17%
Purchase	523	12,17%
Sales	508	11,82%
Totalt	4 298	100,00%

Breakdown Filter

Select property

- Country
- Company
- City
- Department
- Office
- Mail domain
- Manager name
- Job title
- Extension Attribute 1
- Extension Attribute 2

User Details Table

Use the column selector to customize how you view your data

User principal name	Created	Last sign in	Days since sign-in	Display name	User source	Manager	Sponsors	Coun
Jerry.Walker@bsuredemo.com	30.06.2020	01.03.2024	636	Jerry Walker	On-premises	Stetson Wilson	None	Franc
Dominik.Cross@bsuredemo.com	16.06.2021	01.03.2024	636	Dominik Cross	On-premises	Atticus Olsen	None	Engla
Ishaan.Sosa@bsuredemo.com	10.09.2022	07.03.2024	630	Ishaan Sosa	On-premises	Messiah Rice	None	Engla
Julia.Estrada@bsuredemo.com	31.05.2023	19.03.2024	618	Julia Estrada	On-premises	Taylor Watts	None	Norw.
James.Sullivan@bsuredemo.com	21.12.2023	22.03.2024	615	James Sullivan	On-premises	Taylor Watts	None	Norw.
Abigail.Castro@bsuredemo.com	21.10.2021	04.04.2024	602	Abigail Castro	On-premises	Emerson Krueger	None	Franc
Dakari.Paul@bsuredemo.com	07.07.2016	16.04.2024	590	Dakari Paul	On-premises	Emerson Krueger	None	Franc
Caleb.Chambers@bsuredemo.com	05.06.2016	19.04.2024	587	Caleb Chambers	On-premises	Liana Cabrera	None	Franc
Everest.Lewis@bsuredemo.com	18.04.2024	20.04.2024	586	Everest Lewis	On-premises	Daniella Dixon	None	Norw.
Iris.Sandoval@bsuredemo.com	10.09.2022	24.04.2024	582	Iris Sandoval	On-premises	Missing Data	None	Missir
Dexter.Garza@bsuredemo.com	23.11.2023	24.04.2024	582	Dexter Garza	On-premises	Fiona Vaughn	None	Norw.
Ian.Hill@bsuredemo.com	28.02.2024	24.04.2024	582	Ian Hill	On-premises	Liana Cabrera	None	Franc
Tadeo.Welch@bsuredemo.com	28.03.2024	25.04.2024	581	Tadeo Welch	On-premises	Messiah Rice	None	Engla
Cal.Rojas@bsuredemo.com	07.07.2016	03.05.2024	573	Cal Rojas	On-premises	Missing Data	None	Missir
Ivy.Young@bsuredemo.com	23.02.2024	05.05.2024	571	Ivy Young	On-premises	Taylor Watts	None	Norw.
Amiac.Hoffman@bsuredemo.com	03.10.2020	07.05.2024	569	Amiac Hoffman	On-premises	Frava Morales	None	Engla

Column Selector

Select properties

- Velg alt
- Created
- Last sign in
- Days since sign-in
- Display name
- User source
- Manager
- Sponsors
- Country
- Company
- Department
- Office
- Job title

Insights

- Find inactive and stale accounts
- Reveal identities with no owner or department
- Misconfigured identities
- Identify guest, shared mailboxes, room
- See who uses the environment — and who doesn't
- Detect high-risk identity entry points

Live Demo - Security

HA hallvard@bsuredemo.com

bsure.

Main Dashboard

Users

Microsoft Licences

Applications

Groups

Security

Dashboard

Authentication Methods

Entra ID Roles

Service Principals

Devices

Customer Settings

Configuration

Book support

User Guides

Glossary

Documentation

Log Out

www.bsure.io

User Guide

Filter Templates

SECURITY – AUTHENTICATION METHODS

Clear all slicers

Users Enabled 3 667	User Purpose Alle	Created Date 06.02.2016 - 26.11.2025	Last Sign-in 01.03.2024 - 26.11.2025	Sign-in Status <input type="checkbox"/> Never signed in <input type="checkbox"/> Signed In	MFA Reg <input type="checkbox"/> Usann <input type="checkbox"/> Sann	SSPR Reg <input type="checkbox"/> Usann <input type="checkbox"/> Sann	License Status <input type="checkbox"/> Licensed <input type="checkbox"/> Unlicensed	User is Admin <input type="checkbox"/> Usann	User Principal Name Search
---	-----------------------------	--	--	---	---	--	---	--	--------------------------------------

Focus table

Default MFA method

Main	Users	%Users
MFA Not Registered	2 301	62,75%
PhoneAppNotification	877	23,92%
Sms	430	11,73%
Fido2	55	1,50%
SoftwareOTP	3	0,08%
PhoneAppOTP	1	0,03%
Total	3 667	100,00%

Breakdown Table

Customize data with breakdown filter

Department	Users	%Users
Missing Data	1 052	28,69%
Finance	447	12,19%
Sales	443	12,08%
Operations	439	11,97%
Marketing	431	11,75%
Purchase	431	11,75%
Human Resources	424	11,56%
Total	3 667	100,00%

Breakdown Filter

Select property

- Country
- Company
- City
- Department
- Office
- Mail domain
- Manager name
- Job title
- Extension Attribute 1
- Extension Attribute 2

User Details Table

Use the column selector to customize how you view your data

User principal name	Created date	Last sign-in	Days since sign-in	User default MFA method	Mfa registered	SSPR registered	User preferred method	Syste
Jerry.Walker@bsuredemo.com	30.06.2020	01.03.2024	636	MicrosoftAuthenticatorPush	Sann	Sann	Push	Sann
Dominik.Cross@bsuredemo.com	16.06.2021	01.03.2024	636					
James.Sullivan@bsuredemo.com	21.12.2023	22.03.2024	615	None	Usann	Usann	None	Sann
Dakari.Paul@bsuredemo.com	07.07.2016	16.04.2024	590	MobilePhone	Sann	Sann	Sms	Sann
Dexter.Garza@bsuredemo.com	23.11.2023	24.04.2024	582	None	Usann	Usann	None	Sann
Ian.Hill@bsuredemo.com	28.02.2024	24.04.2024	582	MobilePhone	Sann	Sann	Sms	Sann
Tadeo.Welch@bsuredemo.com	28.03.2024	25.04.2024	581	MicrosoftAuthenticatorPush	Sann	Sann	Push	Sann
Reign.White@bsuredemo.com	05.06.2016	19.05.2024	557	None	Usann	Usann	None	Sann
Aurora.Lindsey@bsuredemo.com	30.06.2020	19.05.2024	557	MobilePhone	Sann	Sann	Sms	Sann
Abigail.Cummings_hotmail.com#EXT#@bsuredemo.onmicrosoft.com	25.01.2024	29.05.2024	547	None	Usann	Usann	None	Sann
Anders.Liu_gmail.com#EXT#@bsuredemo.onmicrosoft.com	20.05.2021	05.07.2024	510	None	Usann	Usann	None	Sann
Matias.Odonnell@bsuredemo.com	24.05.2024	07.07.2024	508	None	Usann	Usann	None	Sann
Amara.Whitaker@bsuredemo.com	11.07.2024	11.07.2024	504	MobilePhone	Sann	Sann	Sms	Sann
Andres.Short_gmail.com#EXT#@bsuredemo.onmicrosoft.com	27.02.2021	16.07.2024	499	None	Usann	Usann	None	Sann
Anaya.Jefferson_gmail.com#EXT#@bsuredemo.onmicrosoft.com	02.06.2024	27.07.2024	488	None	Usann	Usann	None	Sann
Amiri.Reed@bsuredemo.com	23.11.2023	16.08.2024	468	None	Usann	Usann	None	Sann

Column Selector

Select properties

- Velg alt
- Created date
- Last sign-in
- Days since sign-in
- User default MFA method
- Mfa registered
- SSPR registered
- User preferred method
- System preferred authentication
- Methods registered
- SSPR enabled
- System preferred authentication ...
- Admin role

Insights

- Expose users who can be breached
- Reveal accounts that attackers can take over from any device
- Identify identities with full data access but zero real protection
- Uncover privileged users without MFA
- Pinpoint the weakest entry points in your entire organization

Live Demo – Security – Entra ID Roles

bsure.

Main Dashboard

Users

Microsoft Licences

Applications

Groups

Security

Dashboard

Authentication Methods

Entra ID Roles

Service Principals

Devices

Customer Settings

Configuration

Book support

User Guides

Glossary

Documentation

Log Out

www.bsure.io

HA hallvard@bsuredemo.com

SECURITY – ENTRA ID ROLES

Filter Templates

Entities: 13

Entity Type: All (Velg alt, Group, ServicePr...)

Created Date: 06.02.2016 - 26.11.2025

Last Sign-in: 01.03.2024 - 26.11.2025

User State: Active, Inactive, Disabled, Enabled

Sign-in Status: Never signed in, Signed In

MFA Reg: Usa..., Sann

License Status: Licensed, Unlicensed

Entra Level: Alle

Principal Display Name: Search

Clear all slicers

Focus Table

Role	Entities
Active Entra ID	
User	
Directory Reac	3
Fabric Adminis	3
Global Admini	2
Global Reader	2
Application Administrator	1
Billing Administrator	1
Directory Synchronization Accounts	1
Directory Writers	1
Privileged Authentication Administrator	1
Privileged Role Administrator	1
Service Support Administrator	1
Total	13

Breakdown Table

Customize data with breakdown filter

Department	Entities	%Entities
	13	100,00%
Total	13	100,00%

Breakdown Filter

Select property

- Country
- Company
- City
- Department
- Office
- Mail domain
- Manager name
- Job title
- Extension Attribute 1
- Extension Attribute 2

Entity Details Table

Use the column selector to customize how you view your data

Principal display name	Role	Entity type	Entra level	User principal name	Created	Last sign in	Days since sign-in	Display name	User source	Ma
Pax8 GDAP Azure Admins @(\ Pax8 - Res...	Directory Readers	Group								
Pax8 GDAP Support Reader @(\ Pax8 - Re...	Directory Readers	Group								
Pax8 GDAP Privileged Access Admins @(\...	Directory Writers	Group								
Pax8 GDAP Support Reader @(\ Pax8 - Re...	Global Reader	Group								
Pax8 GDAP Privileged Access Admins @(\...	Privileged Authentication Administrator	Group								
Pax8 GDAP Privileged Access Admins @(\...	Privileged Role Administrator	Group								
Pax8 GDAP Support Reader @(\ Pax8 - Re...	Service Support Administrator	Group								
Microsoft.Azure.SyncFabric	Directory Readers	ServicePrincipal								
Test Olav	Application Administrator	User								
Olav Helland	Billing Administrator	User								
On-Premises Directory Synchronization ...	Directory Synchronization Accounts	User								
Adrian Flejszer	Fabric Administrator	User								
Dawid Jachowicz	Fabric Administrator	User								
Gunnar Weld	Fabric Administrator	User								
admingunnar without pbi license	Global Administrator	User								
Bsure Demo Admin	Global Administrator	User								

Column Selector

Select properties

- Velg alt
- Created
- Last sign in
- Days since sign-in
- Display name
- User source
- Manager
- Sponsors
- Country
- Company
- Department
- Office
- Job title

Insights

- Expose identities with dangerous, high-impact permissions
- Reveal accounts that could change or delete critical systems
- Identify privileged users with weak or missing protection
- Uncover roles that grant attackers full control if compromised
- Pinpoint the most powerful and risky identities in your organization

Live Demo – Security – Service Principals

bsure.

- Main Dashboard
- Users
- Microsoft Licences
- Applications
- Groups
- Security
 - Dashboard
 - Authentication Methods
 - Entra ID Roles
 - Service Principals**
 - Devices
 - Customer Settings
 - Configuration
 - Book support
 - User Guides
 - Glossary
 - Documentation
 - Log Out

www.bsure.io

SECURITY – SERVICE PRINCIPALS Clear all slicers

User Guide | Filter Templates

Service Principals: 35 | Last Sign-in Period: 26.11.2025 | Security Risk: All (Critical, High, Low, Medium) | Service Principal: Alle | Permission Value: Alle | Resource Name: Alle | Service Principal: Search

Focus Table
Additional filter options available

- Service Principal
- ArubaCentral
- AutoPilotRegistration
- AvePoint Cloud Backup for Azure VM
- AvePoint Online Services Administration for Office 365
- AvePoint Online Services Tenant Registration for Microsoft...
- Bedriftsnett Exchange sync
- Backup Exchange Sync
- Bsure-UMI-d2hkyocloqg
- ClearPass Intune Extension
- ClearPass-EntraID-Auth
- collector-m4srjgfybkye
- collector-ue6zrtqgsyod4

Principals Details Table
Use the column selector to customize how you view your data

Service principal	Risk	Permission	Permission value	Resource name
AvePoint Online Services Administration for Office 365	Critical	Create, edit, and delete items and lists in all site collections	Sites.Manage.All	Microsoft Graph
AvePoint Online Services Administration for Office 365	Critical	Have full control of all site collections	Sites.FullControl.All	Microsoft Graph
AutoPilotRegistration	High	Read and write Microsoft Intune configuration	DeviceManagementServiceConfig.ReadWrite.All	Microsoft Graph
AvePoint Cloud Backup for Azure VM	High	Manage app permission grants and app role assignments	AppRoleAssignment.ReadWrite.All	Microsoft Graph
AvePoint Cloud Backup for Azure VM	High	Read and write all administrative units	AdministrativeUnit.ReadWrite.All	Microsoft Graph
AvePoint Cloud Backup for Azure VM	High	Read and write all applications	Application.ReadWrite.All	Microsoft Graph
AvePoint Cloud Backup for Azure VM	High	Read and write all authentication method policies	Policy.ReadWrite.AuthenticationMethod	Microsoft Graph
AvePoint Cloud Backup for Azure VM	High	Read and write all directory RBAC settings	RoleManagement.ReadWrite.Directory	Microsoft Graph
AvePoint Cloud Backup for Azure VM	High	Read and write all groups	Group.ReadWrite.All	Microsoft Graph
AvePoint Cloud Backup for Azure VM	High	Read and write all users' authentication methods	UserAuthenticationMethod.ReadWrite.All	Microsoft Graph
AvePoint Cloud Backup for Azure VM	High	Read and write all users' full profiles	User.ReadWrite.All	Microsoft Graph
AvePoint Cloud Backup for Azure VM	High	Read and write directory data	Directory.ReadWrite.All	Microsoft Graph
AvePoint Cloud Backup for Azure VM	High	Read and write your organization's application configuration policies	Policy.ReadWrite.ApplicationConfiguration	Microsoft Graph
AvePoint Cloud Backup for Azure VM	High	Read and write your organization's authorization policy	Policy.ReadWrite.Authorization	Microsoft Graph
AvePoint Cloud Backup for Azure VM	High	Read and write your organization's conditional access policies	Policy.ReadWrite.ConditionalAccess	Microsoft Graph
Totalt				

Breakdown Table
Customize data with Breakdown Filter

Country	Entities
Norway	8
	4
Ireland	3
Germany	2
Netherlands	2
Totalt	18

Column Selector
Select properties

- Velg alt
- Risk
- Permission
- Permission value
- Resource name
- Permission description
- Principal id

Insights

- Expose apps and integrations with dangerous, unrestricted access
- Reveal automated accounts that no one monitors
- Identify services that can read, change, or delete critical business data
- Uncover permissions that would give attackers full control if exploited
- Pinpoint the hidden, always-on identities posing the highest risk

Live Demo – Applications – Applications Overview

HA hallvard@bsuredemo.com

User Guide

APPLICATIONS – APPLICATION OVERVIEW

Clear all slicers

Applications 1305
Microsoft Application No Yes
Application Used No Yes
User Sign-in No Yes
Latest User Sign-In 09.01.2025 26.11.2025
System Sign-in No Yes
Service Principal Type ManagedIdentity ServicePrincipal

Search
 Application Name
 Search

User Details Table
Use the column selector to customize how you view your data

Application name	Microsoft app	App used	User sign-in	Users count	Last user sign-in	System sign-in	Last system sign-in	Last serviceprincipal type	Applid
Office Online Service	No	Yes	Yes	1557	26.11.2025 09:59:34	No			e03a13ee-9730-4cae
Minecraft Education Edition Services	No	Yes	Yes	804	26.11.2025 09:59:40	No			16556bfc-5102-43c9-
ComplianceApp	No	Yes	Yes	749	26.11.2025 09:59:37	Yes	26.11.2025 09:20:34	ServicePrincipal	f5dd9677-caaf-403c-
RDS access2	No	Yes	Yes	725	26.11.2025 09:59:37	No			d7d65083-8a1e-40b0-
Microsoft Reflect and Insights	No	Yes	Yes	550	26.11.2025 09:58:52	No			f7691d3f-18be-4a7b-
ERP4	No	Yes	Yes	540	26.11.2025 09:59:06	No			b6c3e6b6-ba08-4067-
RDS access3	No	Yes	Yes	468	26.11.2025 09:58:27	No			df8e71a9-fc18-44ed-
Designer	No	Yes	Yes	369	26.11.2025 09:59:32	No			5e2795e3-ce8c-4cfb-
comtech5	No	Yes	Yes	300	26.11.2025 09:57:25	No			febfa82e-c9c2-4bac-
Ayfie Personal Assistant	No	Yes	Yes	191	26.11.2025 09:59:44	No			d598e835-8462-4b1f-
Pureservice SSO	No	Yes	Yes	158	26.11.2025 09:32:29	No			5aeeaf9a-efd5-427a-
App4	No	Yes	Yes	136	26.11.2025 09:59:39	No			fcc7828f-511c-4de5-
NanoLearning lesson report recipients	No	Yes	Yes	91	26.11.2025 09:54:30	No			79dbc9b2-b50d-405f-
Pureservice SSO OIDC	No	Yes	Yes	90	26.11.2025 09:58:32	No			7a97206d-2f2c-4c73-
ACOS Interact+ Front - Bsurre kommune	No	Yes	Yes	71	26.11.2025 09:51:35	Yes	26.11.2025 09:29:33	ServicePrincipal	8d4f8aea-8459-48e1-
App8	No	Yes	Yes	69	26.11.2025 09:55:39	No			b7f3f15a-0959-486e-
Microsoft Teams Analytics	No	Yes	Yes	55	26.11.2025 09:56:52	No			5a128dfa-2ded-4deb-
Apple Internet Accounts	No	Yes	Yes	54	26.11.2025 09:51:23	No			f8d98a96-0999-43f5-
Kahoot!	No	Yes	Yes	53	26.11.2025 08:06:12	No			8d7c2290-349a-4f07-
Loopfront	No	Yes	Yes	52	26.11.2025 09:43:51	No			d015e75c-6cb9-4839-
ERP2	No	Yes	Yes	47	26.11.2025 09:55:26	No			5a21082c-c5b0-499d-
Gemini Portal+	No	Yes	Yes	45	26.11.2025 09:55:10	No			bd80307f-a8ce-4585-
MapSystem Web	No	Yes	Yes	44	26.11.2025 09:53:37	No			68f4d117-942e-4399-
ERP1	No	Yes	Yes	41	26.11.2025 09:42:10	No			bb89a751-a31d-447e-
Acos Interact	No	Yes	Yes	32	26.11.2025 09:15:22	No			ba1c42cf-86c1-4edd-
App1	No	Yes	Yes	31	26.11.2025 09:58:00	No			a0fee855-394c-4757-
Arealplaner	No	Yes	Yes	31	26.11.2025 09:37:56	No			8fe8b171-89b8-419a-
ADlibizaUX	No	Yes	Yes	30	26.11.2025 18:49:28	No			74658136-14ec-4630-
App6	No	Yes	Yes	30	26.11.2025 09:48:32	No			c6b9c5c0-348a-4a64-
App10	No	Yes	Yes	25	26.11.2025 09:04:18	No			5431817e-104c-48e4-
App3	No	Yes	Yes	23	26.11.2025 09:50:22	No			847c1216-c5b6-4506-
Apps3	No	Yes	Yes	22	26.11.2025 09:59:37	No			a3e21bd9-590b-4d8f-
BookUp	No	Yes	Yes	22	26.11.2025 09:57:40	No			bd0ce3d6-b6b1-4ffb-

Column Selector
 Select column properties

- Velg alt
- Application name
- Microsoft app
- App used
- User sign-in
- Users count
- Last user sign-in
- System sign-in
- Last system sign-in
- Last serviceprincipal type
- Applid
- Tenantid

Insights

- Expose applications that still access your data — even if no one uses them
- Reveal unknown or forgotten apps operating inside your environment
- Identify systems that log in automatically without oversight
- Uncover apps with broad user access and no meaningful protection
- Pinpoint integrations that create hidden entry points for attackers

bsure.
 Main Dashboard
 Users
 Microsoft Licences
 Applications
 Usage
 Cost
 Sign-in Locations
Applications Overview
 Groups
 Security
 Devices
 Customer Settings
 Configuration
 Book support
 User Guides
 Glossary
 Documentation
 Log Out
 www.bsurre.io

Live Demo – Microsoft Licences – Drilldown

bsure.

Main Dashboard

Users

Microsoft Licences

Cost Dashboard

Licenses Overview

Subscription Overview

Inactive and Disabled Users

Overlapping Licenses

Cost Allocation

Drilldown

Price Settings

Applications

Groups

Security

Devices

Customer Settings

Configuration

Book support

User Guides

Glossary

Documentation

HA hallvard@bsuredemo.com

MICROSOFT LICENCES – DRILLDOWN

Users: 2 987 | Cost: kr 626,784 | User Purpose: Alle | Created Date: 06.02.2016 - 26.11.2025 | Last Sign-in: 01.03.2024 - 26.11.2025 | User State: Active, Inactive | Sign-in Status: Never signed in, Signed In | Account: Disabled, Enabled | User Principal Name: Search

Focus Table
Licenses assigned to a user

Licenses	Count	Cost
Microsoft 365 E3	576	205 440
Microsoft 365 F3	1 618	134 294
Microsoft 365 F5 Security Add-on	1 618	129 440
Microsoft 365 E5 Security	576	69 120
Microsoft 365 A3 for Faculty	727	53 798
Identity Threat Protection Faculty	708	24 780
Planner and Project Plan 3	16	4 960
Office 365 E3	12	2 880
Office 365 E1	16	1 040
Power BI Pro	4	372
Visio Plan 2	2	320
Total	15 633	626 784

Breakdown Table
Customize data with breakdown filter

Department	Count	Cost	Users	%Users
Missing Data	3 303	94 636	1 143	26,63%
Human Resources	2 043	91 639	525	12,23%
Sales	2 005	90 932	508	11,84%
Purchase	2 061	89 249	523	12,19%
Marketing	2 047	88 086	530	12,35%
Finance	2 132	87 414	540	12,58%
Operations	2 042	84 829	523	12,19%
Total	15 633	626 784	4 292	100,00%

Breakdown Filter
Select property

- Country
- Company
- City
- Department
- Office
- Mail domain
- Manager name
- Job title
- Extension Attribute 1
- Extension Attribute 2

User Details Table
Use the column selector to customize how you view your data

User principal name	Department	Created	Last sign-in	Days since sign-in	Cost	Licenses combined
Rowen.Zhang@bsuredemo.com	Finance	20.08.2022	26.11.2025	1	1 899	Microsoft 365 E3; Microsoft 365 E5 Security; Microsoft 365 F3; Microsoft 365 F5 Security Add-on; Micr
Cohen.Carson@bsuredemo.com	Human Resources	09.12.2016	26.11.2025	1	1 573	Microsoft 365 E3; Microsoft 365 E5 Security; Microsoft Power Automate Free; Planner and Project Plan
Ayla.Hubbard@bsuredemo.com	Human Resources	09.10.2024	26.11.2025	1	1 573	Microsoft 365 E3; Microsoft 365 E5 Security; Microsoft Power Apps for Developer; Microsoft Power Aut
Steven.Hayes@bsuredemo.com	Missing Data	25.04.2019	26.11.2025	1	1 573	Microsoft 365 E3; Microsoft 365 E5 Security; Microsoft Power Apps for Developer; Microsoft Power Aut
Lee.Arnold@bsuredemo.com	Operations	28.10.2018	26.11.2025	1	1 573	Microsoft 365 E3; Microsoft 365 E5 Security; Planner and Project Plan 3
Winter.Lynch@bsuredemo.com	Operations	06.02.2022	26.11.2025	1	1 573	Microsoft 365 E3; Microsoft 365 E5 Security; Microsoft Power Automate Free; Planner and Project Plan
Cassius.Maynard@bsuredemo.com	Purchase	05.06.2016	26.11.2025	1	1 573	Microsoft 365 E3; Microsoft 365 E5 Security; Microsoft Power Automate Free; Planner and Project Plan
Bianca.Buck@bsuredemo.com	Purchase	28.06.2024	26.11.2025	1	1 573	Microsoft 365 E3; Microsoft 365 E5 Security; Microsoft Fabric (Free); Microsoft Power Automate Free; Pl
Liliana.Mcdonald@bsuredemo.com	Finance	13.05.2017	26.11.2025	1	1 279	Microsoft 365 E3; Microsoft 365 E5 Security
Marcos.Schmidt@bsuredemo.com	Operations	20.01.2022	26.11.2025	1	1 279	Microsoft 365 E3; Microsoft 365 E5 Security; Microsoft Power Automate Free
Israel.Payne@bsuredemo.com	Purchase	09.07.2020	26.11.2025	1	1 279	Microsoft 365 E3; Microsoft 365 E5 Security; Microsoft Power Automate Free
Brielle.Esquivel@bsuredemo.com	Purchase	28.08.2024	07.11.2025	20	1 279	Microsoft 365 E3; Microsoft 365 E5 Security; Microsoft Power Automate Free
Oakley.Duncan@bsuredemo.com	Sales	09.08.2023	26.11.2025	1	1 279	Microsoft 365 E3; Microsoft 365 E5 Security; Microsoft 365 F3; Microsoft 365 F5 Security Add-on
Trey.English@bsuredemo.com	Human Resources	05.06.2016	26.11.2025	1	1 273	Microsoft 365 E3; Microsoft 365 E5 Security; Visio Plan 2
Winston.Ware@bsuredemo.com	Missing Data	20.05.2021	26.11.2025	1	1 120	Microsoft 365 E3; Microsoft 365 E5 Security; Microsoft Power Automate Free; Power BI Pro
Total					626 784	

Column Selector
Select properties

- Velg alt
- Created
- Last sign-in
- Days since sign-in
- Cost
- Licenses combined
- License in rows
- User source
- Display name
- Manager
- Country
- Company
- Department

Insights

- Identify licenses paid for but not actively used
- Reveal users with expensive licenses they don't need
- Uncover duplicated or overlapping license assignments
- See which departments drive the highest cost
- Find users who haven't signed in for months — but still cost money

Want to Discover Your Identity Blind Spots?

-  **Full identity visibility** Know exactly what you have
-  **Security improvements** You can't protect what you can't see
-  **Cost savings** Cut unnecessary license spend
-  **High-risk misconfigurations** Find dangerous setups instantly
-  **Clear, prioritized actions** Know what to fix, and in what order

Don't wait for an incident — take control now



Tack för mig! 😊

*"NÄR VI SER VERKLIGHETEN SÅDAN SOM DEN ÄR OCH HAR
MODET ATT GÖRA NÅGOT ÅT DEN, BÖRJAR VÄGEN MOT
ETT SÄKRARE OCH MER KOSTNADSEFFEKTIVT MOLN"*

gustav@bsure.se

073 985 66 33

www.linkedin.com/in/gustav-jannerland/

bsure.