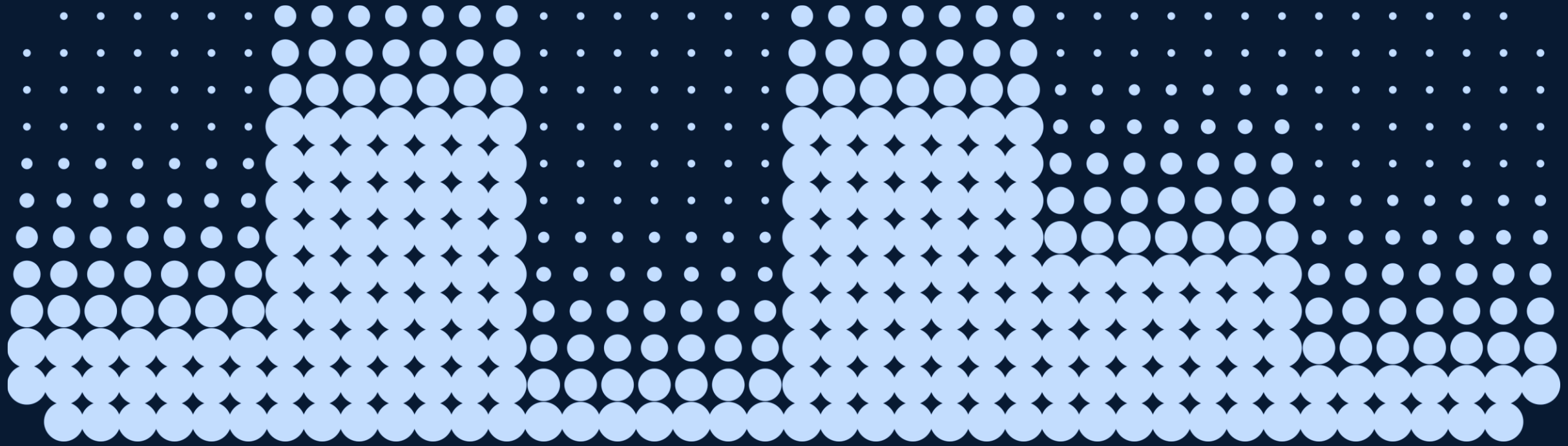


Attackers don't break in, they log in

Webinar 28. November 2025

Hallvard Eide, Co-Founder Bsure

bsure.

"INNSIKT OG ANALYSE AV EGNE DATA KOMBINERT MED KOMPETANSE OG ERFARING GIR ALLTID BEDRE BESLUTNINGER."

bsure.

hallvard.eide@bsure.no

Microsoft Digital Defense Report

Source: www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

bsure.

Microsoft - Top Recommendations from Microsoft

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 identity 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 clean 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.

Source: www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

bsure.

Microsoft - Strategic Cybersecurity

Hierarchy of cybersecurity needs

Drawing inspiration from Maslow's hierarchy of needs, this graphic illustrates a prioritization of cybersecurity, starting with the most basic need: protecting identities. AI has a role at each tier, underscoring its potential to enhance security measures. Cultivating a robust security culture within the organization, helps ensure the technological defenses and human practices evolve in concert to mitigate threats effectively.

AUTOMATE SECURITY OPERATIONS
Automating security operations is the holistic approach to building on perspectives and insights across all layers in the pyramid.

IMPACT...
Automating processes at scale creates new opportunities for insights as well as relief for stressed defenders.

DETECT AND REMEDIATE THREATS
Monitoring your ecosystem to identify anomalous activity and contain threats.

IMPACT...
The ability to identify and respond quickly can limit lateral movement, contain damage to assets and deny persistence.

SECURE DIGITAL ASSETS
Digital assets, whether code, traditional data stores, and now generative AI models are all key components of modern workloads.

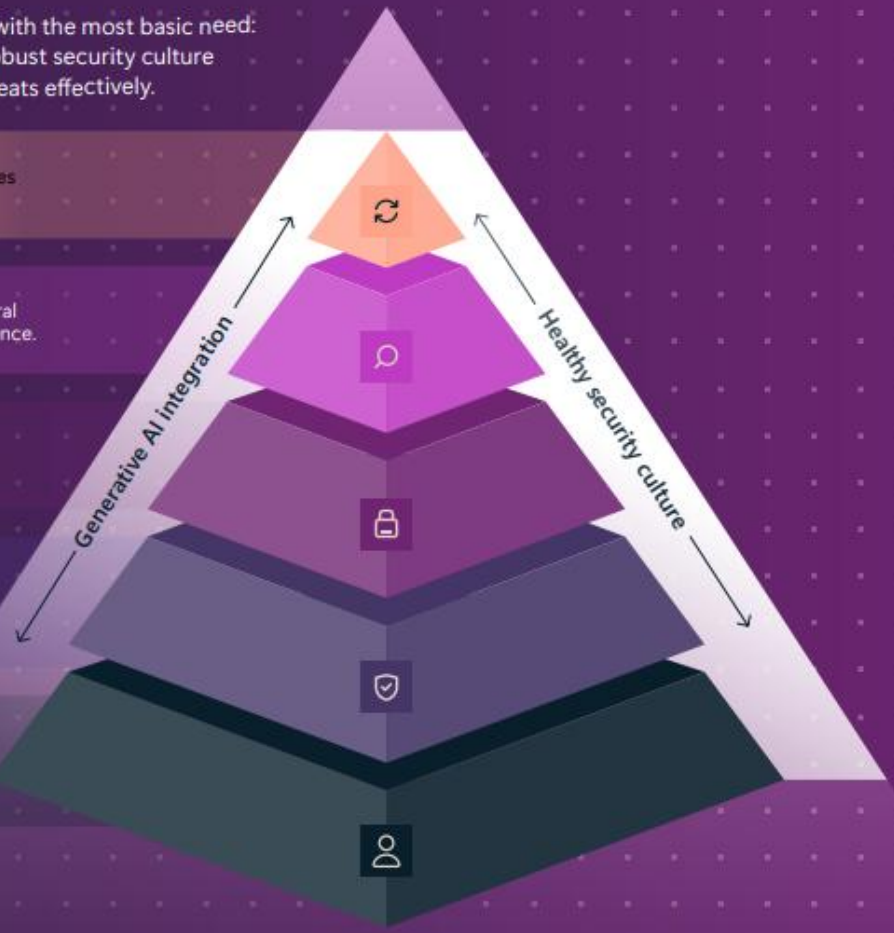
IMPACT...
Modern workloads deliver the value-add to end users who increasingly rely on their integrity and availability.

PROTECT ENDPOINTS
Protected endpoints include the multiple dimensions of devices in use today – from PCs and mobile devices, to network and operational technology (OT), and servers in datacenters.

IMPACT...
Effective endpoint protection can limit the repercussions of unauthorized access.

PROTECT IDENTITIES
"Attackers don't break in, they log in." Credentials for both individuals and machines are the perimeter of the modern attack surface.

IMPACT...
Strong identity security can greatly reduce risk exposure—particularly for ransomware attacks.

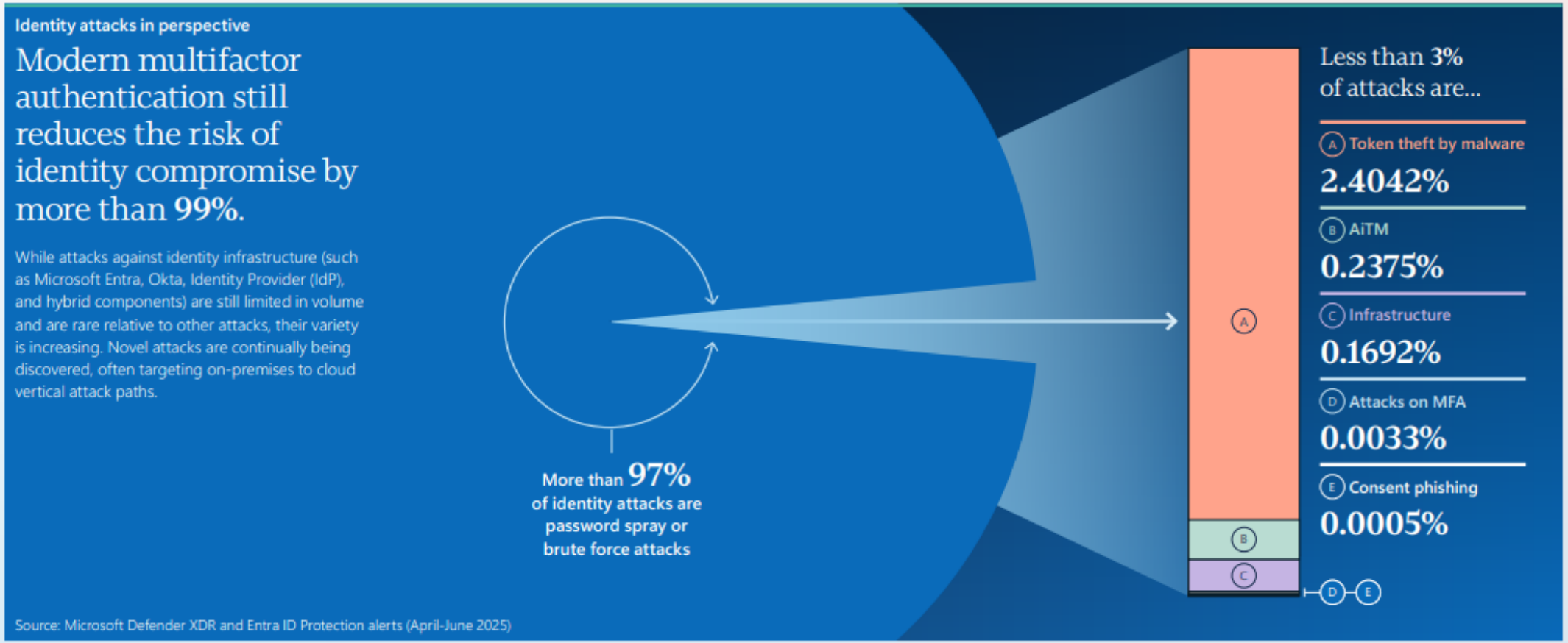


Source: https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024

bsure.

Microsoft Digital Defence Report

Identity, access, and the cybercrime economy



Source: www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

bsure.

Identity Categories in Microsoft 365

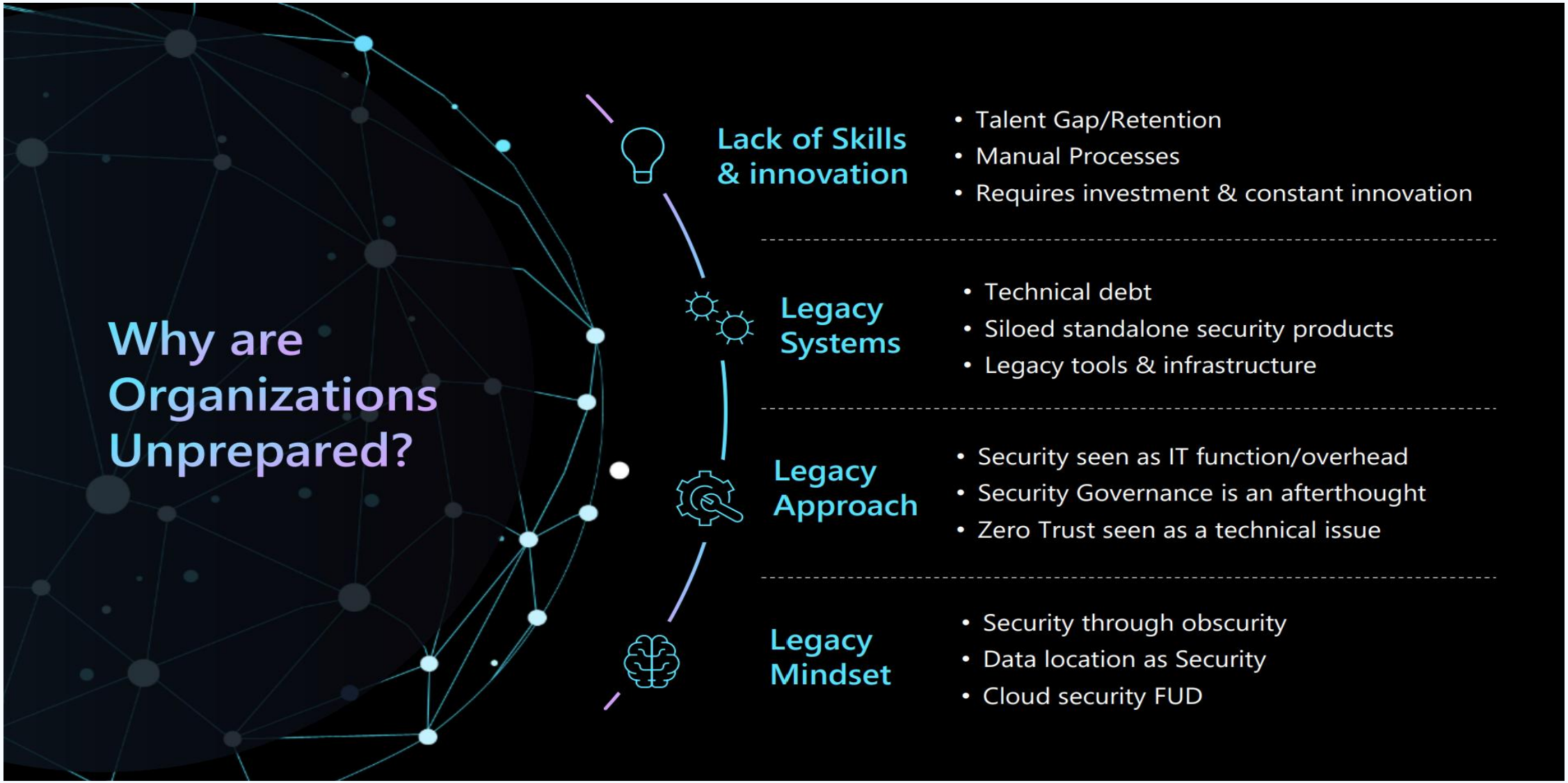
bsure.

Identity Categories in Microsoft 365

Category	Description	Examples
Users	Standard identities for people, both internal and external.	Employees, guest users, synced AD users
Resource Mailboxes	Created as user objects but function as Exchange resources.	Meeting rooms, equipment, shared mailboxes
Service Accounts – App Registrations	Identities for applications you create in the tenant.	Custom apps, internal integrations
Service Accounts – Service Principals	The actual identity apps use to sign in.	Microsoft 365 apps, third-party integrations, automation services
Managed Identities	Identities for Azure resources without passwords/secrets.	Azure Functions, VMs, Logic Apps
Groups	Used for access control, security, and Microsoft 365 features.	Microsoft 365 Groups, Security Groups, Dynamic Groups
Devices	Identities for devices registered or managed in the tenant.	Azure AD Joined PCs, Hybrid Joined devices, mobile devices, BYOD
Contacts	External contacts stored in the directory, often for mail routing.	Mail contacts, external distribution contacts
Privileged Identities / Directory Roles	Role-based identities attached to users or service principals (not standalone objects).	Global Admin, Security Admin, PIM-activated roles
External Identities (B2B/B2C)	External identities authenticated by another identity provider.	Partners, customers, suppliers in B2B scenarios

bsure.

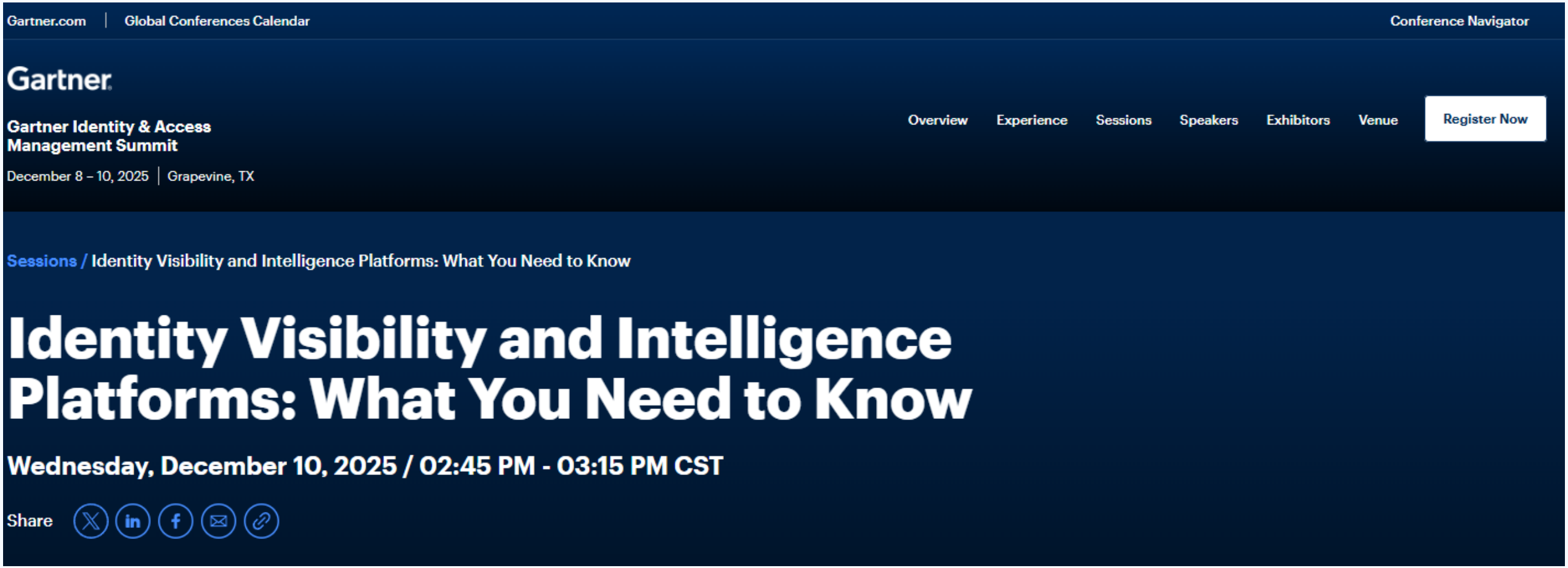
Microsoft - Why are organizations unprepared?



Source: Ole Tom Seierstad - Microsoft Norge

bsure.

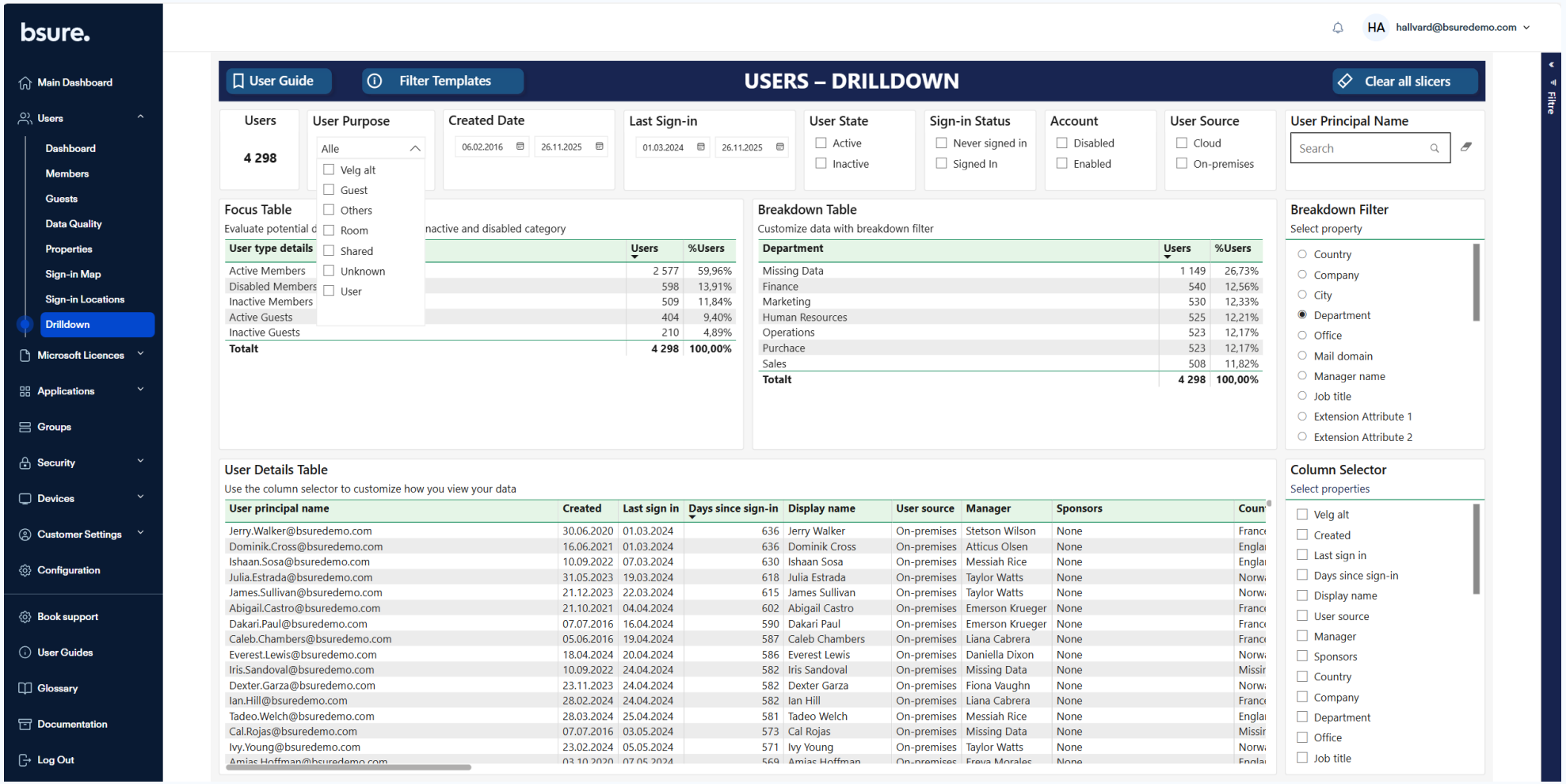
Gartner - Identity Visibility and Intelligence Platforms



Source: www.gartner.com/en/conferences/na/identity-access-management-us/sessions/detail/4046022-Identity-Visibility-and-Intelligence-Platforms-What-You-Need-to-Know

bsure.

Live Demo - Users

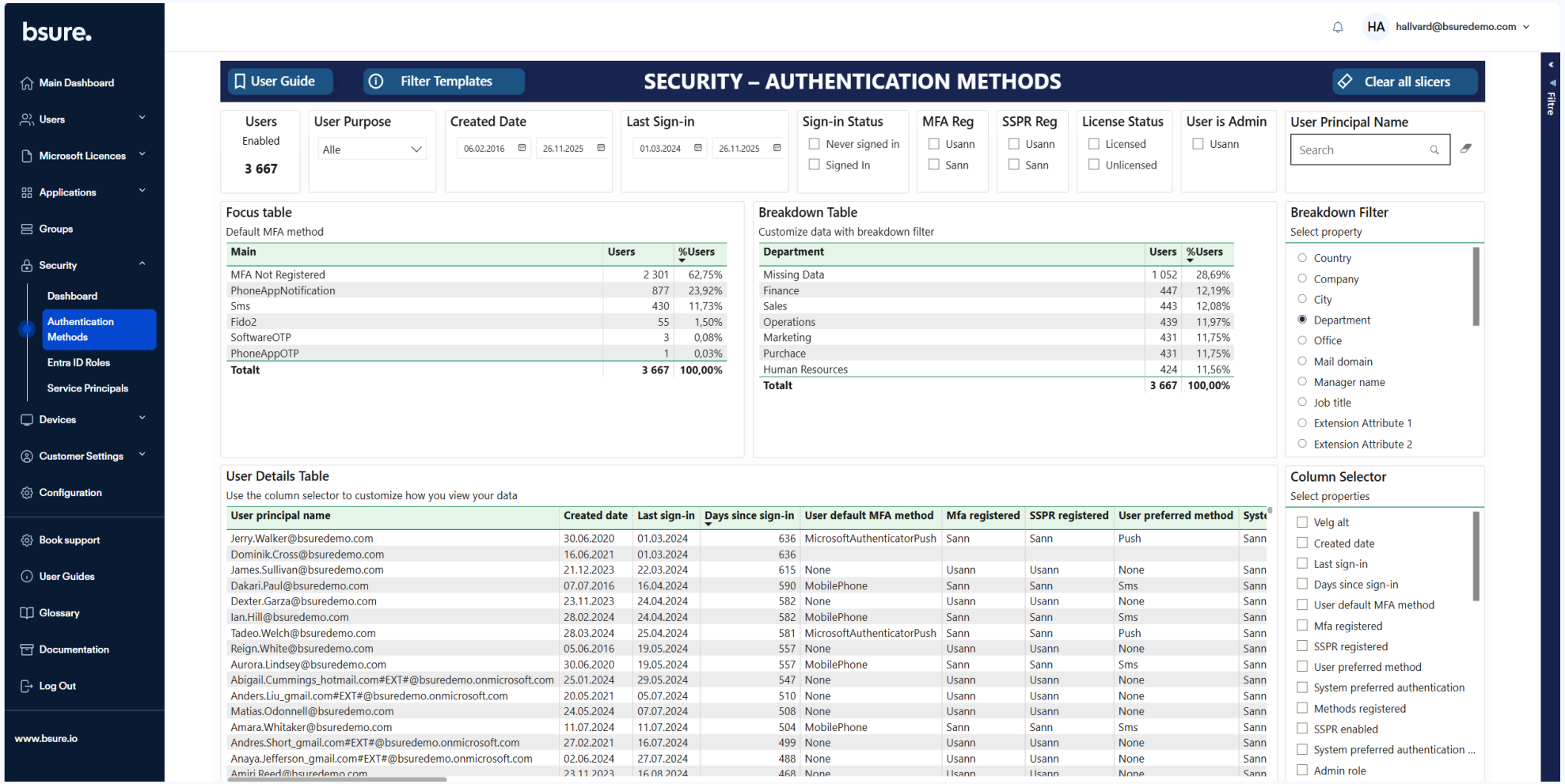


Insights

- 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

bsure.

Live Demo - Security

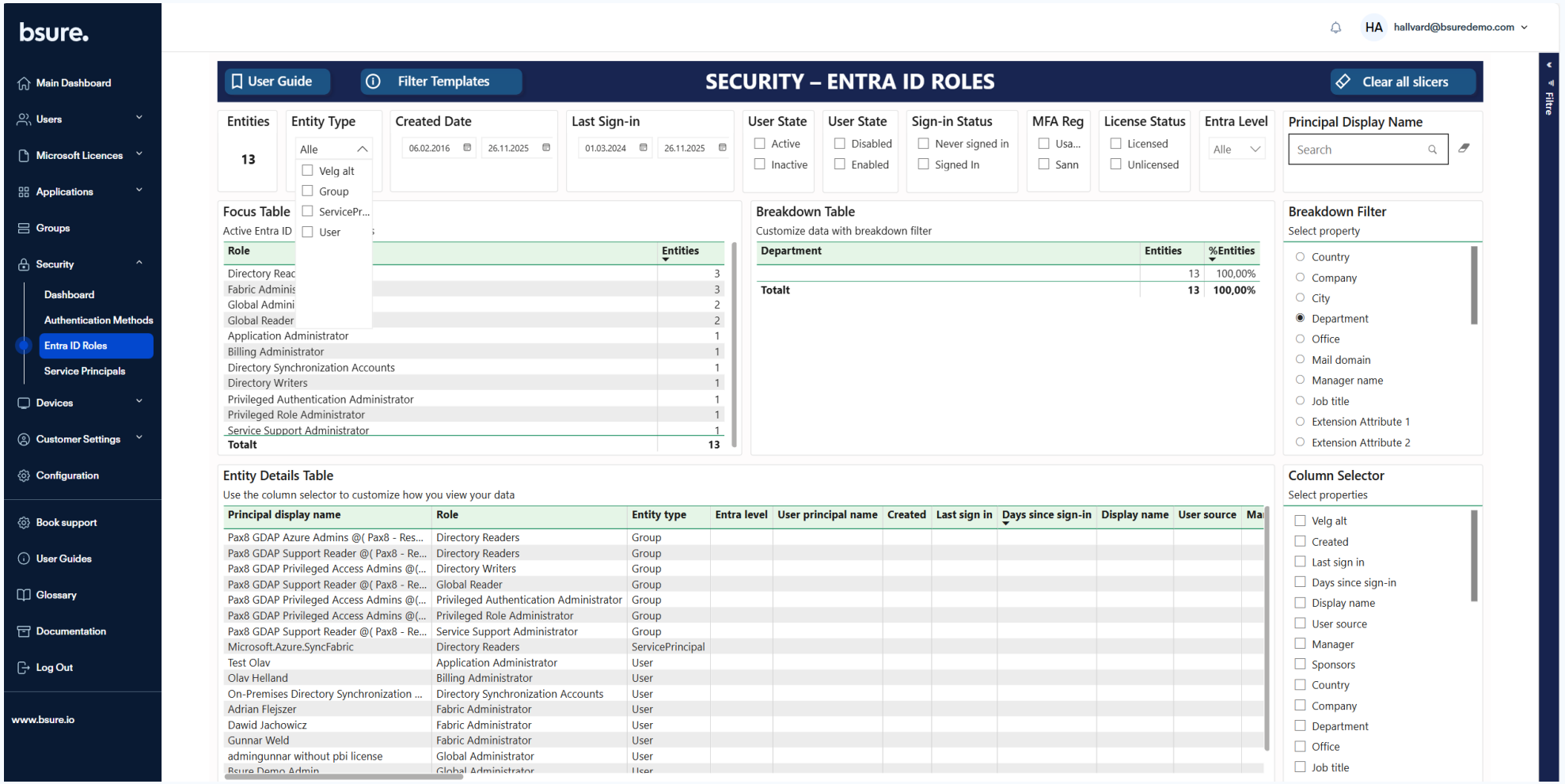


Insights

- 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

bsure.

Live Demo – Security – Entra ID Roles

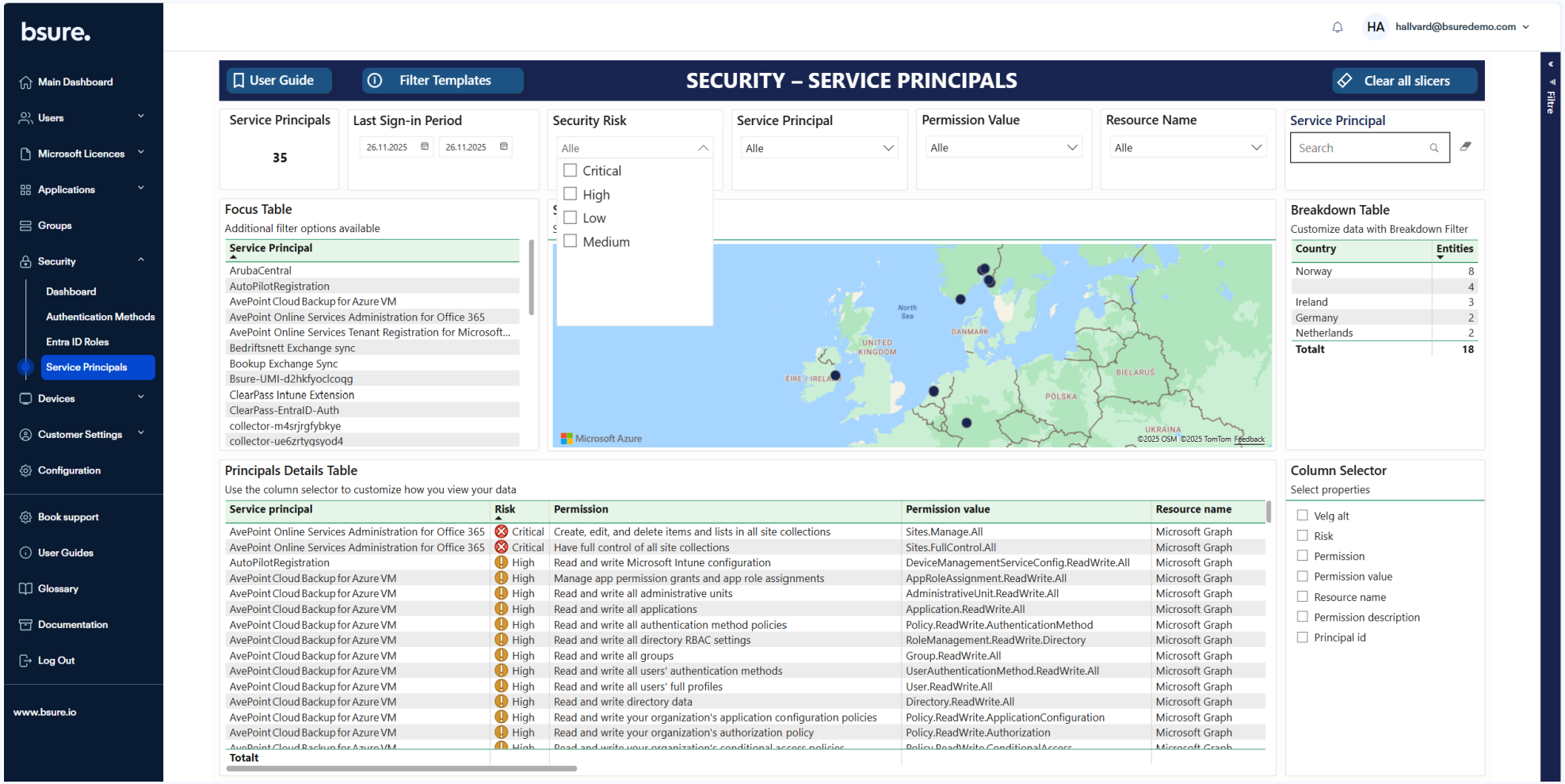


Insights

- 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

bsure.

Live Demo – Security – Service Principals

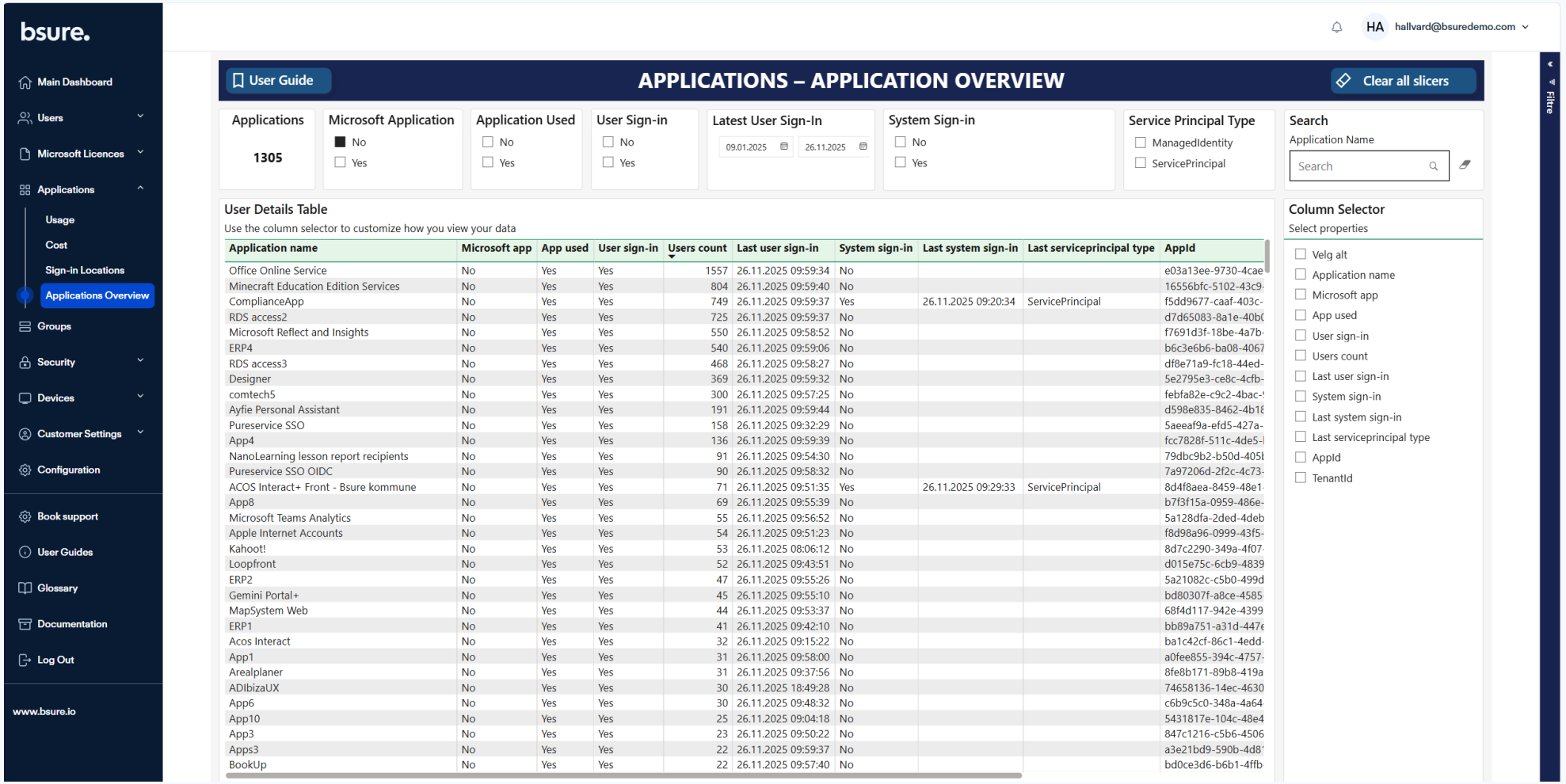


Insights

- 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

bsure.

Live Demo – Applications – Applications Overview

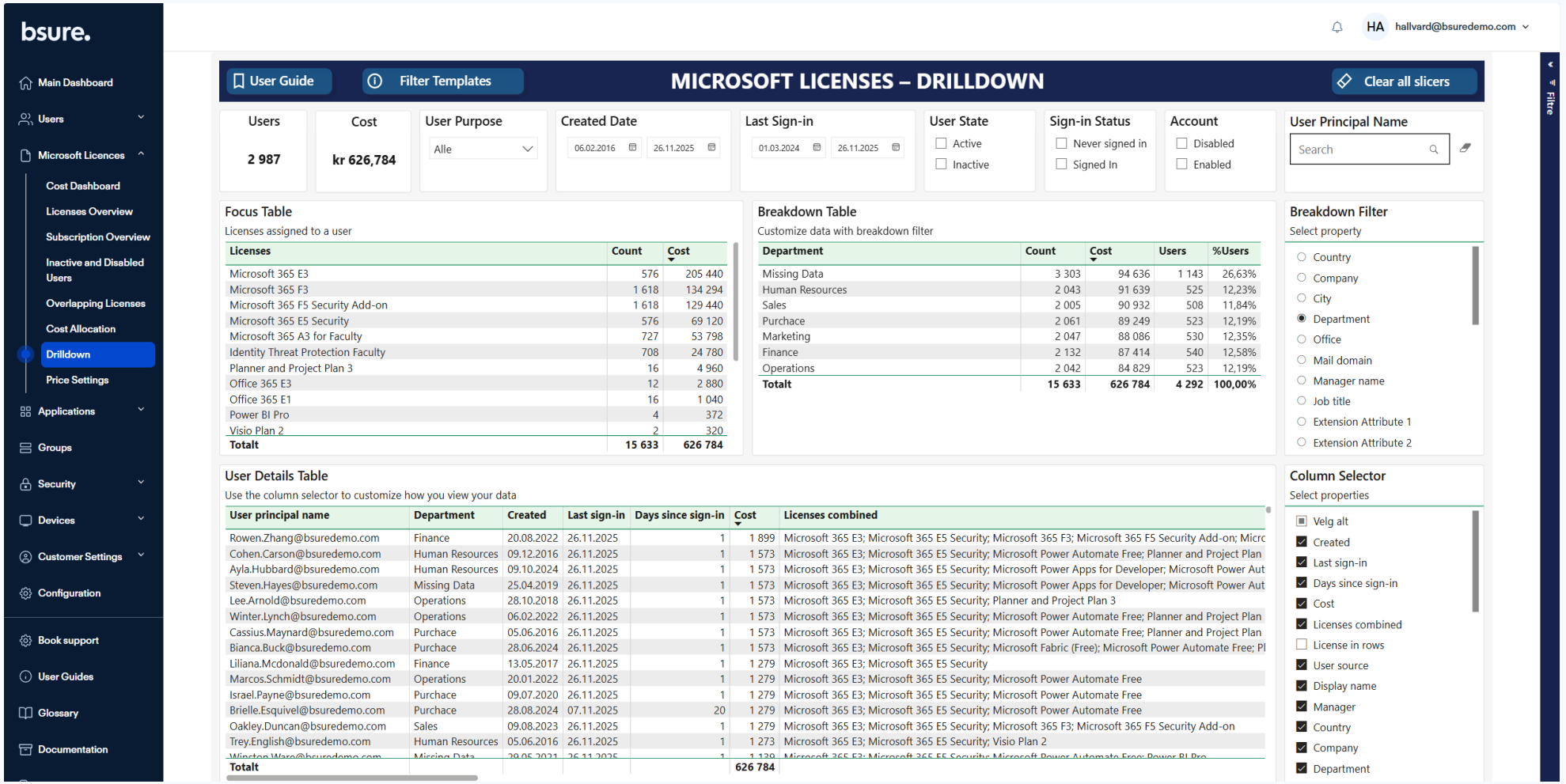


Insights

- 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.

Live Demo – Microsoft Licences – Drilldown



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

bsure.

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

bsure.

Takk for meg ☺

"INNSIKT OG ANALYSE AV EGNE DATA
I KOMBINASJON MED KOMPETANSE OG ERFARING
BIDRAR ALLTID TIL BEDRE BESLUTNINGER."

bsure.