DigitalBunker365

Montana Primary Care Association

June 13th 2024

Jason Pomaski, MBA, CISSP
Virtual CISO

DigitalBunker365

Microsoft 365 Made Simple & Secure

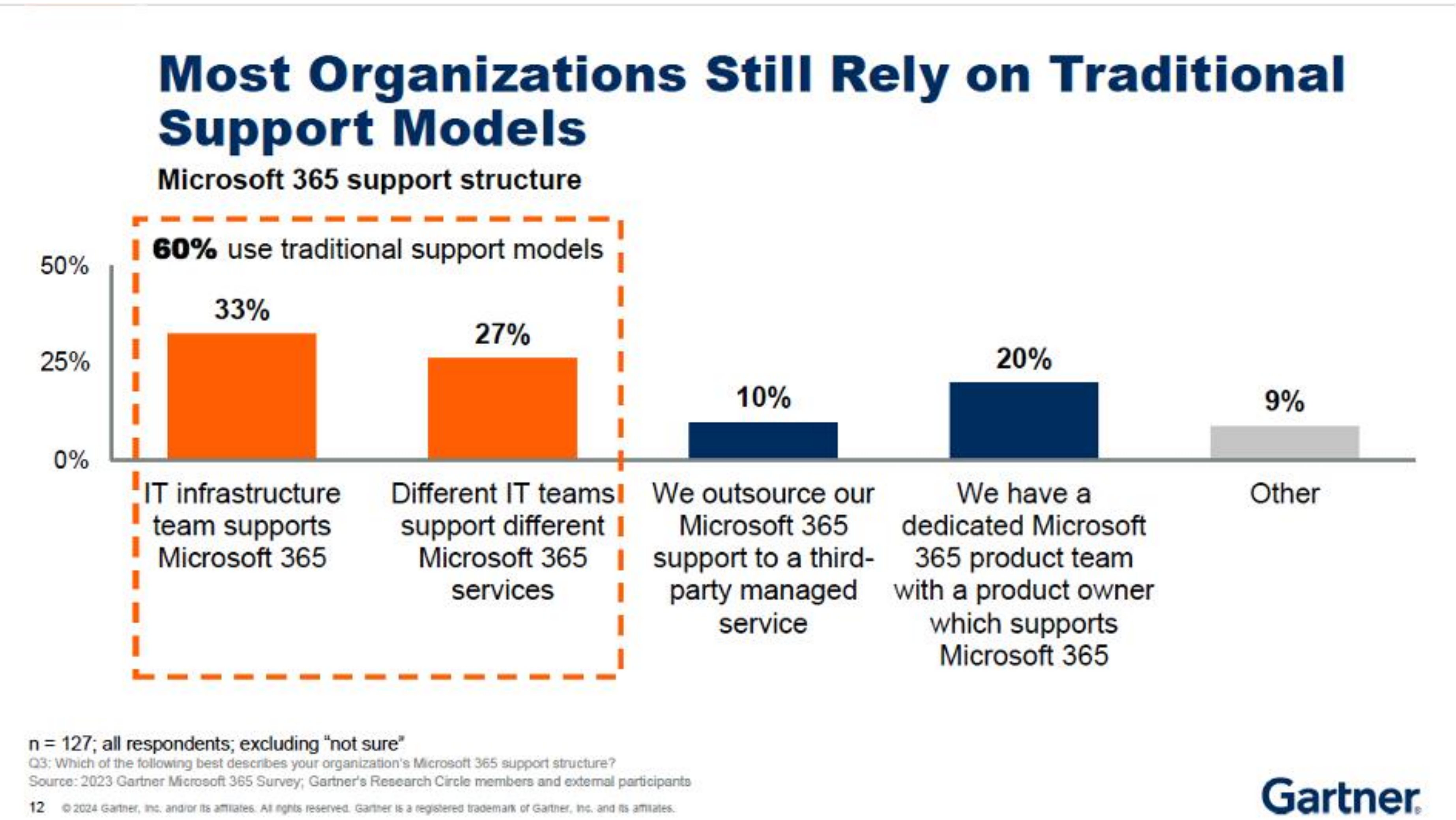
We Manage Complexity - You Focus on Business

Microsoft 365
Management Made Simple

Security & Compliance
Security Made Simple

Business Automation
Provisioning Made Simple

Flat Pricing
Made Simple



Most Organizations Still Rely on Traditional Support Models

Microsoft 365 support structure

n = 127; all respondents; excluding "not sure"

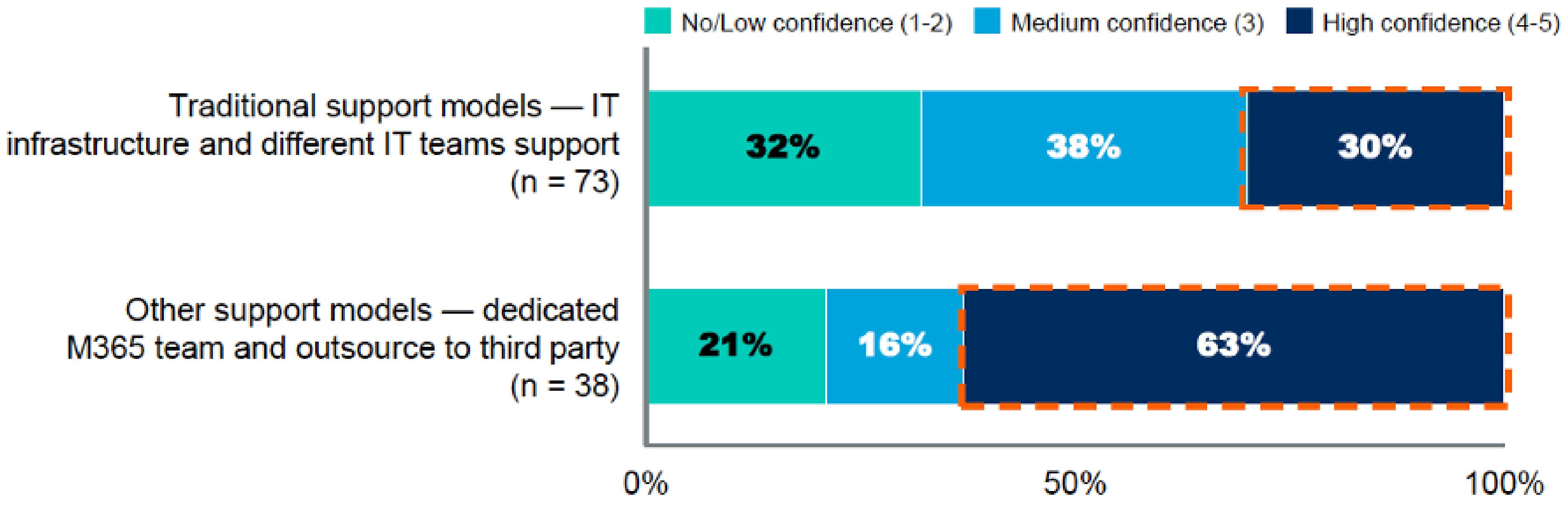
Q3: Which of the following best describes your organization's Microsoft 365 support structure?

Source: 2023 Gartner Microsoft 365 Survey; Gartner's Research Circle members and external participants

Traditional Support Models Do Not Work With Microsoft 365

Level of confidence in the organization's Microsoft 365 support model

Scale: 1 — no confidence to 5 — high confidence



n = varies, excluding "not sure"

Q: Which of the following best describes your organization's Microsoft 365 support structure?

Q: Do you have confidence that your organization has the right support model in place to succeed with Microsoft 365?

Source: 2023 Gartner Microsoft 365 Survey; Gartner's Research Circle members and external participants

Gartner

The Challenge of Microsoft 365:

Complexity

- Hundreds of configurable controls
- Keeping pace with new features
- Shared Responsibility Gaps
- Consistency of enterprise permissions
- Backups must be properly configured
- Maintaining and securing legacy platforms including point solutions.
- Data management and classification
- Hybrid deployments

Security & Regulatory Compliance

- Healthcare
- Financial Services
- Real Estate
- Government
- Generative AI unknowns

Productivity

- Hybrid Workplace
- Onboarding staff quickly
- Offboarding securely
- Use of BYOD
- Getting the most out of Microsoft 365
- Collaboration
- Document / Version Control

Resource Contention

- Ownership and Accountability
- Resource constrained IT team
- Continuous Learning Requirements
- IT is not aligned to business objectives or priorities

Why Digital Bunker 365:

Easy Onboarding with Assessment & Remediation

- Assess and report on Microsoft 365 environment
- Triaged Remediation Roadmap
- Project Management of Remediation Plan
- Implementation of Remediation Plan

Platform Implementation

- Architect Customer Environment
- Onboard customer to platform

Security & Compliance

- Configure and manage Entra Identity and Access Management (IAM)
- Monitor security controls and events
- Generate automated alerts
- Continuous enforcement of over 125 controls
- Alignment with organization’s Policies, Procedures, and Process.
- Independent third-party oversight

Microsoft 365 Experts

- Configure and manage Microsoft Exchange, SharePoint, Teams and OneDrive
- Manage Files/Directories and data classification
- Manage backups and data retention
- Business automation - Onboarding / Offboarding of staff
- Expert's Expert

Customer Engagement

- Secure Customer Portal
- Help Desk
- Automated Change Control Request and Approval Process
- Monthly reviews including security assessment reports and associated remediation.
- Customer Dashboard
- Custom Alerting and Monitoring

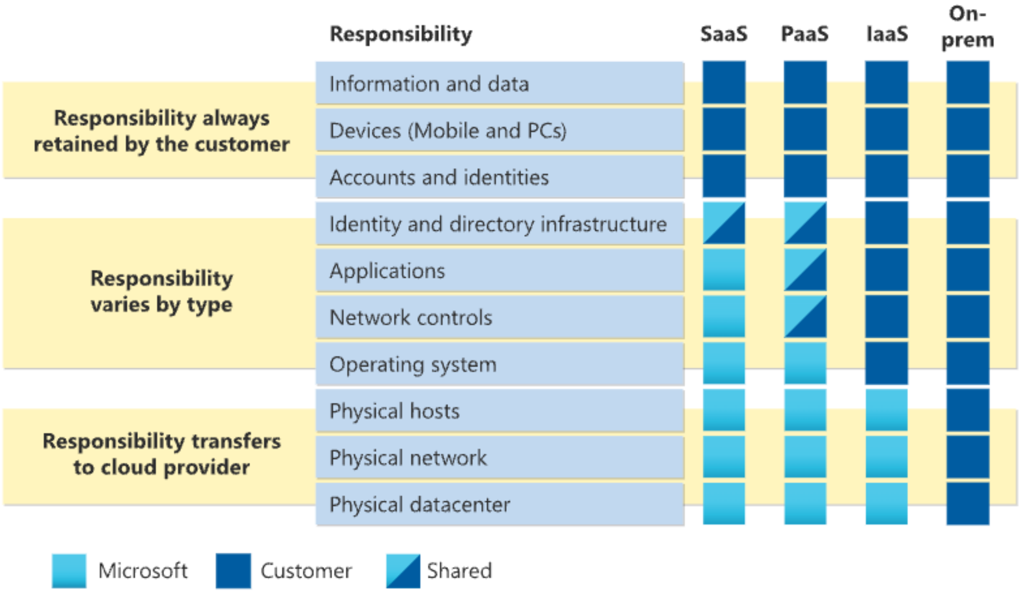
Navigating Shared Responsibility:

Client Responsibility

- Assess and report on Microsoft 365 environment
- Triaged Remediation Roadmap
- Project Management of Remediation Plan
- Implementation of Remediation Plan

Digital Bunker 365 Responsibilities

- Assess and report on Microsoft 365 environment
- Triaged Remediation Roadmap
- Project Management of Remediation Plan
- Implementation of Remediation Plan



	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	■	■	■	■
	Devices (Mobile and PCs)	■	■	■	■
	Accounts and identities	■	■	■	■
Responsibility varies by type	Identity and directory infrastructure	◩	◩	■	■
	Applications	□	◩	■	■
	Network controls	□	◩	■	■
	Operating system	□	□	■	■
Responsibility transfers to cloud provider	Physical hosts	□	□	□	■
	Physical network	□	□	□	■
	Physical datacenter	□	□	□	■

□ Microsoft ■ Customer ◩ Shared

DigitalBunker365

Managing Complexity

```
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
 operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

selection at the end -add
 _ob.select= 1
ier_ob.select=1
ntext.scene.objects.active
("Selected" + str(modifier
irror_ob.select = 0
 bpy.context.selected_ob
ata.objects[one.name].se

int("please select exactly

 OPERATOR CLASSES ----

types.Operator):
 X mirror to the selected
ject.mirror_mirror_x"
ror X"

context):
xt.active_object is
```

- Assess and Remediate
- Implementation
- Manage Multifactor Authentication (MFA)
- Establish Access Controls
- Create Conditional Access Policies
- Establish Compliance Protocols
- Spam Filtering
- Phishing Detection and Prevention
- Data Loss Prevention (DLP) Policies
- Email Spoofing Protection (SPF, DKIM, DMARC)
- Email Content Filtering
- Attachment Scanning for Malware
- Block Executable File Attachments
- Implement Email Archiving
- Monitor and Analyze Email Logs
- Secure Email Gateway
- Automatic Forwarding Restrictions
- Enforce Strong Password Policies
- Audit Email Access and Usage
- Retention Policies for Emails
- Email Encryption
- Access Control for Sensitive Emails
- Disable Auto-Download of Email Attachments
- Monitor for Unusual Email Activity
- Quarantine Suspicious Emails
- Whitelisting and Blacklisting of Email Addresses
- Backup Solutions
- Email Account Compromise Detection
- Manage Email Protocols
- Monitor for Outbound Data Exfiltration
- Restrict External Email Access
- Implement Advanced Threat Protection (ATP)
- Regularly Update Email Security Policies
- Protect Against Business Email Compromise (BEC)
- Use Secure Links in Emails
- Use Secure Links in Emails
- Restrict Email Access on Mobile Devices
- Secure Email Client Configurations
- Monitor Email Flow for Anomalies
- Manage Use of Trusted Email Domains
- Limit Email Attachment Size
- Implement Email Sender Verification
- Restrict Administrative Access to Email Settings
- Disable Email Auto-Reply to External Addresses
- Enable Audit Logging for Email Admin Activities
- Secure Email Distribution Lists
- Configure Email Alerts for Suspicious Activities
- Monitor Email Bounce-Backs
- Implement Role-Based Access Control (RBAC) for Email
- Protect Against Email Address Harvesting
- Deploy Anti-Malware Solutions for Email
- Conduct Regular Email Security Audits
- Restrict Email Use for Critical Communications Only
- Monitor Email Metadata for Anomalies
- Implement Least Privilege for Email Access
- Ensure Secure Email Deletion Practices
- Regularly Test Email Security Controls
- Enforce Secure Email Usage Policies
- Protect Email Accounts with Conditional Access
- Review and Update Email Security Configurations Periodically
- Monitor and Control Third-Party Email Integrations
- Implement Strong Email Authentication Methods
- Enable Email Notifications for Security Events
- Ensure Compliance with Email Retention Laws
- Secure Shared Email Inboxes
- Implement Geo-Fencing for Email Access
- Enforce Use of Secure Email Clients
- Regularly Review and Purge Inactive Email Accounts
- Dashboards
- Ticketing System

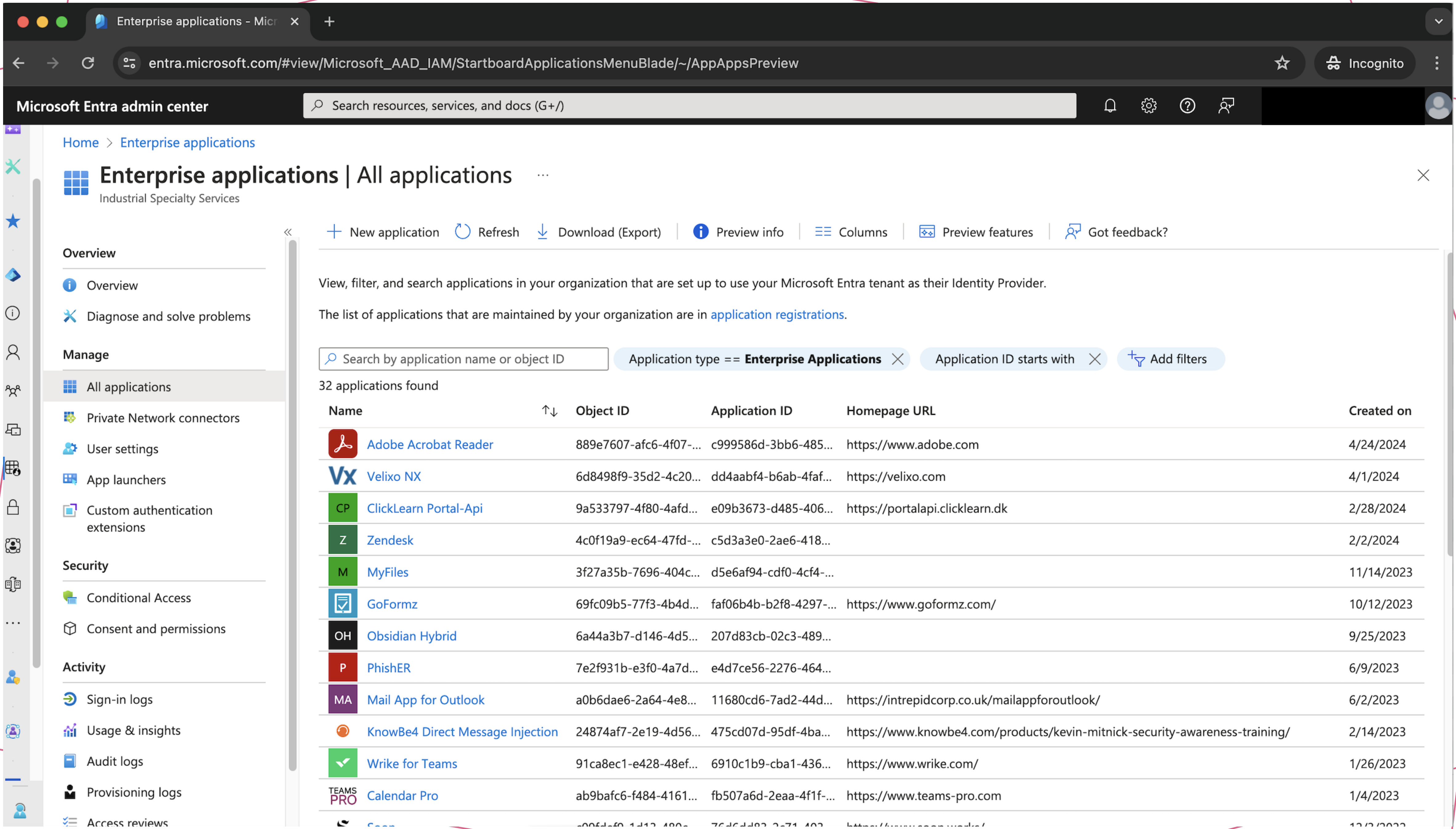
VALUE ADD SPECIFIC TO MTPCA MEMBERS

- In-kind of up to four hours per week of Microsoft 365 consulting
- Navigating Microsoft including accessing non-profit pricing and getting value from not-for-profit offerings. This includes the free $3500 of Azure credit per year.
- Addressing Gaps including Multi-Factor authentication for VPN access and roadmap to Zero Trust.
- Best practice in helping people understand where the data goes and how to manage that to keep it easy to find and secure
- HIPAA monitoring configuration from within Microsoft 365. Same for MT
- Securing the M365 environment/identity management
- Piloting Defender for automated response
- Piloting Vulnerability scans and Automated updates
- Incorporation of CISA SCuBA baseline

Montana Primary Care Association

KEY TAKEAWAYS AND GO DOES

- Check all aspects of Enterprise Applications
- Conditional Access Polices are awesome, especially Risky User / Logon
- SMS and Voice as MFA methods need to be phased out Microsoft 365
- Don’t afraid to ”break some eggs” addressing issues. Speed is important.
- Build a non-punitive culture for reporting and addressing security issues.
- Monitoring and Managing Microsoft 365 is an ongoing process.
- Phase out ADFS ASAP
- Schedule a complimentary workshop



Enterprise applications - Micr
entra.microsoft.com/#view/Microsoft_AAD_IAM/StartboardApplicationsMenuBlade/~/AppAppsPreview
Incognito
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Home > Enterprise applications

Enterprise applications | All applications

Industrial Specialty Services

+ New application
Refresh
Download (Export)
Preview info
Columns
Preview features
Got feedback?
Overview
Overview
Diagnose and solve problems
Manage
All applications
Private Network connectors
User settings
App launchers
Custom authentication extensions
Security
Conditional Access
Consent and permissions
Activity
Sign-in logs
Usage & insights
Audit logs
Provisioning logs
Access reviews

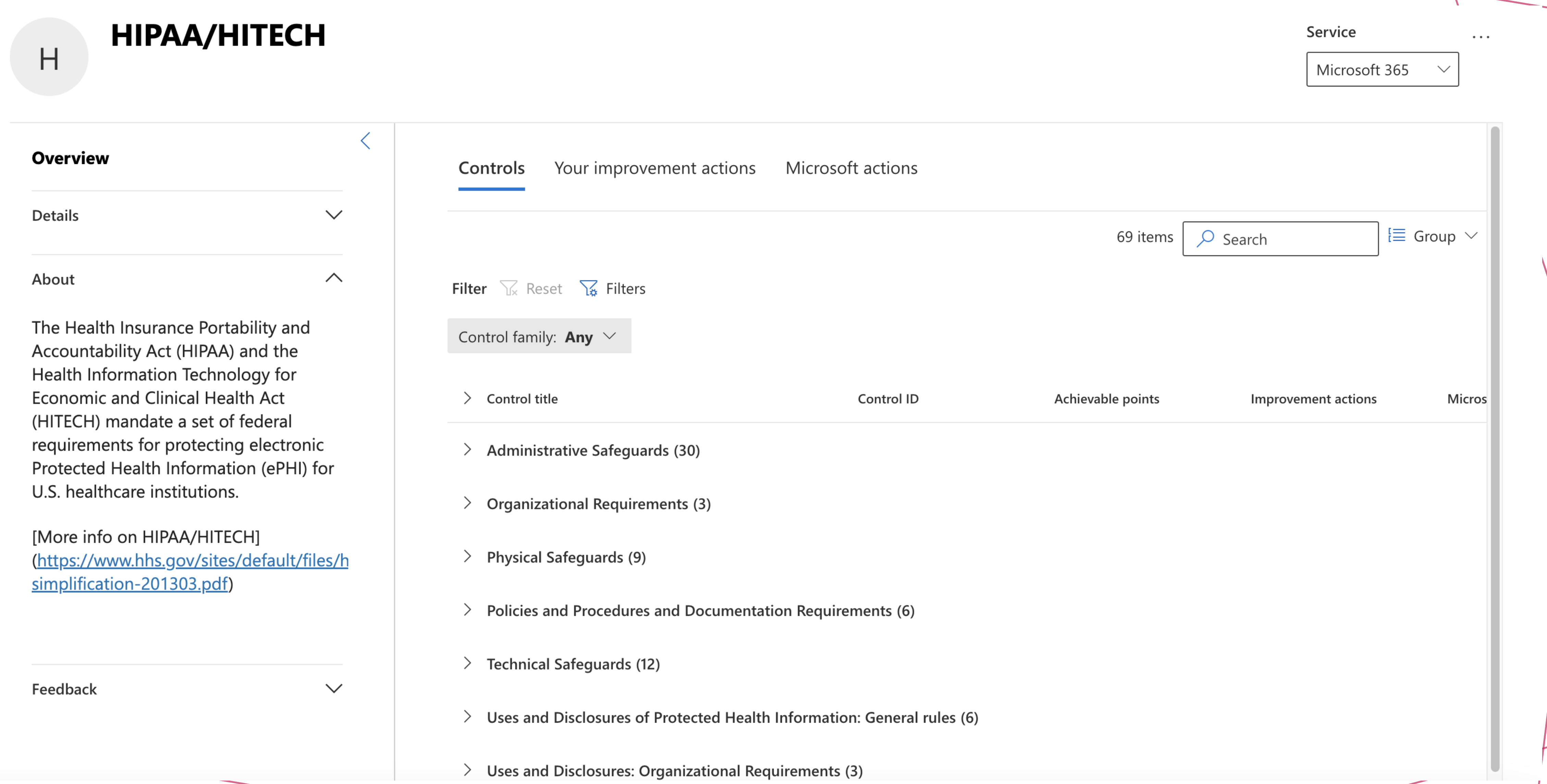
View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

Search by application name or object ID
Application type == **Enterprise Applications**
Application ID starts with
Add filters

32 applications found

Name	Object ID	Application ID	Homepage URL	Created on
Adobe Acrobat Reader	889e7607-afc6-4f07-...	c999586d-3bb6-485...	https://www.adobe.com	4/24/2024
Velixo NX	6d8498f9-35d2-4c20...	dd4aabf4-b6ab-4faf...	https://velixo.com	4/1/2024
CP ClickLearn Portal-Api	9a533797-4f80-4afd...	e09b3673-d485-406...	https://portalapi.clicklearn.dk	2/28/2024
Z Zendesk	4c0f19a9-ec64-47fd-...	c5d3a3e0-2ae6-418...		2/2/2024
M MyFiles	3f27a35b-7696-404c...	d5e6af94-cdf0-4cf4-...		11/14/2023
GoFormz	69fc09b5-77f3-4b4d...	faf06b4b-b2f8-4297-...	https://www.goformz.com/	10/12/2023
OH Obsidian Hybrid	6a44a3b7-d146-4d5...	207d83cb-02c3-489...		9/25/2023
P PhishER	7e2f931b-e3f0-4a7d...	e4d7ce56-2276-464...		6/9/2023
MA Mail App for Outlook	a0b6dae6-2a64-4e8...	11680cd6-7ad2-44d...	https://intrepidcorp.co.uk/mailappforoutlook/	6/2/2023
KnowBe4 Direct Message Injection	24874af7-2e19-4d56...	475cd07d-95df-4ba...	https://www.knowbe4.com/products/kevin-mitnick-security-awareness-training/	2/14/2023
Wrike for Teams	91ca8ec1-e428-48ef...	6910c1b9-cba1-436...	https://www.wrike.com/	1/26/2023
TEAMS PRO Calendar Pro	ab9bafc6-f484-4161...	fb507a6d-2eaa-4f1f-...	https://www.teams-pro.com	1/4/2023



HIPAA/HITECH

Service: Microsoft 365

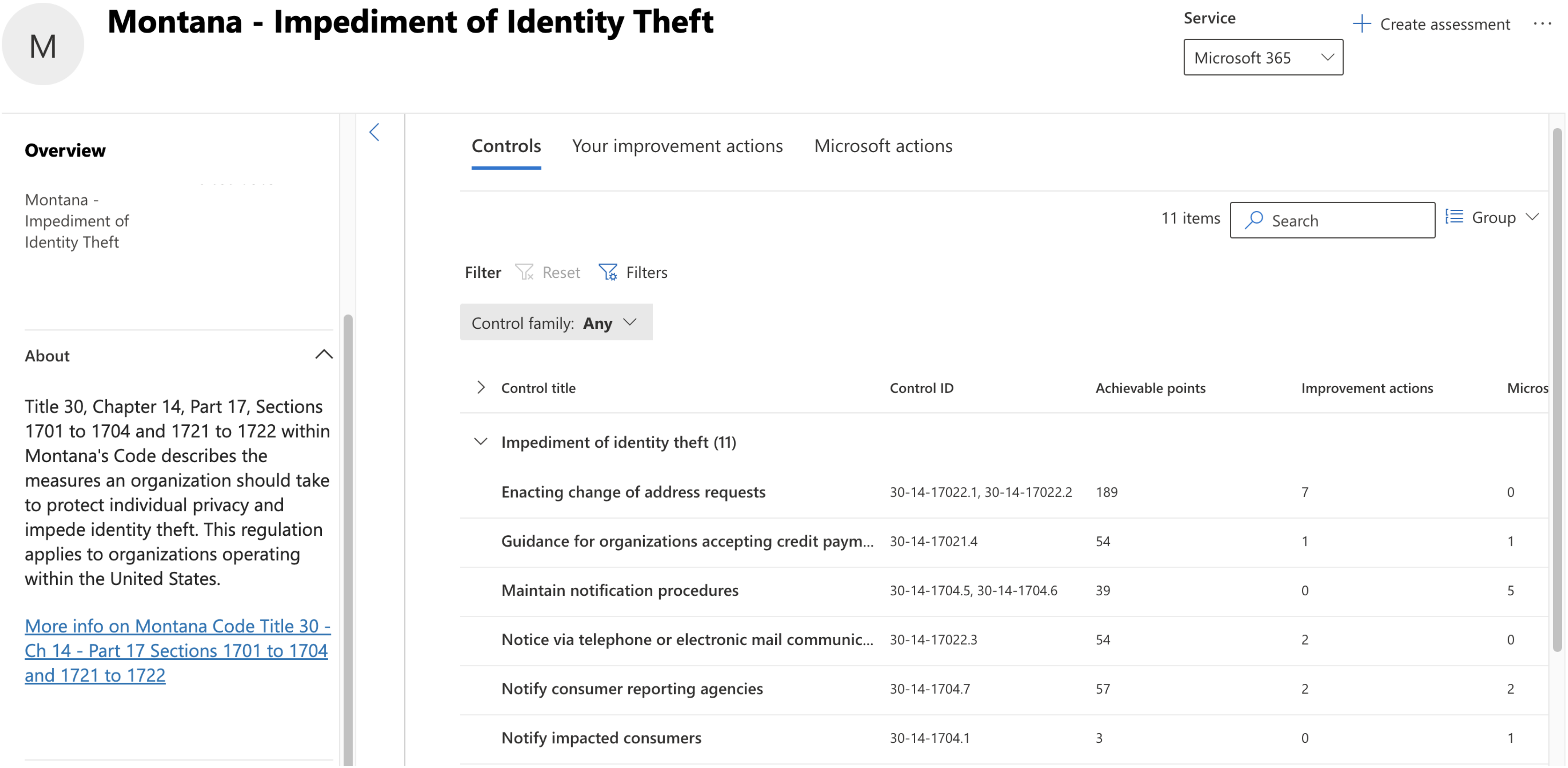
The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) mandate a set of federal requirements for protecting electronic Protected Health Information (ePHI) for U.S. healthcare institutions.

[More info on HIPAA/HITECH] (https://www.hhs.gov/sites/default/files/h simplification-201303.pdf)

69 items

Control family: **Any**

Control title	Control ID	Achievable points	Improvement actions	Micros
Administrative Safeguards (30)				
Organizational Requirements (3)				
Physical Safeguards (9)				
Policies and Procedures and Documentation Requirements (6)				
Technical Safeguards (12)				
Uses and Disclosures of Protected Health Information: General rules (6)				
Uses and Disclosures: Organizational Requirements (3)				



Montana - Impediment of Identity Theft

Control family: **Any**

Overview

Montana - Impediment of Identity Theft

About

Title 30, Chapter 14, Part 17, Sections 1701 to 1704 and 1721 to 1722 within Montana's Code describes the measures an organization should take to protect individual privacy and impede identity theft. This regulation applies to organizations operating within the United States.

More info on Montana Code Title 30 - Ch 14 - Part 17 Sections 1701 to 1704 and 1721 to 1722

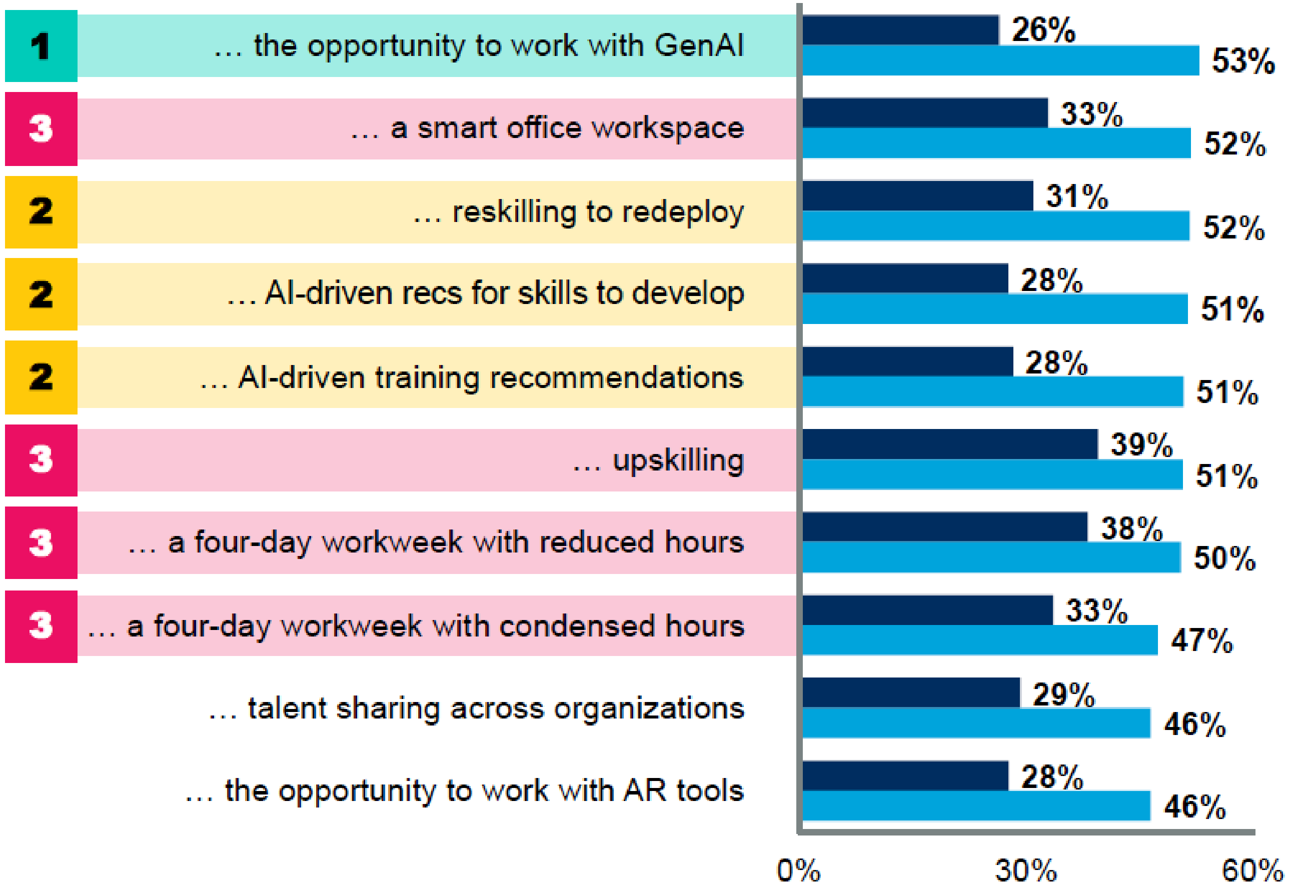
Control title	Control ID	Achievable points	Improvement actions	Micros
Impediment of identity theft (11)				
Enacting change of address requests	30-14-17022.1, 30-14-17022.2	189	7	0
Guidance for organizations accepting credit paym...	30-14-17021.4	54	1	1
Maintain notification procedures	30-14-1704.5, 30-14-1704.6	39	0	5
Notice via telephone or electronic mail communic...	30-14-17022.3	54	2	0
Notify consumer reporting agencies	30-14-1704.7	57	2	2
Notify impacted consumers	30-14-1704.1	3	0	1

Appendix

Just How Different?

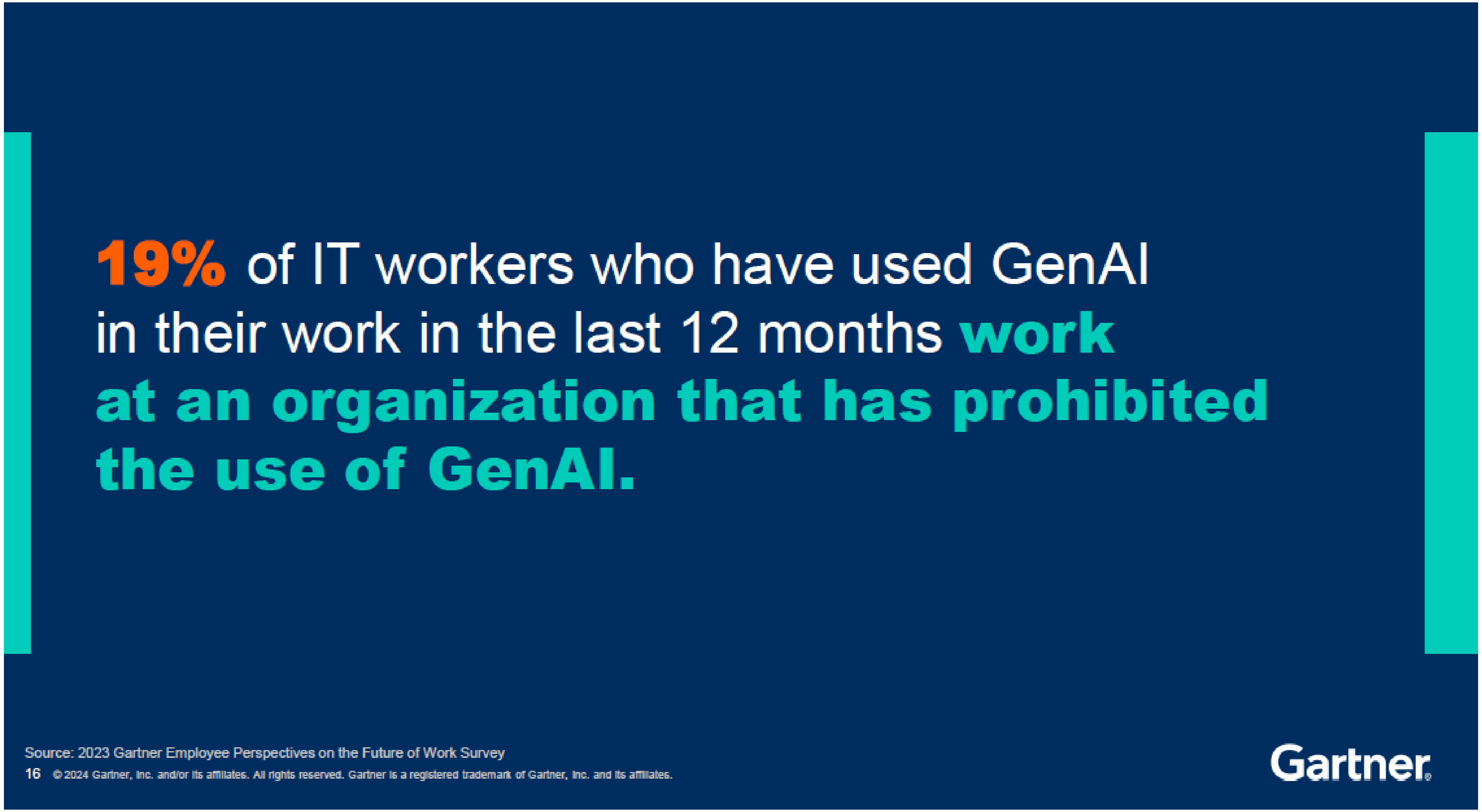
Willingness to switch roles if offered …

- 🟦 Non-IT workers
- 🟦 IT workers
- 🟩 Work with GenAI
- 🟨 New skills
- 🟥 Smart office/four-day workweek



n = 2,761 (non-IT workers), 739 (IT workers)
Source: 2023 Gartner Employee Perspectives on the Future of Work Survey

Gartner



19% of IT workers who have used GenAI in their work in the last 12 months **work at an organization that has prohibited the use of GenAI.**

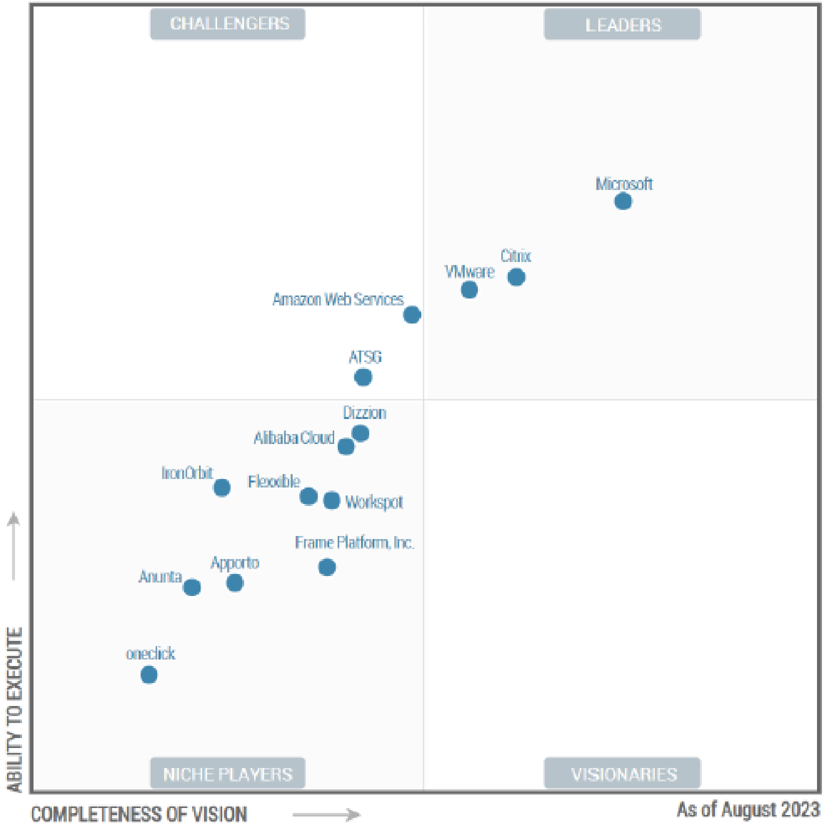
Source: 2023 Gartner Employee Perspectives on the Future of Work Survey

Windows 10 End of Support

494 : 10 : 07 : 10

DAYS HOURS MINUTES SECONDS

Magic Quadrant for Desktop as a Service, 2023



Source: Magic Quadrant for Desktop as a Service , 5 September 2023

DigitalBunker365