2024 OneCon IntegraONE

I think I've Been Hacked Cloud Email Compromise

Al Kayal
Director of Security

akayal@integraone.com
https://www.linkedin.com/in/allenkayal/

Me in a nutshell

1990's

- Basement NOC specialist, Linux hacker, web/programming

2000's

- Real NOCs / ISPs, systems & networking

2006 - Present

- Professionally consulting with VARs

I Think I've Been Hacked

Tell tale signs your account may be compromised:

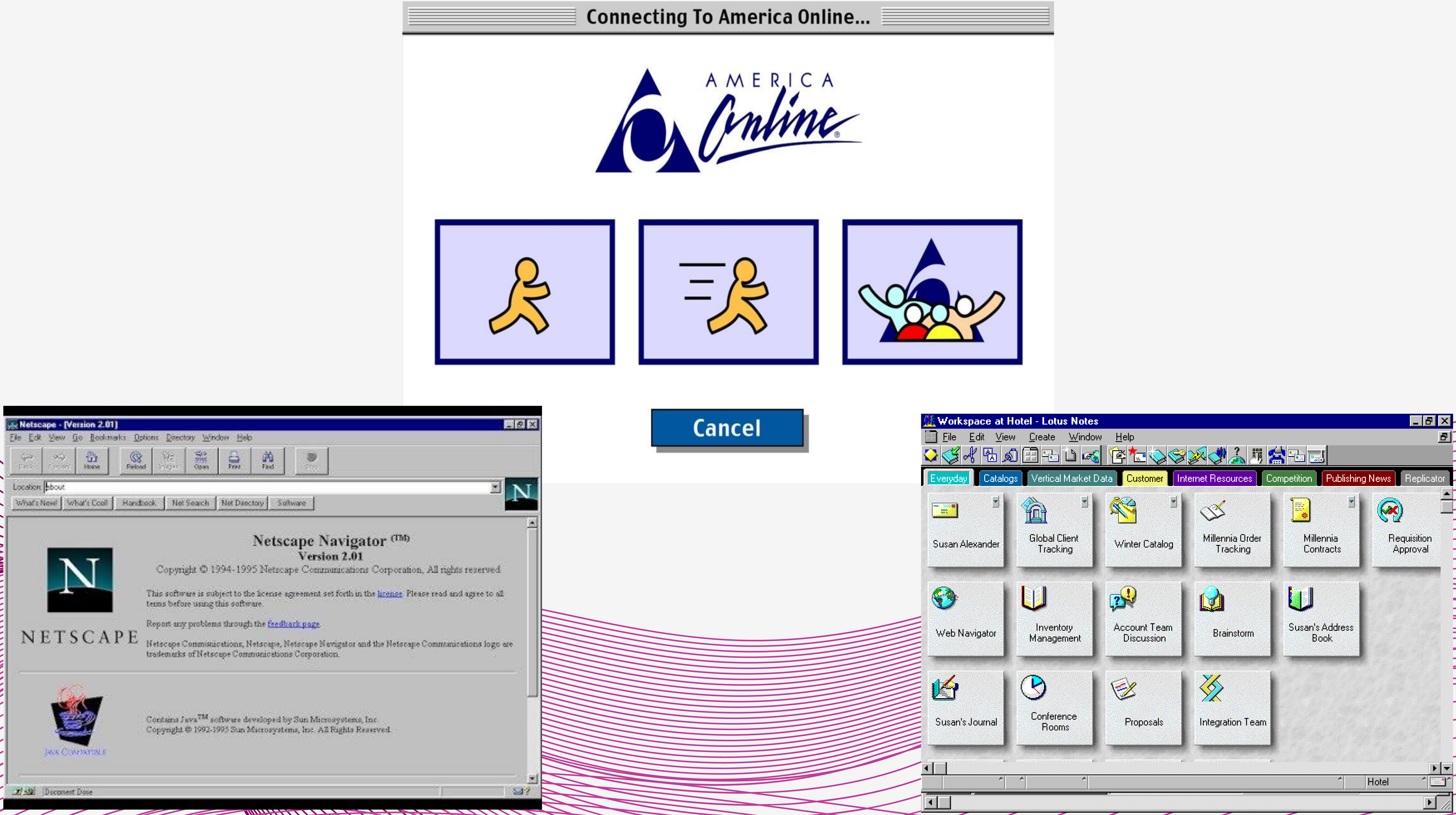
- **Suspicious activity observed, such as deleted or missing emails**
- **Receive bounce back or failure notices about messages to unknown addresses you never sent**
- **Receiving strange questions/emails from contacts and colleagues**
- **Messages landing in unusual folders - Notes, Junk Email, RSS Subscriptions**
- **Unknown/unread messages in Sent or Deleted folder**
- **Calendar or Profile changes**
- **Messages being forwarded to unknown external addresses**

Email has been around for a long time. It has become a large part of our daily occurrence.

Could you imagine a day where you wake up in the morning, brew a cup of coffee, and move onto your next task which isn't checking email?

Fun Email History

1960’s	Concept of email adopted and attempted
1970’s	“@” symbol introduced, FTP for transport
1980’s	SMTP born, LANs emerge, protocol wars
1990’s	Heavily utilized, web email was born



Netscape Navigator (TM)
Version 2.01
Copyright © 1994-1995 Netscape Communications Corporation, All rights reserved.

This software is subject to the license agreement set forth in the license. Please read and agree to all terms before using this software.

Report any problems through the feedback page.

Netscape Communications, Netscape, Netscape Navigator and the Netscape Communications logo are trademarks of Netscape Communications Corporation.

Contains Java™ software developed by Sun Microsystems, Inc. Copyright © 1992-1995 Sun Microsystems, Inc. All Rights Reserved.

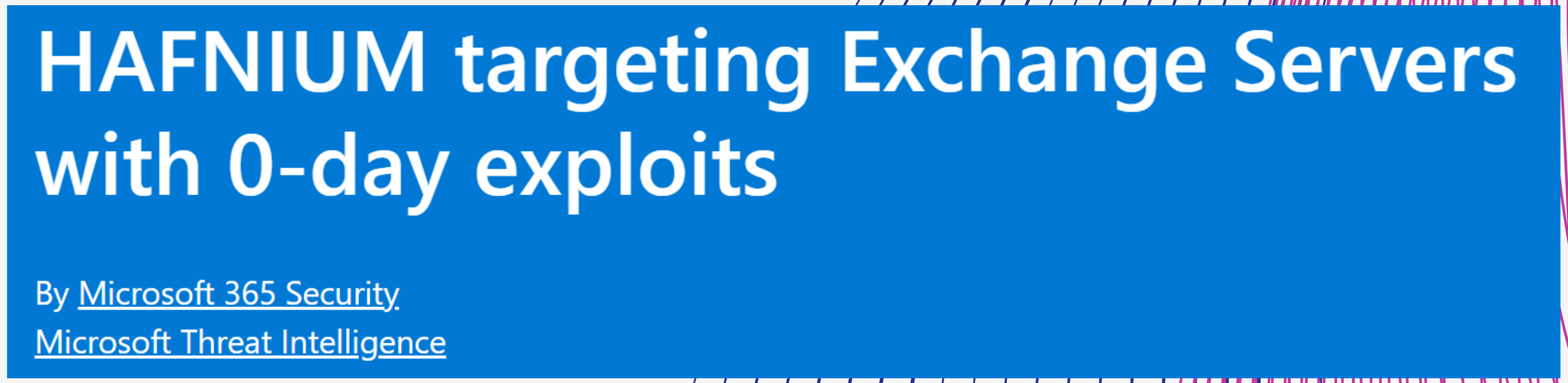
Microsoft Exchange

Mid 1990's Microsoft's flagship mail server product

Web based service exposure (EWS/NTLM)

Struggled with vulnerabilities throughout the years

ProxyLogon, ProxyShell



HAFNIUM targeting Exchange Servers with 0-day exploits

By Microsoft 365 Security
Microsoft Threat Intelligence

Office 365 - Exchange Online

Collaboration

Microsoft 365's apps and services can improve collaboration between employees, partners, and teams. For example, Microsoft Teams allows for real-time collaboration, while Outlook offers shared calendars and advanced email functionality.

Scalability

Microsoft 365 is a cloud-based platform that can grow with a business as its needs change. This can help businesses adapt to market trends and drive innovation.

Productivity

Microsoft 365 can help boost employee productivity. For example, it can streamline workflows and information exchange, which can lead to faster turnaround times.

Security

Microsoft 365 offers advanced security features to protect sensitive data and prevent unauthorized access. These features include multi-factor authentication, data loss prevention, and threat protection.

Accessibility

Microsoft 365 can be accessed from anywhere with an internet connection. This can give businesses greater flexibility in how their employees work.

Software Expenses

Microsoft 365 is subscription-based, so businesses only pay for the software they use.

Security Concerns?

Weak/Reused Passwords

Many users rely on a common password across various platforms. Attackers use credentials posted in lists from 3rd party compromises.

Misconfigurations

Tenants left at default settings. Users with elevated permissions instead of implementing using the least-privilege methodology. Users may have access to sensitive information and share publicly by mistake.

Account Management

Ghost user accounts – Stale/dormant accounts that haven't been properly decommissioned through the lifecycle. User accounts containing elevated privileges.

Multifactor Authentication

MFA provides effective defenses protecting users from having weak passwords, credential stuffing, or brute force attacks. But, many organizations do not enforce MFA for standard user access.

Weak Filtering/Protection

Phishing still remains one of the most effective techniques for external threat actors. Additionally, strong endpoint protection is a necessity to protect against accidental clicks, attachments, and malware.

Cloud Backups

Users assume their data is backed up automatically because it's located in the cloud. Microsoft provides uptime and infrastructure security. Data protection is the end-users responsibility. Accidental deletion, malware/ransomware, can result in permanent data loss.

#1 Account Compromise

Weak/Reused Passwords – Lack of Multifactor Authentication

- Attackers gain access to low privileged accounts
- A backdoor using Microsoft Graph API is created
- Download/Send/Receive user messages
- Create inbox forwarding rules
- Conduct phishing campaigns against trusted contacts (internal/external)
- Access sensitive information stored in m365, OneDrive, Teams
- Harvest additional credentials from sensitive files/phishing campaigns
  - Worst case scenario - User account has global admin privileges

Some of the basics in Microsoft Entra related to the backdoor implant

Principal

- An identity that can be authenticated. (user or service principal)

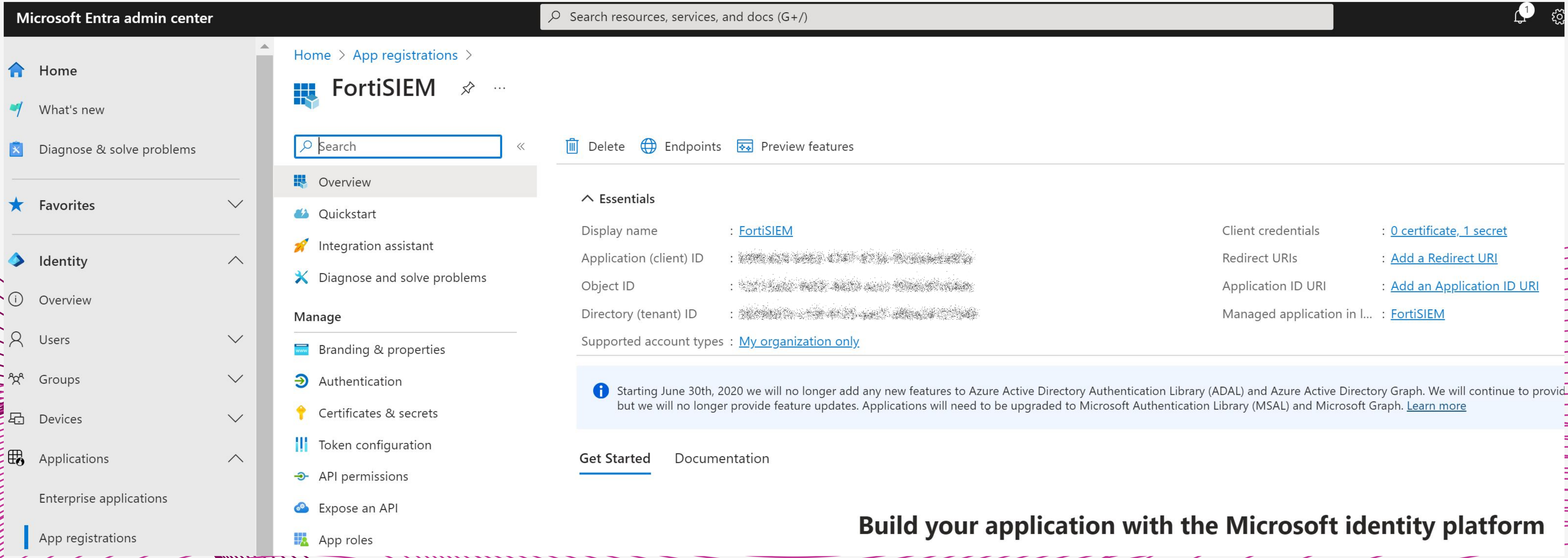
App Registration

- An application object that resides in the Entra tenant. This is where users grant permissions to applications to perform things.

Service Principal

- The identity an app uses when authenticating to Entra.

App Registration

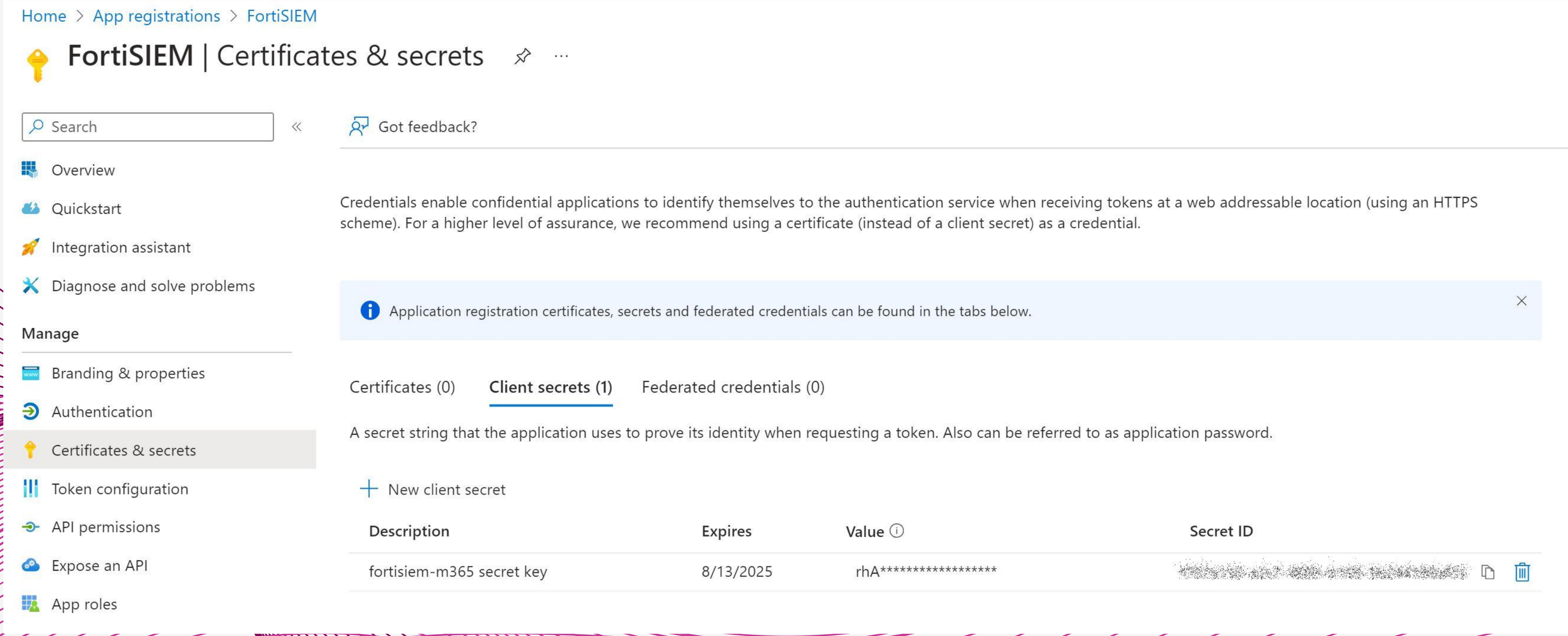


Display name	:	FortiSIEM	Client credentials	:	0 certificate, 1 secret
Application (client) ID	:	[redacted]	Redirect URIs	:	Add a Redirect URI
Object ID	:	[redacted]	Application ID URI	:	Add an Application ID URI
Directory (tenant) ID	:	[redacted]	Managed application in l...	:	FortiSIEM
Supported account types	:	My organization only			

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provid
but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

App Registration - Secret



FortiSIEM | Certificates & secrets

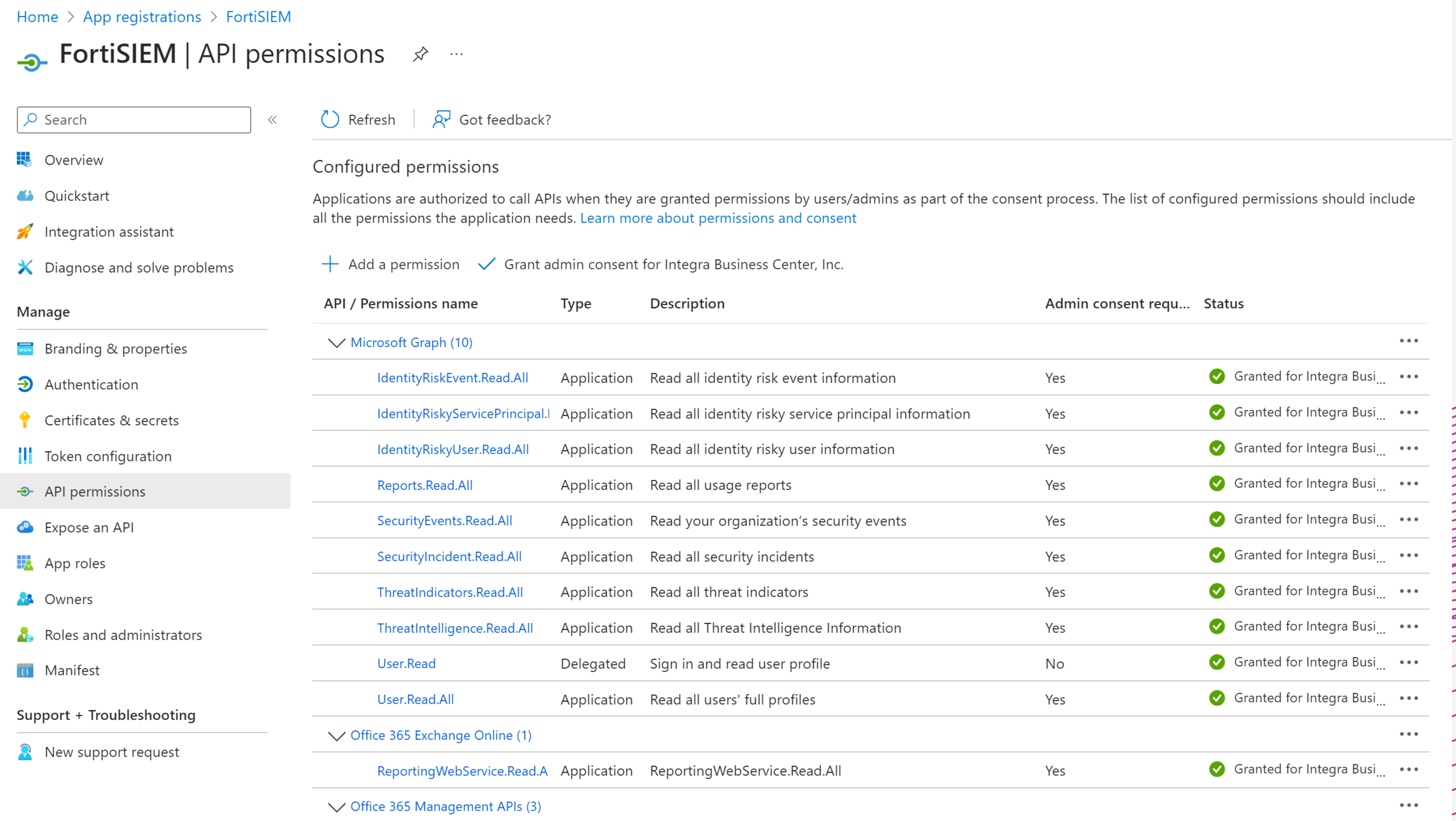
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
fortisiem-m365 secret key	8/13/2025	rhA******************	[redacted]

App Registration – Permissions



Home > App registrations > FortiSIEM

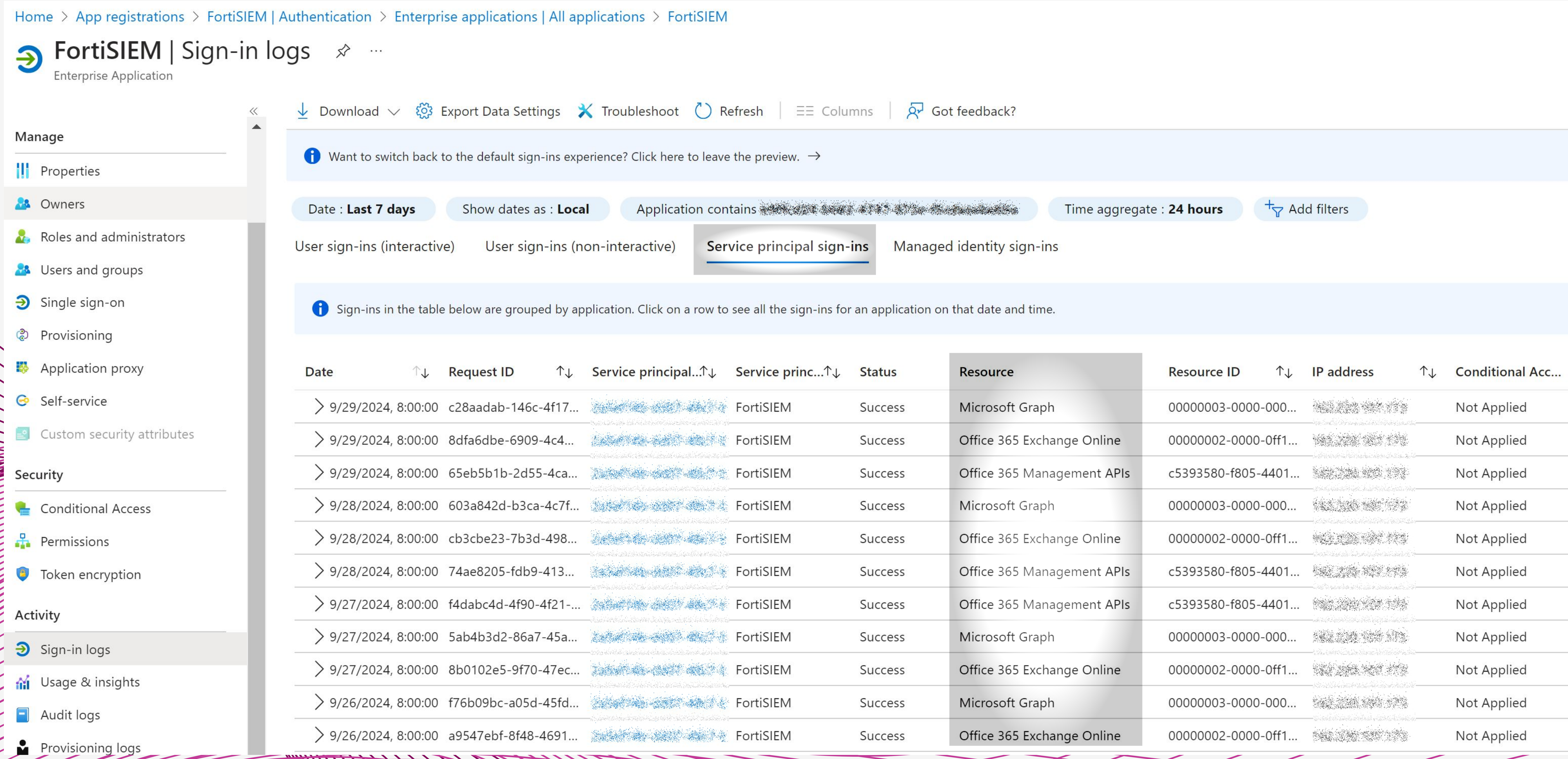
FortiSIEM | API permissions

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (10)				
IdentityRiskEvent.Read.All	Application	Read all identity risk event information	Yes	✓ Granted for Integra Busi...
IdentityRiskyServicePrincipal.I	Application	Read all identity risky service principal information	Yes	✓ Granted for Integra Busi...
IdentityRiskyUser.Read.All	Application	Read all identity risky user information	Yes	✓ Granted for Integra Busi...
Reports.Read.All	Application	Read all usage reports	Yes	✓ Granted for Integra Busi...
SecurityEvents.Read.All	Application	Read your organization's security events	Yes	✓ Granted for Integra Busi...
SecurityIncident.Read.All	Application	Read all security incidents	Yes	✓ Granted for Integra Busi...
ThreatIndicators.Read.All	Application	Read all threat indicators	Yes	✓ Granted for Integra Busi...
ThreatIntelligence.Read.All	Application	Read all Threat Intelligence Information	Yes	✓ Granted for Integra Busi...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Integra Busi...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Integra Busi...
Office 365 Exchange Online (1)				
ReportingWebService.Read.A	Application	ReportingWebService.Read.All	Yes	✓ Granted for Integra Busi...
Office 365 Management APIs (3)				

App Registration - SignIns



Home > App registrations > FortiSIEM | Authentication > Enterprise applications | All applications > FortiSIEM

FortiSIEM | Sign-in logs

Enterprise Application

Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : **Last 7 days** | Show dates as : **Local** | Application contains [redacted] | Time aggregate : **24 hours** | Add filters

User sign-ins (interactive) | User sign-ins (non-interactive) | **Service principal sign-ins** | Managed identity sign-ins

Sign-ins in the table below are grouped by application. Click on a row to see all the sign-ins for an application on that date and time.

Date	Request ID	Service principal...	Service princ...	Status	Resource	Resource ID	IP address	Conditional Acc...
9/29/2024, 8:00:00	c28aadab-146c-4f17...	[redacted]	FortiSIEM	Success	Microsoft Graph	00000003-0000-000...	[redacted]	Not Applied
9/29/2024, 8:00:00	8dfa6dbe-6909-4c4...	[redacted]	FortiSIEM	Success	Office 365 Exchange Online	00000002-0000-0ff1...	[redacted]	Not Applied
9/29/2024, 8:00:00	65eb5b1b-2d55-4ca...	[redacted]	FortiSIEM	Success	Office 365 Management APIs	c5393580-f805-4401...	[redacted]	Not Applied
9/28/2024, 8:00:00	603a842d-b3ca-4c7f...	[redacted]	FortiSIEM	Success	Microsoft Graph	00000003-0000-000...	[redacted]	Not Applied
9/28/2024, 8:00:00	cb3cbe23-7b3d-498...	[redacted]	FortiSIEM	Success	Office 365 Exchange Online	00000002-0000-0ff1...	[redacted]	Not Applied
9/28/2024, 8:00:00	74ae8205-fdb9-413...	[redacted]	FortiSIEM	Success	Office 365 Management APIs	c5393580-f805-4401...	[redacted]	Not Applied
9/27/2024, 8:00:00	f4dabc4d-4f90-4f21-...	[redacted]	FortiSIEM	Success	Office 365 Management APIs	c5393580-f805-4401...	[redacted]	Not Applied
9/27/2024, 8:00:00	5ab4b3d2-86a7-45a...	[redacted]	FortiSIEM	Success	Microsoft Graph	00000003-0000-000...	[redacted]	Not Applied
9/27/2024, 8:00:00	8b0102e5-9f70-47ec...	[redacted]	FortiSIEM	Success	Office 365 Exchange Online	00000002-0000-0ff1...	[redacted]	Not Applied
9/26/2024, 8:00:00	f76b09bc-a05d-45fd...	[redacted]	FortiSIEM	Success	Microsoft Graph	00000003-0000-000...	[redacted]	Not Applied
9/26/2024, 8:00:00	a9547ebf-8f48-4691...	[redacted]	FortiSIEM	Success	Office 365 Exchange Online	00000002-0000-0ff1...	[redacted]	Not Applied

Mitigations - Account Hygeine

The amount of password protected portals has grown significantly over the years. To best plan for account security, lets assume a few things regarding human behavior:

- Users may implement insecure passwords
- Passwords may be used across different platforms
  - Work accounts, Personal cloud accounts, etc
- Passwords may be documented in files stored in folders/OneDrive
- Mobile devices capable of a multifactor authentication app are within reach

Mitigations - Multifactor Auth

Microsoft Entra Security Defaults

- Barely secure, Enabled by default
- Protects administrative logins, sometimes user logins

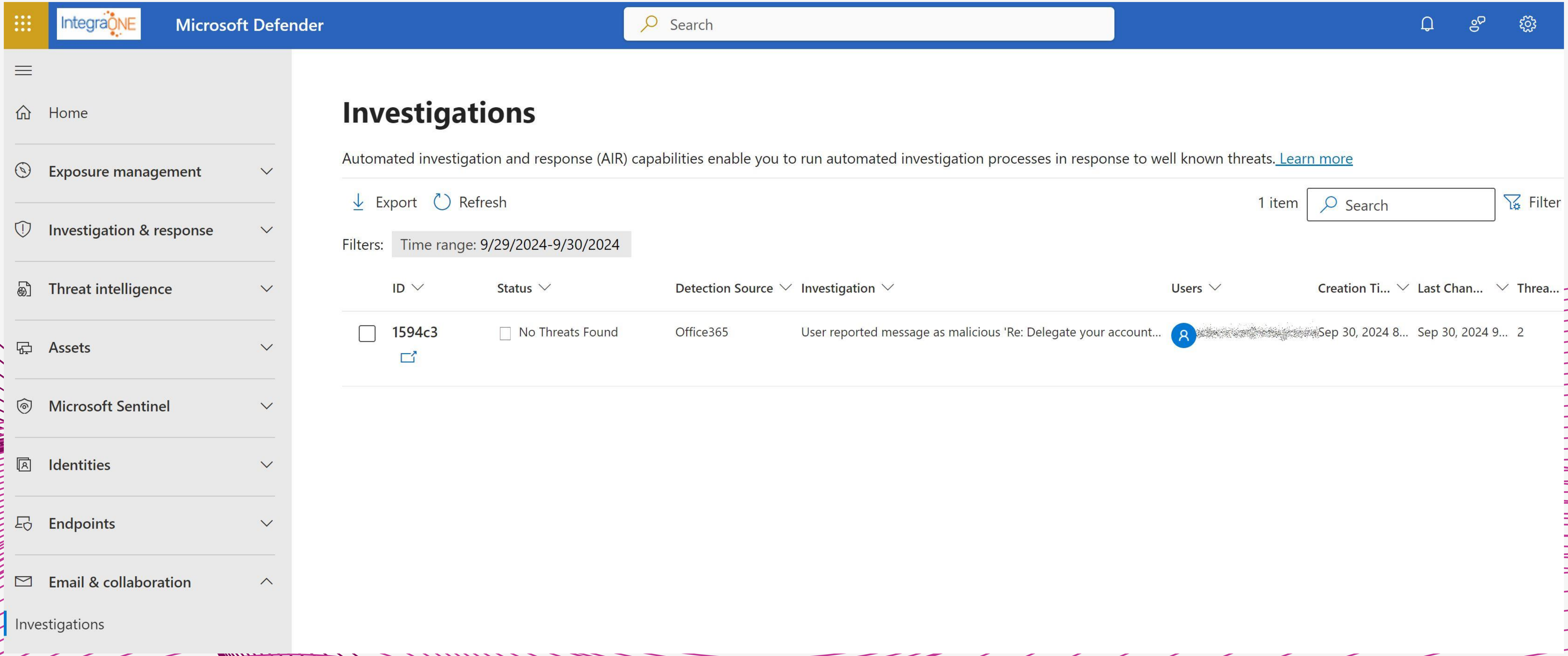
M365 per-user MFA

- Old way of enforcing MFA per user account
- M365 Admin Center - https://admin.microsoft.com

Microsoft Entra Conditional Access Policies

- Most secure method
- Requires minimum Entra Premium 1 license

Logging and Analytics (Defender Portal)



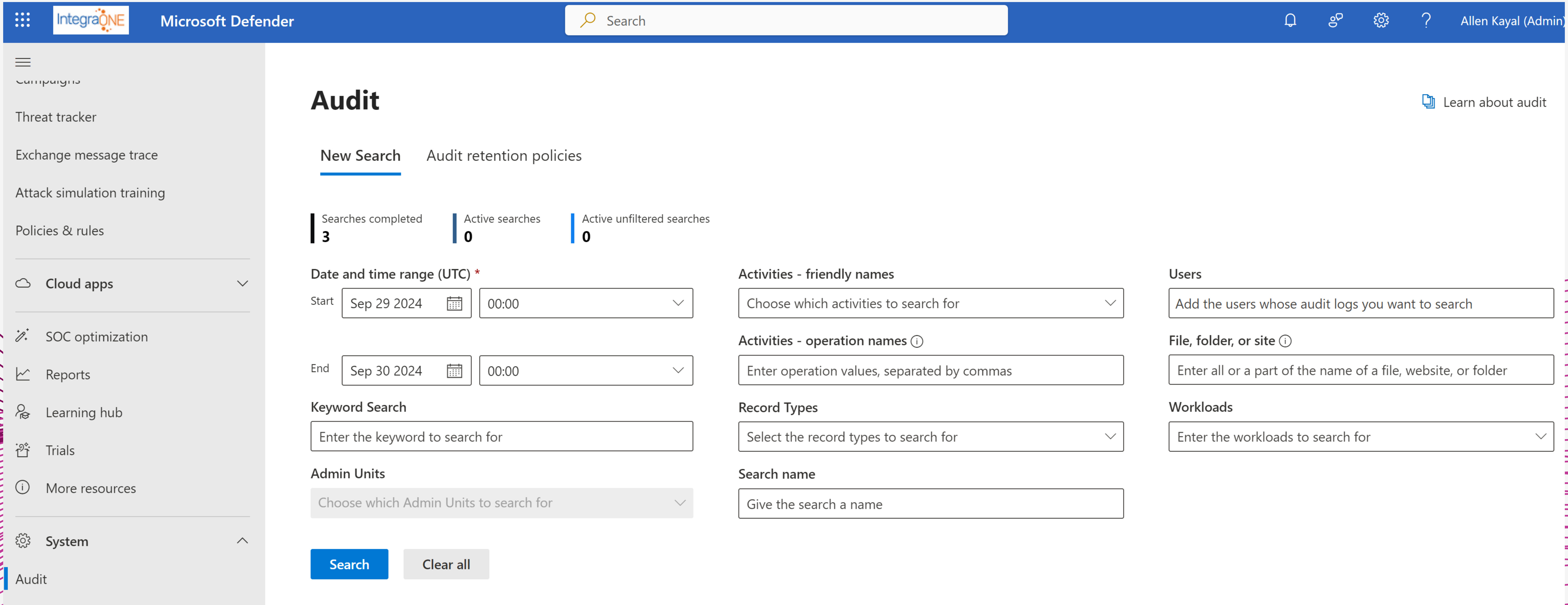
Investigations

Automated investigation and response (AIR) capabilities enable you to run automated investigation processes in response to well known threats. Learn more

Filters: Time range: 9/29/2024-9/30/2024

	ID	Status	Detection Source	Investigation	Users	Creation Ti...	Last Chan...	Threa...
□	1594c3	No Threats Found	Office365	User reported message as malicious 'Re: Delegate your account...	[redacted]	Sep 30, 2024 8...	Sep 30, 2024 9...	2

Logging and Analytics (UAL)



IntegraONE Microsoft Defender

Search

Allen Kayal (Admin)

Campaigns

Threat tracker

Exchange message trace

Attack simulation training

Policies & rules

Cloud apps

SOC optimization

Reports

Learning hub

Trials

More resources

System

Audit

Audit

Learn about audit

New Search | Audit retention policies

Searches completed 3

Active searches 0

Active unfiltered searches 0

Date and time range (UTC) *

Start: Sep 29 2024 00:00

End: Sep 30 2024 00:00

Keyword Search: Enter the keyword to search for

Admin Units: Choose which Admin Units to search for

Activities - friendly names: Choose which activities to search for

Activities - operation names: Enter operation values, separated by commas

Record Types: Select the record types to search for

Search name: Give the search a name

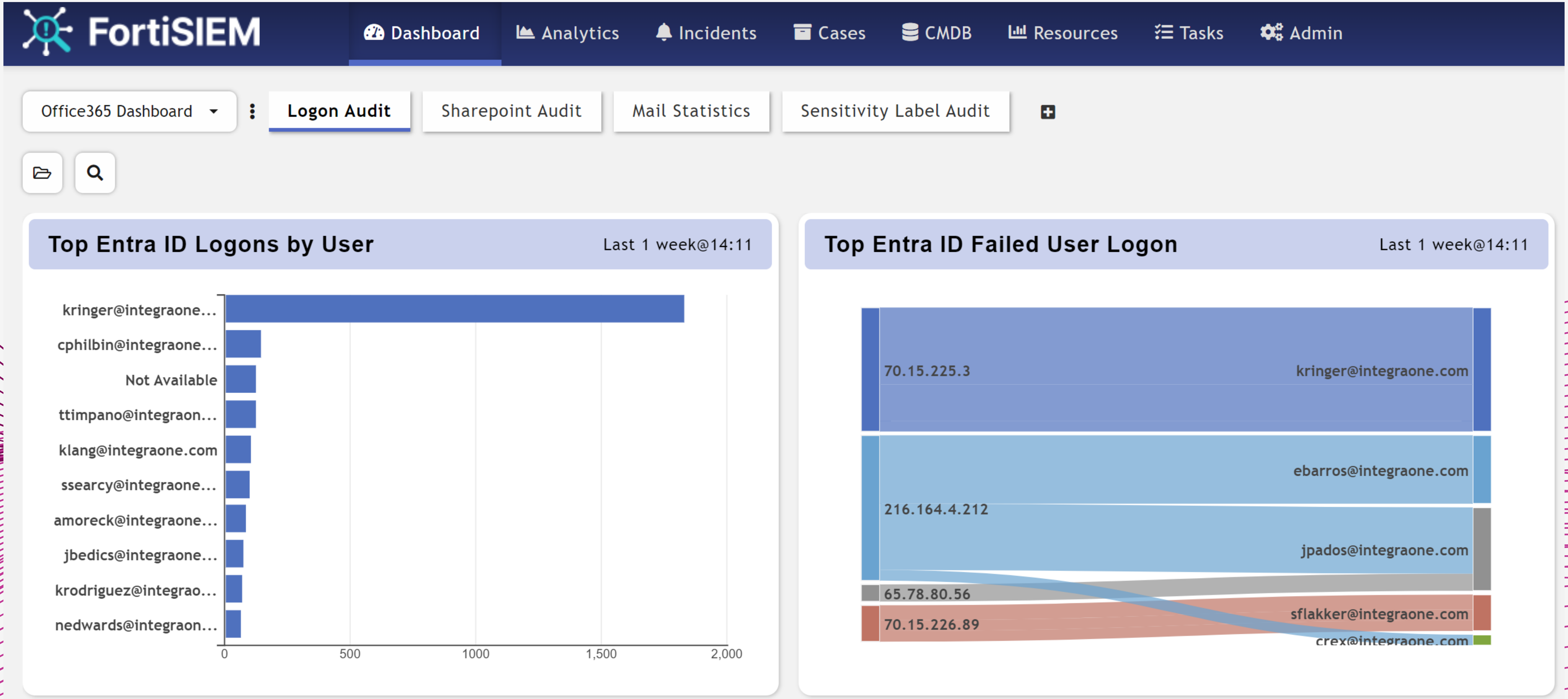
Users: Add the users whose audit logs you want to search

File, folder, or site: Enter all or a part of the name of a file, website, or folder

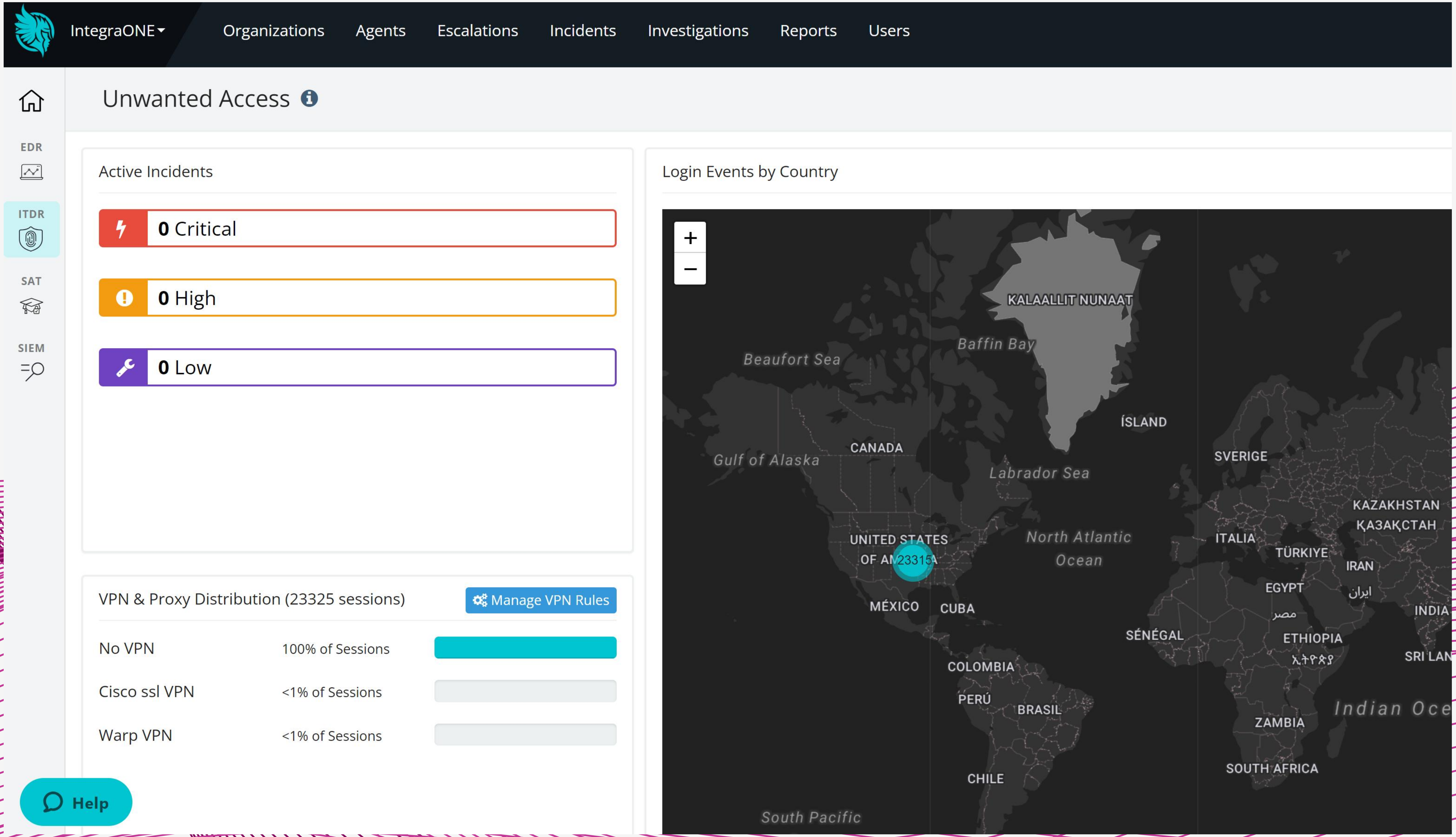
Workloads: Enter the workloads to search for

Search | Clear all

Logging and Analytics (SIEM)



Logging and Analytics (Huntress ITDR)



Unwanted Access

Active Incidents

- 0 Critical
- 0 High
- 0 Low

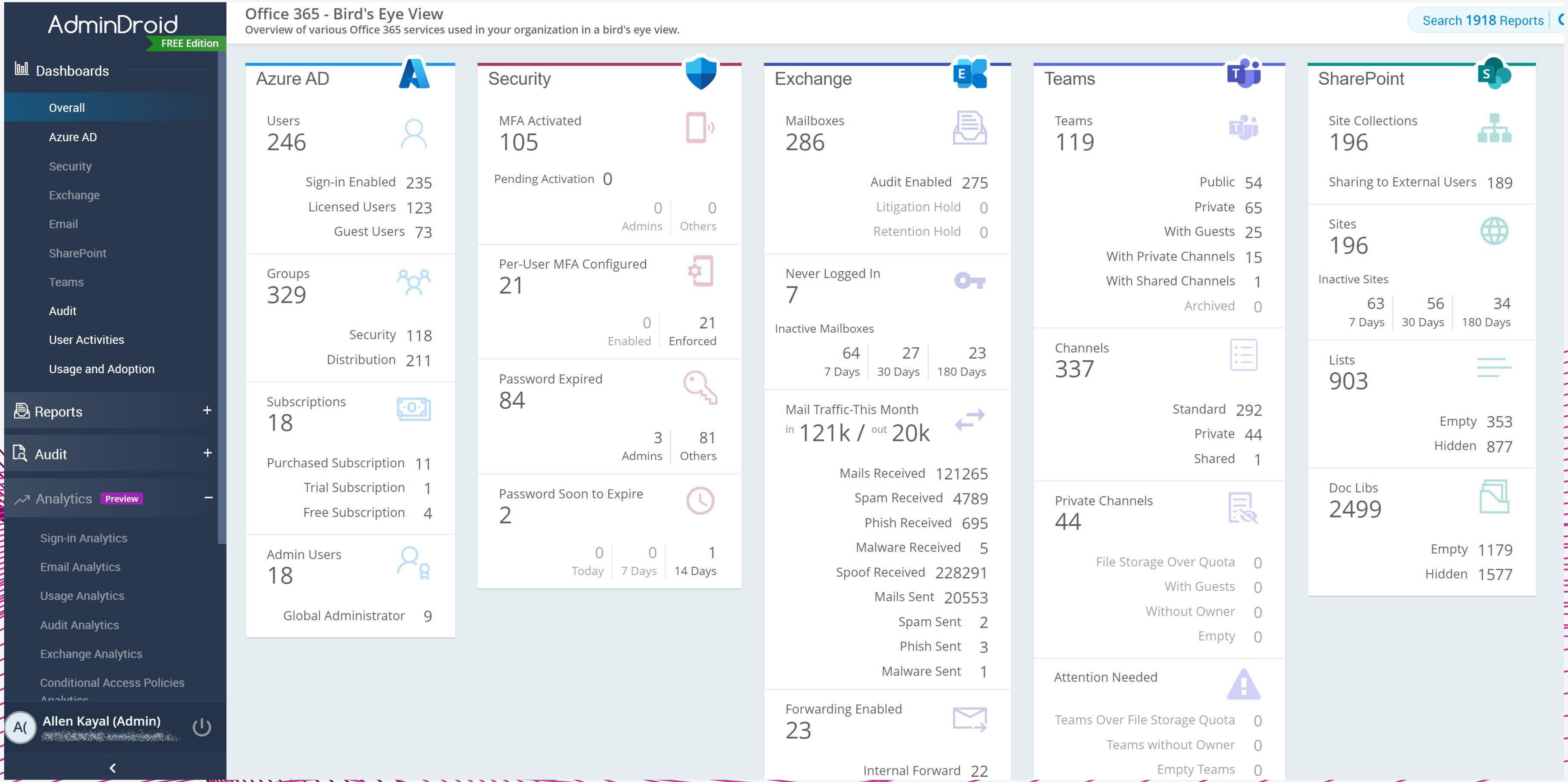
VPN & Proxy Distribution (23325 sessions)

Manage VPN Rules

No VPN	100% of Sessions
Cisco ssl VPN	<1% of Sessions
Warp VPN	<1% of Sessions

Login Events by Country

Logging and Analytics (AdminDroid)



[redacted]

Office 365 - Bird's Eye View

Overview of various Office 365 services used in your organization in a bird's eye view.

Azure AD

Users
246

Sign-in Enabled	235
Licensed Users	123
Guest Users	73

Groups
329

Security	118
Distribution	211

Subscriptions
18

Purchased Subscription	11
Trial Subscription	1
Free Subscription	4

Admin Users
18

Global Administrator	9

Security

MFA Activated
105

Pending Activation 0

Admins	Others
0	0

Per-User MFA Configured
21

Enabled	Enforced
0	21

Password Expired
84

Admins	Others
3	81

Password Soon to Expire
2

Today	7 Days	14 Days
0	0	1

Exchange

Mailboxes
286

Audit Enabled	275
Litigation Hold	0
Retention Hold	0

Never Logged In
7

Inactive Mailboxes

7 Days	30 Days	180 Days
64	27	23

Mail Traffic-This Month
in 121k / out 20k

Mails Received	121265
Spam Received	4789
Phish Received	695
Malware Received	5
Spoof Received	228291
Mails Sent	20553
Spam Sent	2
Phish Sent	3
Malware Sent	1

Forwarding Enabled
23

Internal Forward	22

Teams

Teams
119

Public	54
Private	65
With Guests	25
With Private Channels	15
With Shared Channels	1
Archived	0

Channels
337

Standard	292
Private	44
Shared	1

Private Channels
44

File Storage Over Quota	0
With Guests	0
Without Owner	0
Empty	0

Attention Needed

Teams Over File Storage Quota	0
Teams without Owner	0
Empty Teams	0

SharePoint

Site Collections
196

Sharing to External Users	189

Sites
196

Inactive Sites

7 Days	30 Days	180 Days
63	56	34

Lists
903

Empty	353
Hidden	877

Doc Libs
2499

Empty	1179
Hidden	1577

I Think I’ve Been Hacked (and need help)

IntegraONE

- Proactive & Reactive Solutions
  - Entra/m365 subscriptions
  - Identity and MFA
  - EDR/MDR/XDR, Email and Perimeter Security
  - Incident Response

Trusted Partners

- BlackBerry (Cylance), ConnectWise, Unit 42 (Palo Alto)
  - Digital Forensics and Incident Response
  - Cloud Email Compromise Assessments

Thank You!

I hope this presentation was helpful!

Questions & Answers