CLOUD IDENTITY
SUMMIT '20

Cloud Identity Security

Identity Protection - Deep Dive, find what you usually do not see

Thomas Detzner (Microsoft)

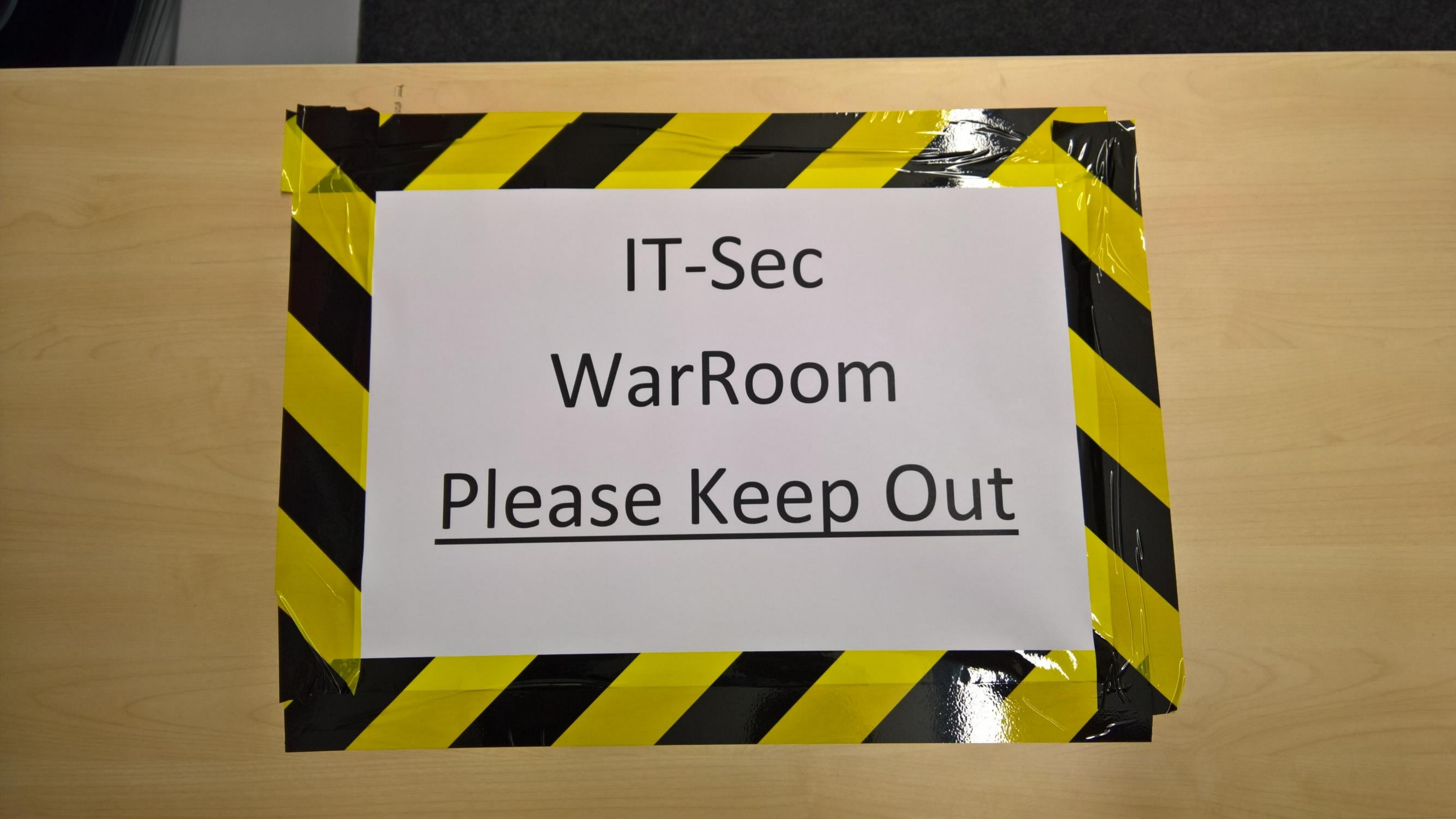
Community Event by

Azure Meetup
BONN

sponsered by

DICE
DEBEKA
INNOVATION
CENTER

yubico



IT-Sec

WarRoom

Please Keep Out

Agenda

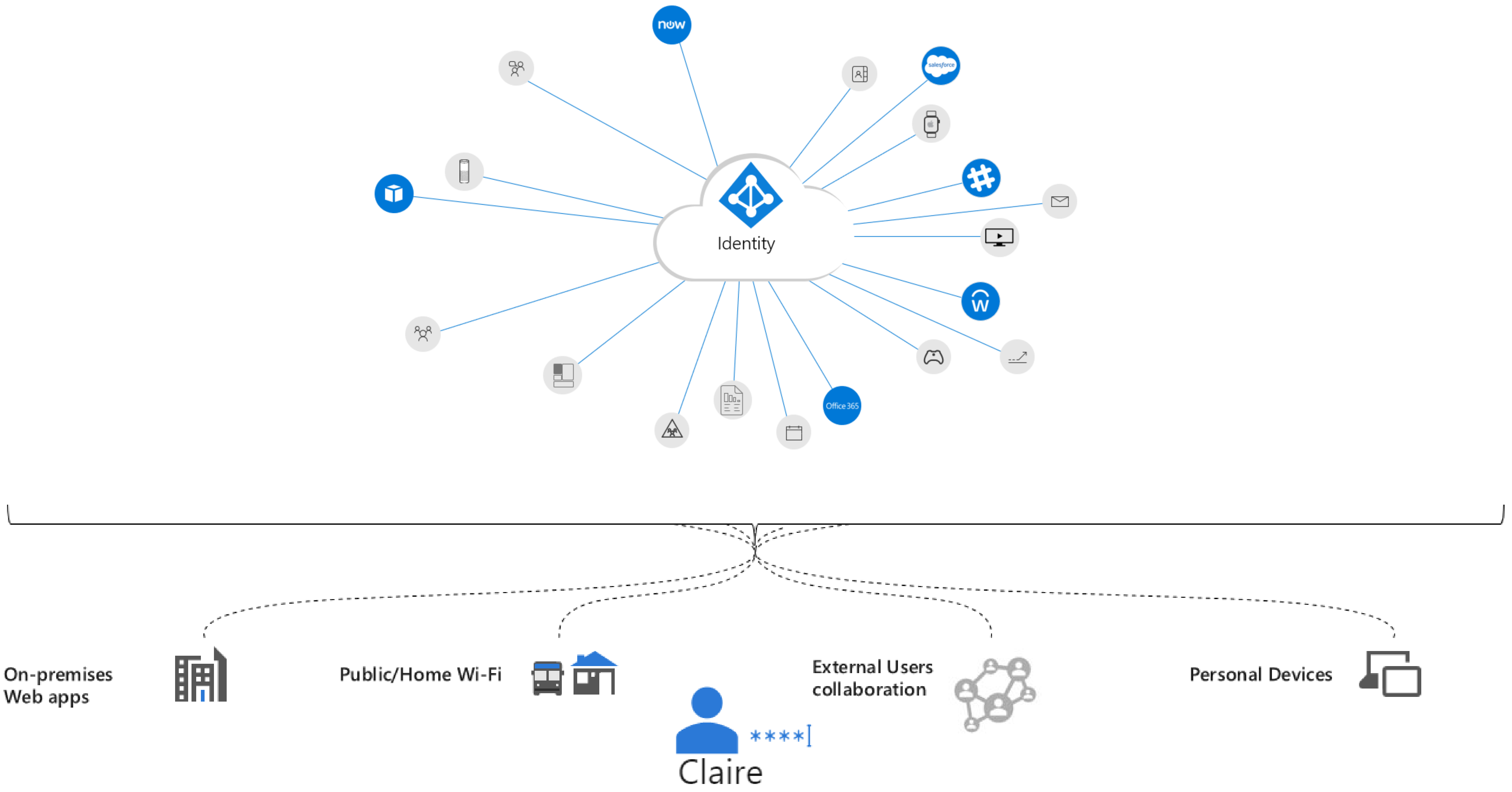
What does our current remote work world look like?

How Identity Protection is even more relevant now

The Data Science behind our machine learning

What’s new in Identity Protection?

What does remote work look like?

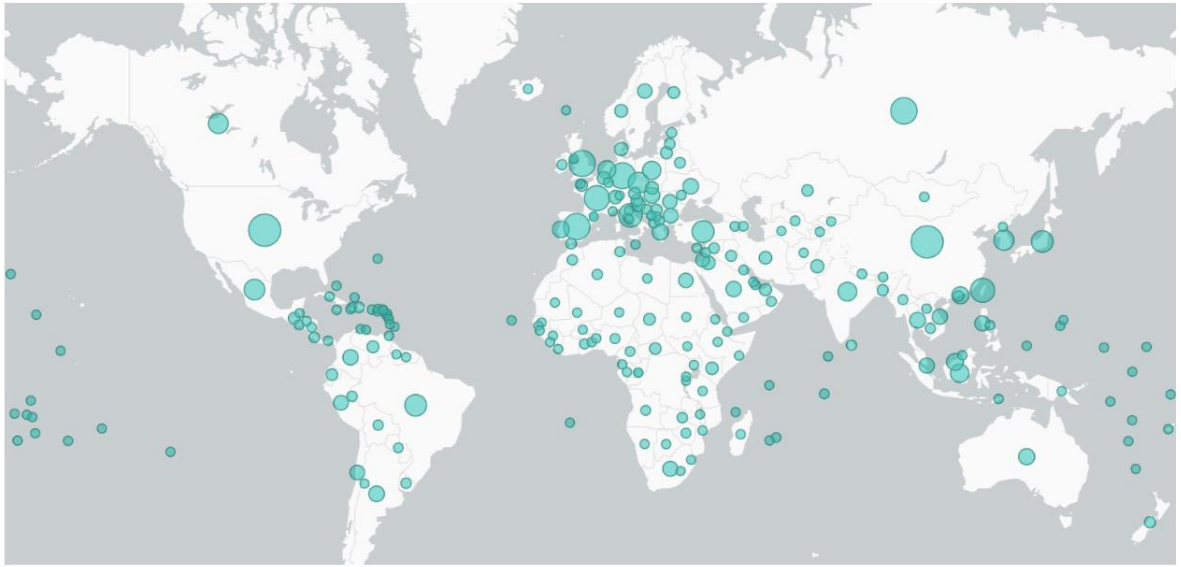


230% increase in password spray attacks this year

Nearly 1 in 3 of all attacks on enterprises involve phishing

9M high-risk enterprise sign-in attempts flagged in **August 2020**

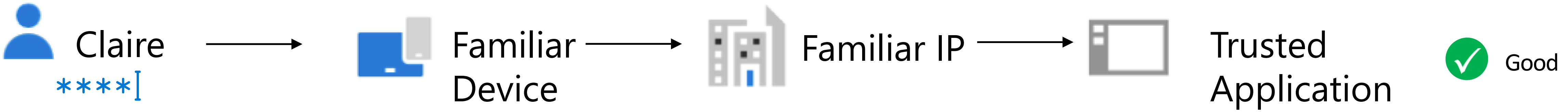
2M compromised accounts detected in **August 2020**



** Chart shows impact of COVID-19 themed attacks across the world by file count (as of April 7, 2020) / Source Microsoft Threat Intelligence*

What do we know about a user?

Heuristic Rules Effective for obvious attack patterns | Faster to implement | But costly to maintain



Session	Date	Time	User	Device	Application	IP Address	Country
1	3-Mar	10:05	Claire	iPhone 8	Exchange	1.2.3.4	US
2	3-Mar	15:07	Claire	iPhone 8	Exchange	1.2.3.5	US
3	3-Mar	16:45	Claire	Windows 10	Salesforce	2.2.2.1	US
4	4-Mar	10:23	Claire	Windows 10	Salesforce	2.2.2.1	US
5	4-Mar	2:04	Claire	Linux	Sway	13.22.12.12	IT
6	5-Mar	11:30	Claire	iPhone 8	Exchange	1.2.3.4	US

✕ Seems Bad

Claire doesn't normally log in at 2 AM

This is not a familiar device for Claire

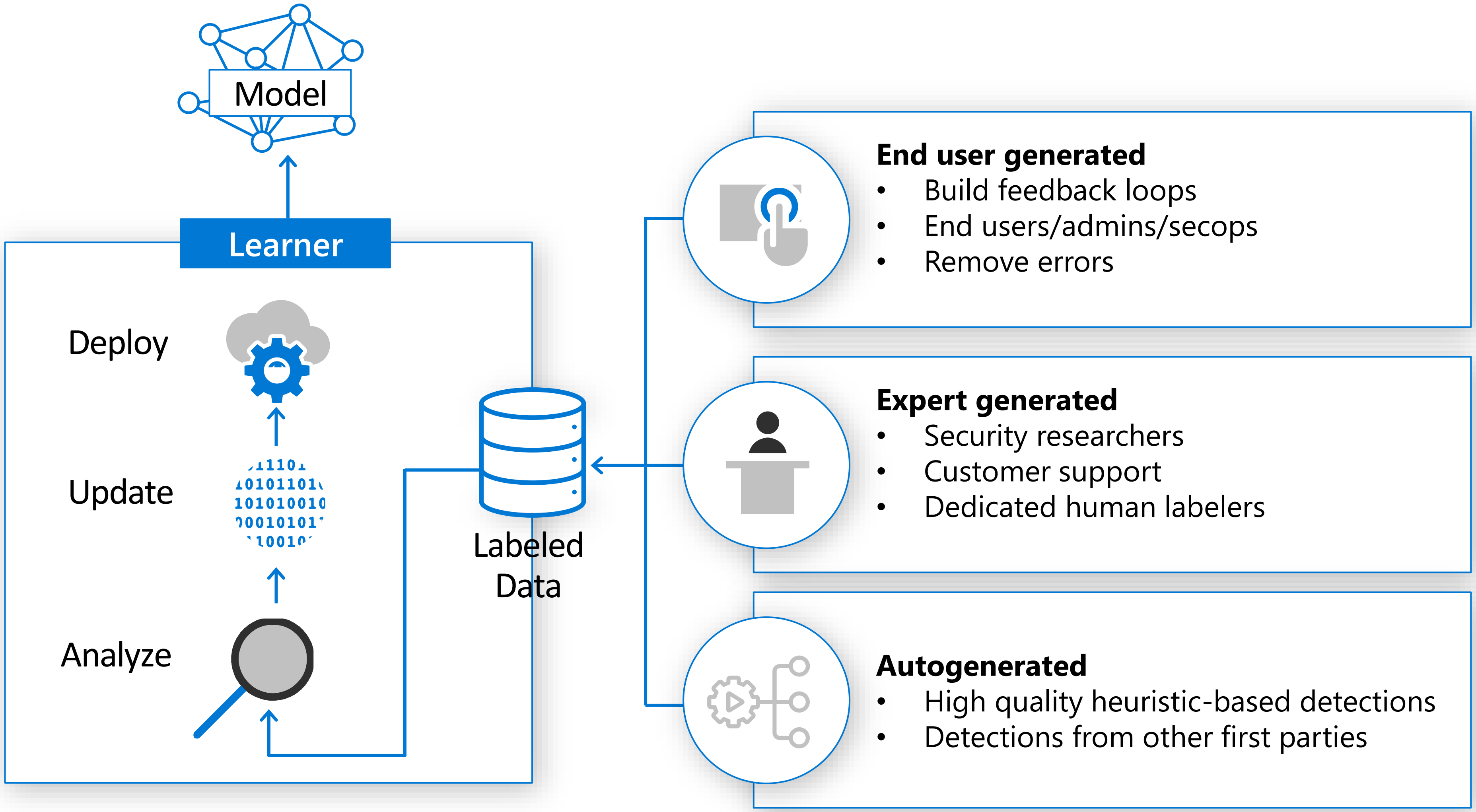
There are 132 other users from different tenants using this IP address

We have never seen Claire log in from Italy

IsNormalTimeOfDay	IsFamiliarDevice	IsFamiliarApp	IsFamiliarIP	IsFamiliarCountry
FALSE	FALSE	FALSE	FALSE	FALSE

Identity Protection is more relevant than ever

Let system intelligence find compromise



End user generated
- Build feedback loops
- End users/admins/secops
- Remove errors

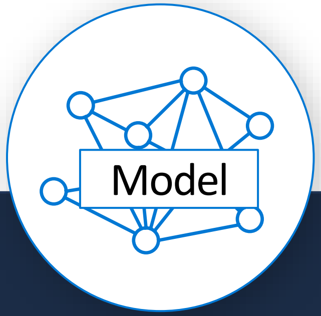
Expert generated
- Security researchers
- Customer support
- Dedicated human labelers

Autogenerated
- High quality heuristic-based detections
- Detections from other first parties

Machine learning

- Better for harder to identify attacks
- Finds patterns in the data
- Less human intervention
- Harder to develop
- Faster to adapt to new patterns

How does ML dynamically determines compromise?

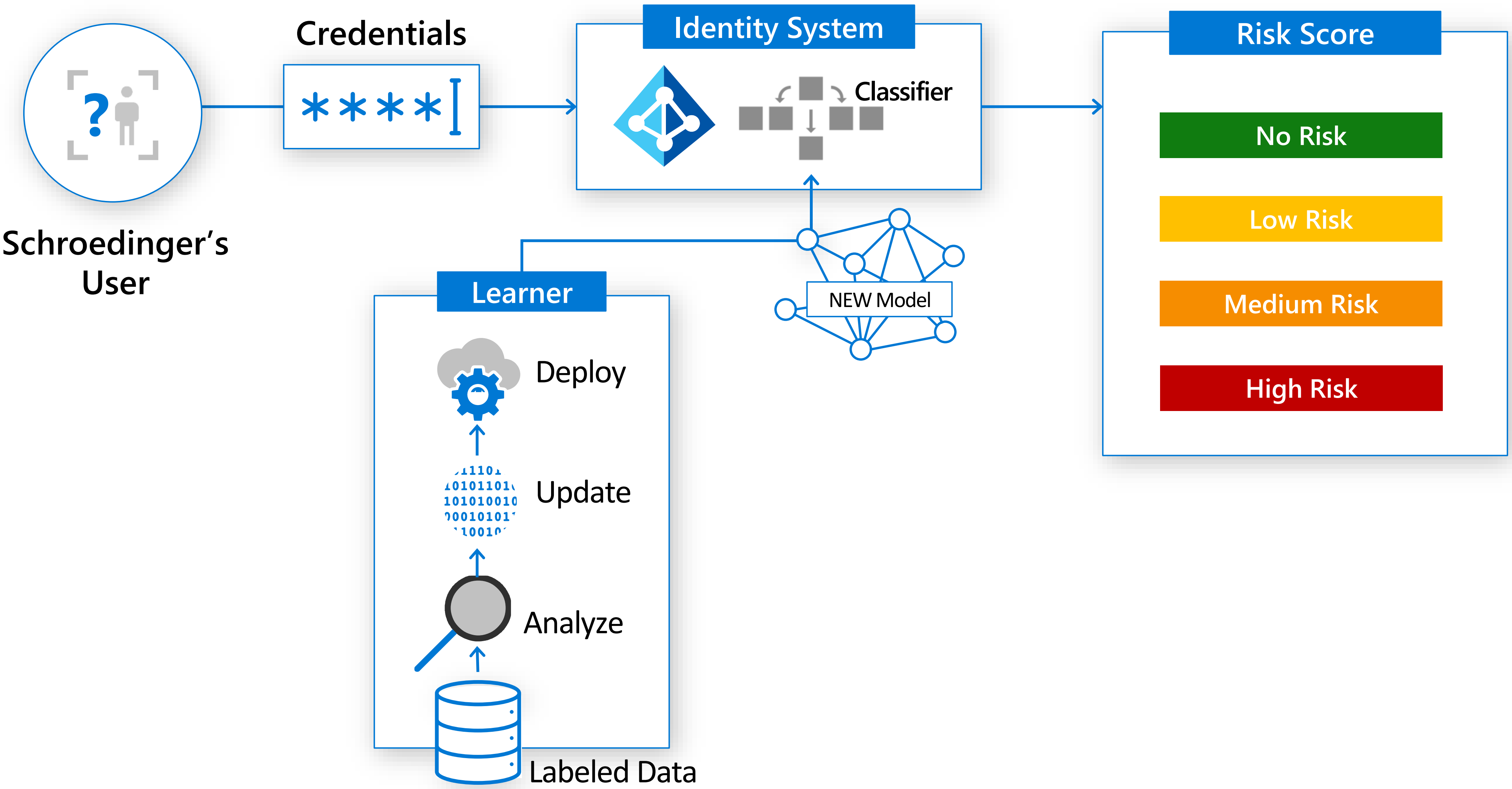


Feature				
IsNormalTimeOfDay	lb			
IsFamiliarDevice	lb	lb	lb	
IsFamiliarApp	lb	lb		
IsFamiliarIP	lb	lb	lb	
IsFamiliarCountry	lb	lb	lb	lb
...				

Model Training indicates what is the most important compromise indicators at that point in time based on the training data

Allows the ML system adapt to new attacks on the fly, just retrain the model

Trained Model sent to Identity System to calculate risk



Risk and Detection Types

User risk

Probability a bad actor has compromised a given identity

Sign-in risk

Probability a given sign-in isn’t authorized by the identity owner

Real-time

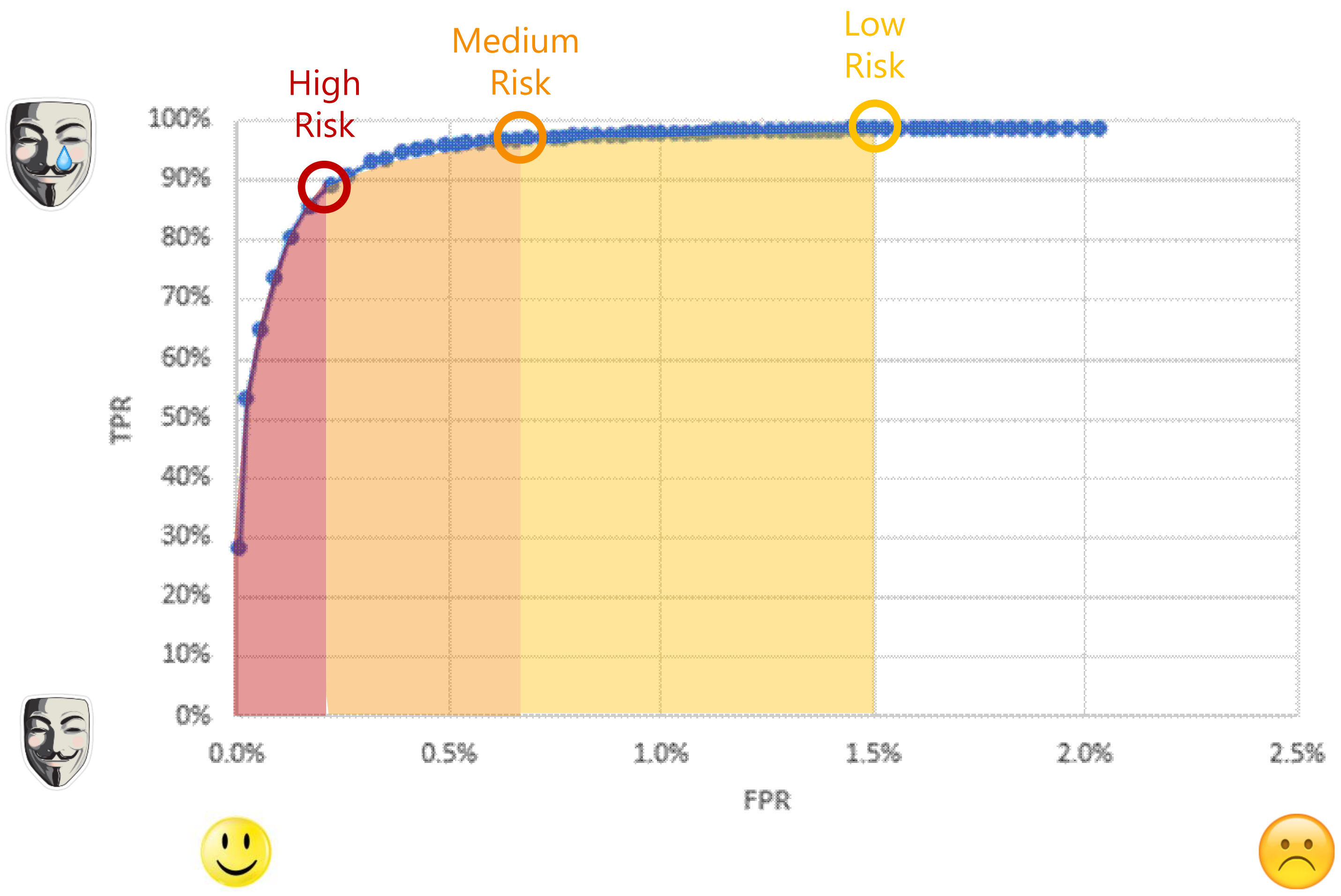
- Fires in real-time i.e. during the sign-in
- Contribute to real-time sign-in risk
- Integrated with Conditional Access sign-in risk-based policies
- Contributes to user risk

Offline

- Fires after the sign-in has taken place
- Contributes to user risk

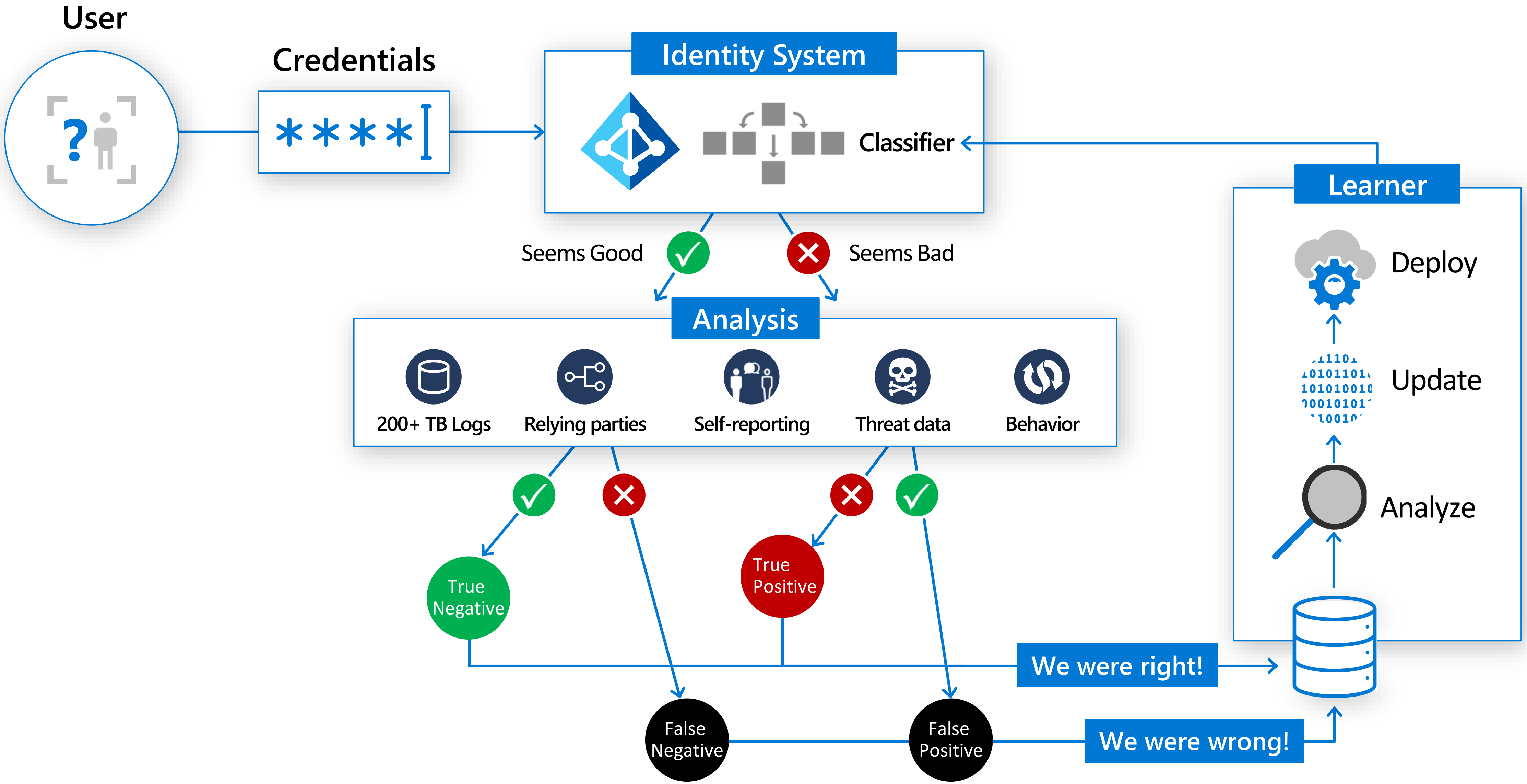
How does Risk Score translate to Risk Decisions?

- Recall (TPR): % of compromise that would be detected
- False Positive Rate (FPR): % of good users we are falsely detecting as compromise
- Pick a score that causes most pain to bad actors with little friction for good users
- To maximize recall: Pick several scores to map to risk levels, e.g High, Medium, Low



*Example values don’t reflect actual thresholds

Let the system adapt to attacks



By the numbers

Billions of evaluations per day

200TB+ of logs parsed per day

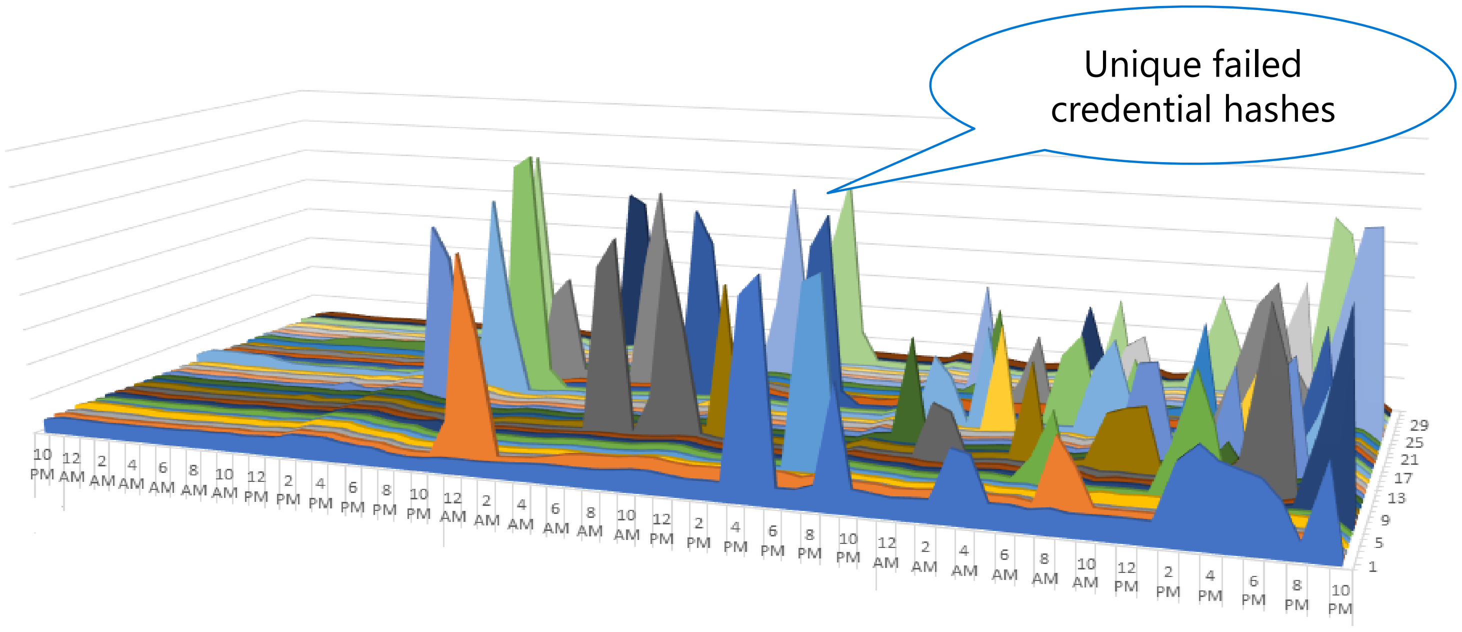
< 1ms evaluation time

Millions of tenants – one identity system means attacks are detected quickly and blocked proactively before other tenants are affected

ML for specific attack patterns: Password Spray

38 % of enterprise compromise

- Password Spray (aka Brute Force, Hammering)
  - Iterate through known account names with most common passwords originating from 100K+ IPs
  - Probability of account compromise by password spray: 1%

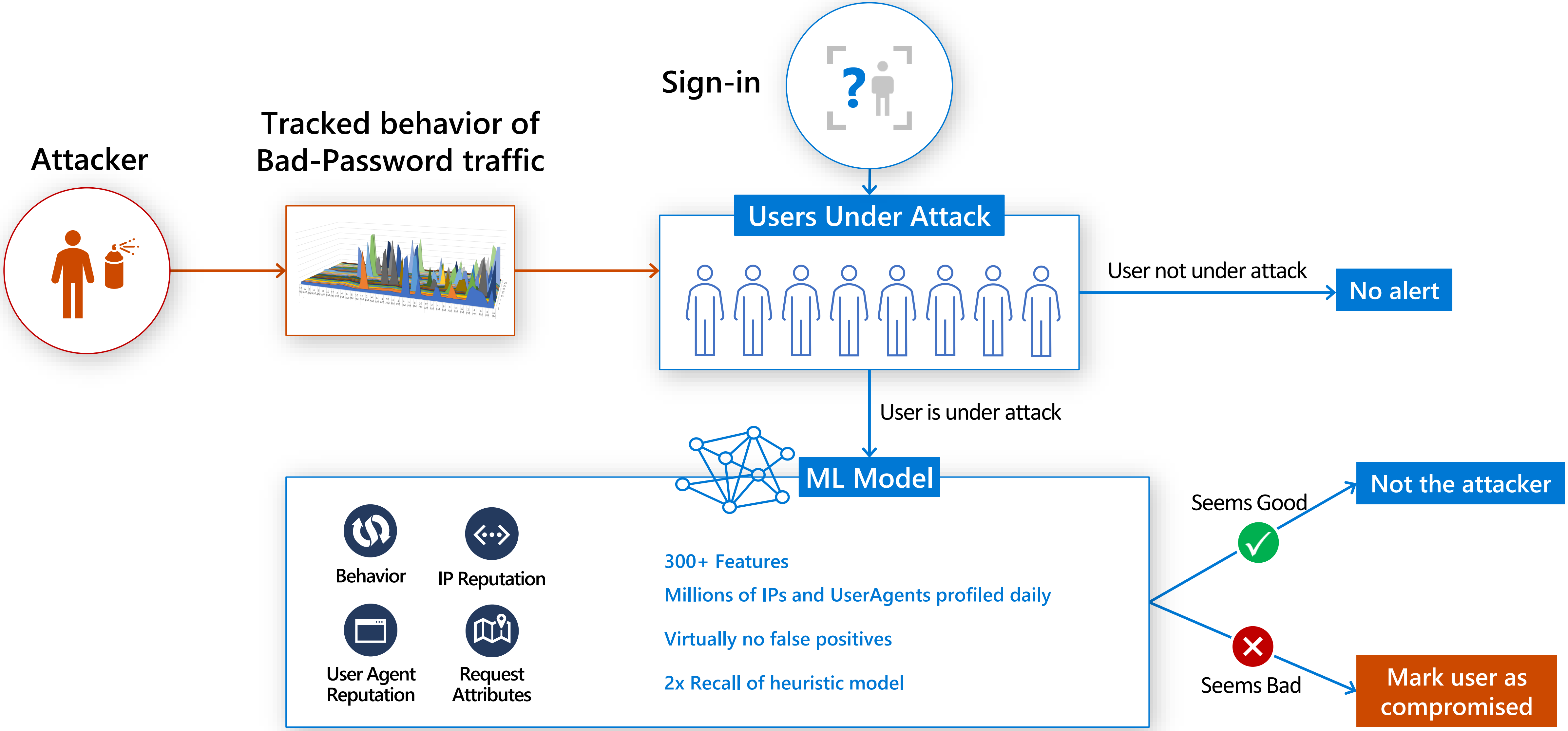


Unique failed credential hashes

Josi@contoso.com	Seahawks2020!
Chance@wingtiptoys.com	Seahawks2020!
Rami@fabrikam.com	Seahawks2020!
TomH@cohowinery.com	Seahawks2020!
AnitaM@cohovineyard.com	Seahawks2020!
EitokuK@redmondbrew.com	Seahawks2020!
Ramanujan@Adatum.com	Seahawks2020!
Maria@Treyresearch.net	Seahawks2020!
LC@adverture-works.com	Seahawks2020!
EW@alpineskihouse.com	Seahawks2020!
info@blueyonderairlines.com	Seahawks2020!
AiliS@fourthcoffee.com	Seahawks2020!
MM39@litwareinc.com	Seahawks2020!
Margie@margiestravel.com	Seahawks2020!
Ling-Pi997@proseware.com	Seahawks2020!

- Heuristic detections look at failures per IP/User
  - This attack type mainly missed because of the distributed nature

Smart Password Spray Detection



Attacker

Tracked behavior of Bad-Password traffic

Sign-in

Users Under Attack

User not under attack

No alert

User is under attack

ML Model

Behavior

IP Reputation

User Agent Reputation

Request Attributes

300+ Features

Millions of IPs and UserAgents profiled daily

Virtually no false positives

2x Recall of heuristic model

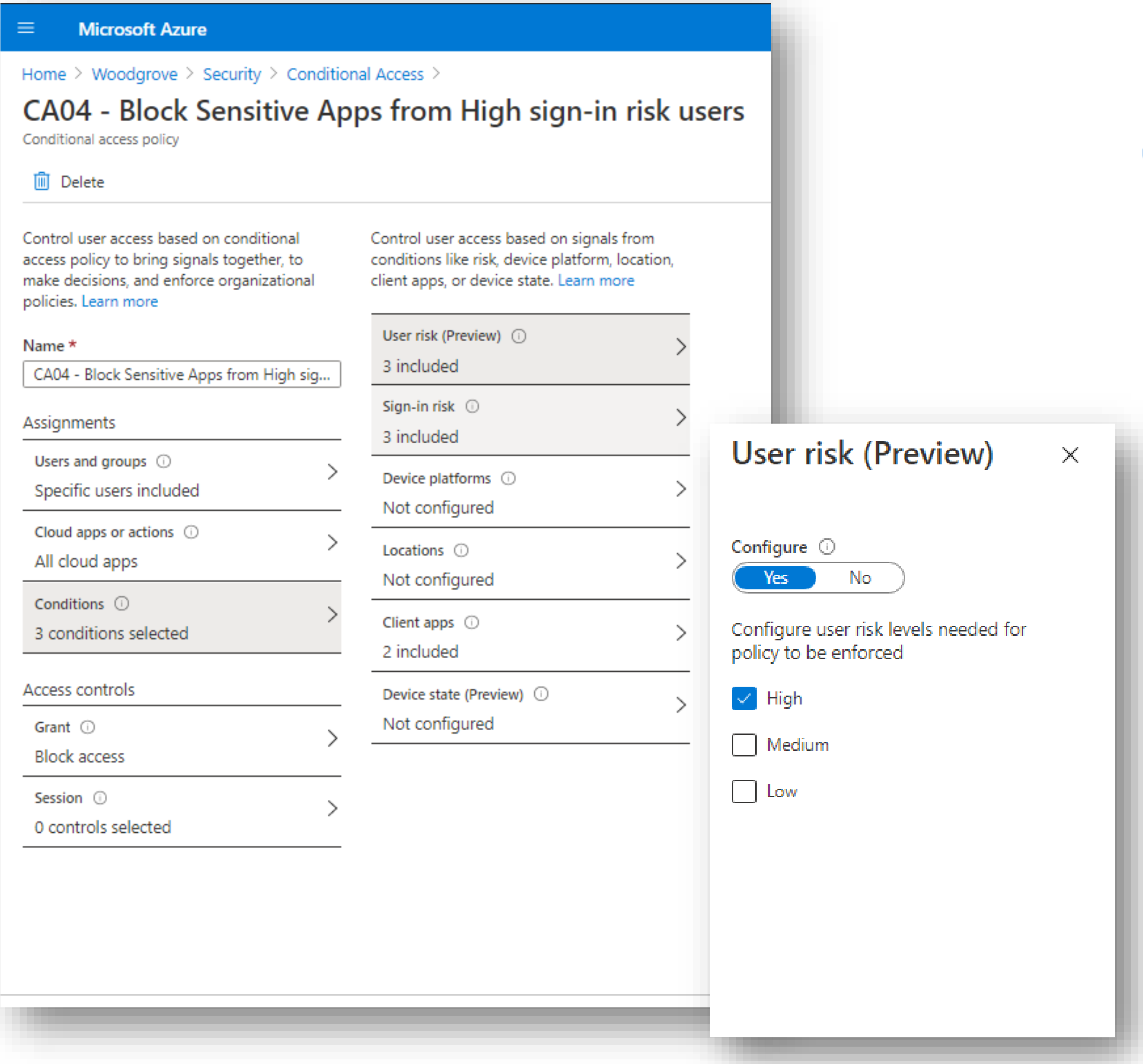
Seems Good

Not the attacker

Seems Bad

Mark user as compromised

Conditional Access and User Risk evaluation



Microsoft Azure

Home > Woodgrove > Security > Conditional Access >

CA04 - Block Sensitive Apps from High sign-in risk users

Conditional access policy

Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

CA04 - Block Sensitive Apps from High sig...

Assignments

Users and groups ⓘ
Specific users included >

Cloud apps or actions ⓘ
All cloud apps >

Conditions ⓘ
3 conditions selected >

Access controls

Grant ⓘ
Block access >

Session ⓘ
0 controls selected >

Control user access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk (Preview) ⓘ
3 included >

Sign-in risk ⓘ
3 included >

Device platforms ⓘ
Not configured >

Locations ⓘ
Not configured >

Client apps ⓘ
2 included >

Device state (Preview) ⓘ
Not configured >

User risk (Preview)

Configure ⓘ

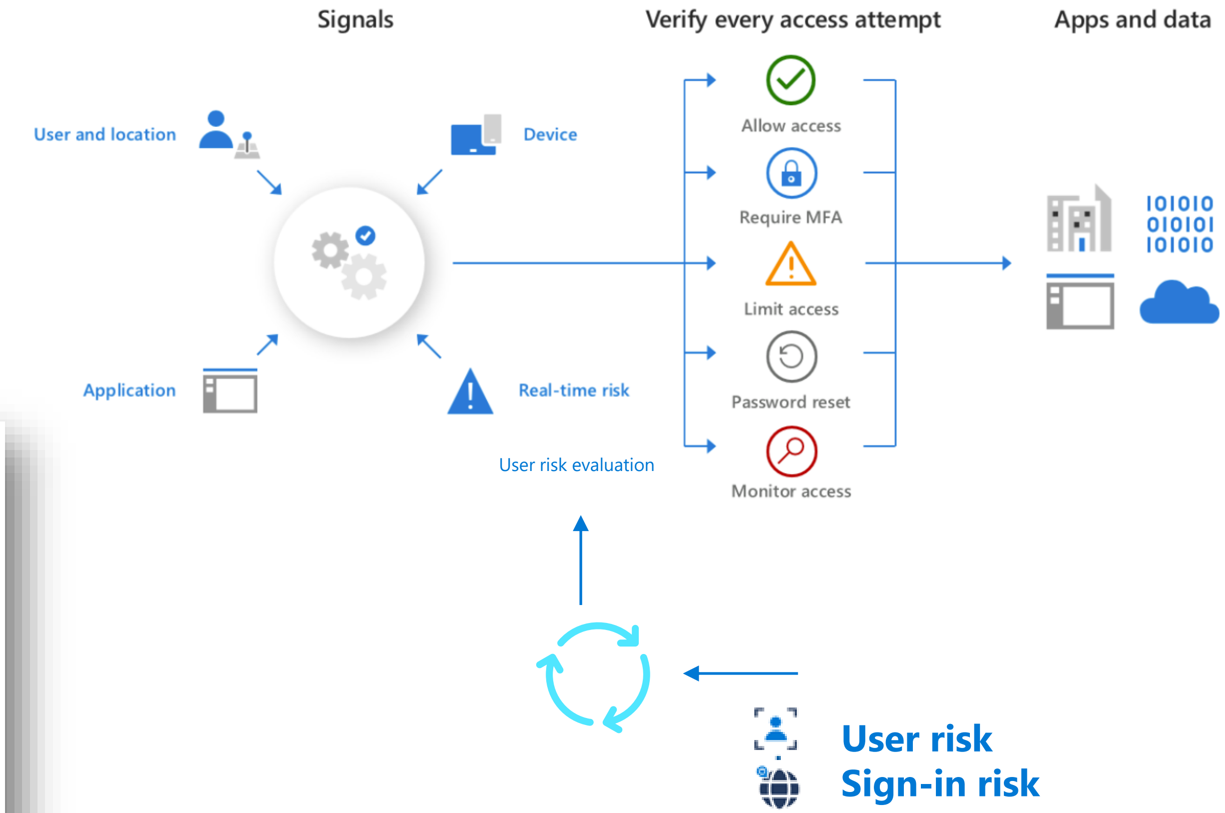
[✓ Yes] No

Configure user risk levels needed for policy to be enforced

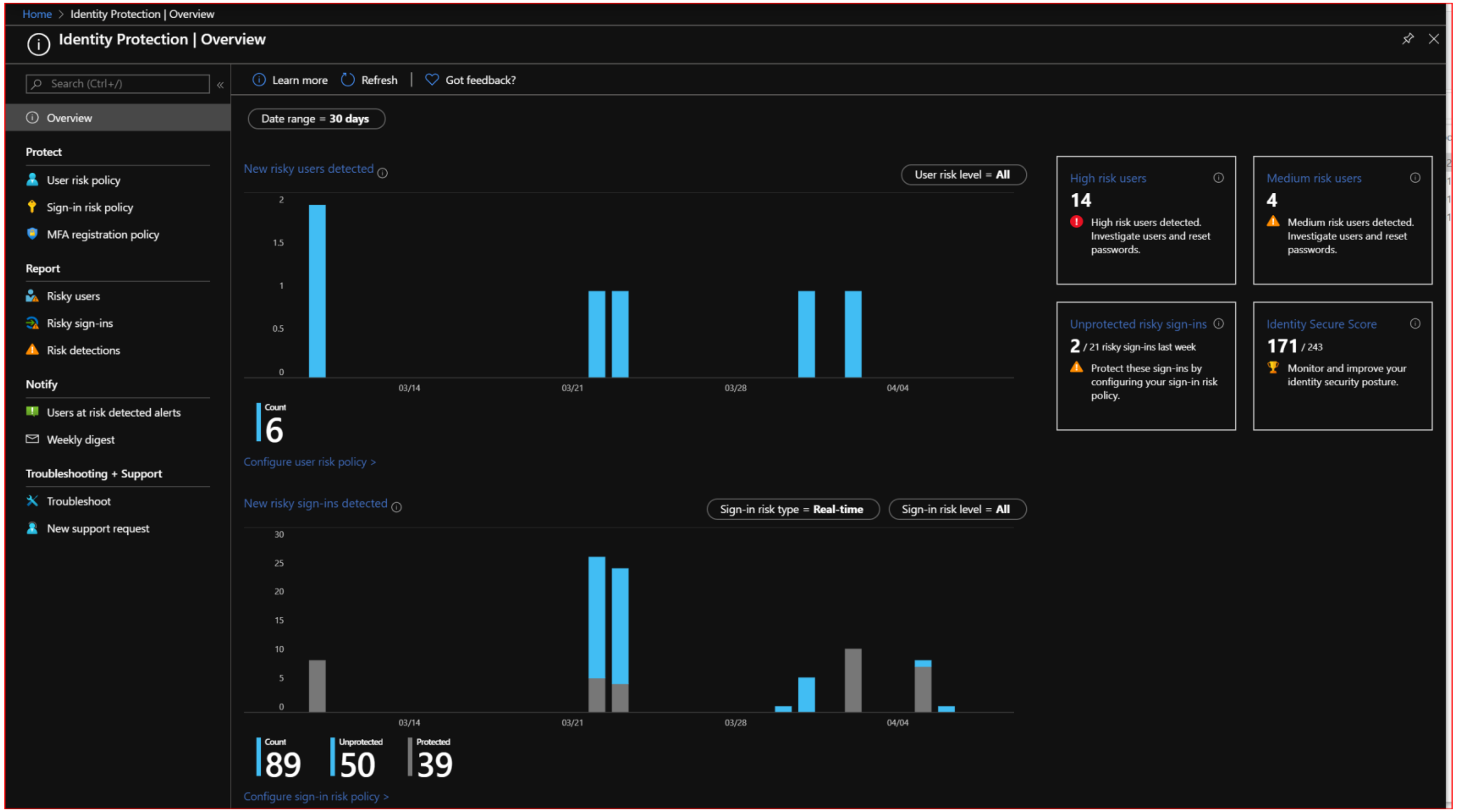
☑ High

□ Medium

□ Low



Demo



Date range = **30 days**

User risk level = **All**

Count 6

Sign-in risk type = **Real-time**

Sign-in risk level = **All**

Count 89

Unprotected 50

Protected 39

High risk users

14

High risk users detected. Investigate users and reset passwords.

Medium risk users

4

Medium risk users detected. Investigate users and reset passwords.

Unprotected risky sign-ins

2 / 21 risky sign-ins last week

Protect these sign-ins by configuring your sign-in risk policy.

Identity Secure Score

171 / 243

Monitor and improve your identity security posture.

What’s new in Identity Protection?

- New powerful APIs and integrations
- Additional risk events
- User risk based conditional access
- End User feedback integration

New Risk APIs in Microsoft Graph

Get real-time Risk detections

Create policies

Manage Compromised Users

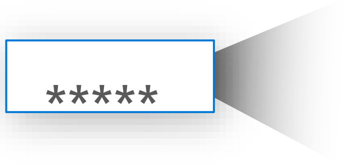
https://graph.microsoft.com

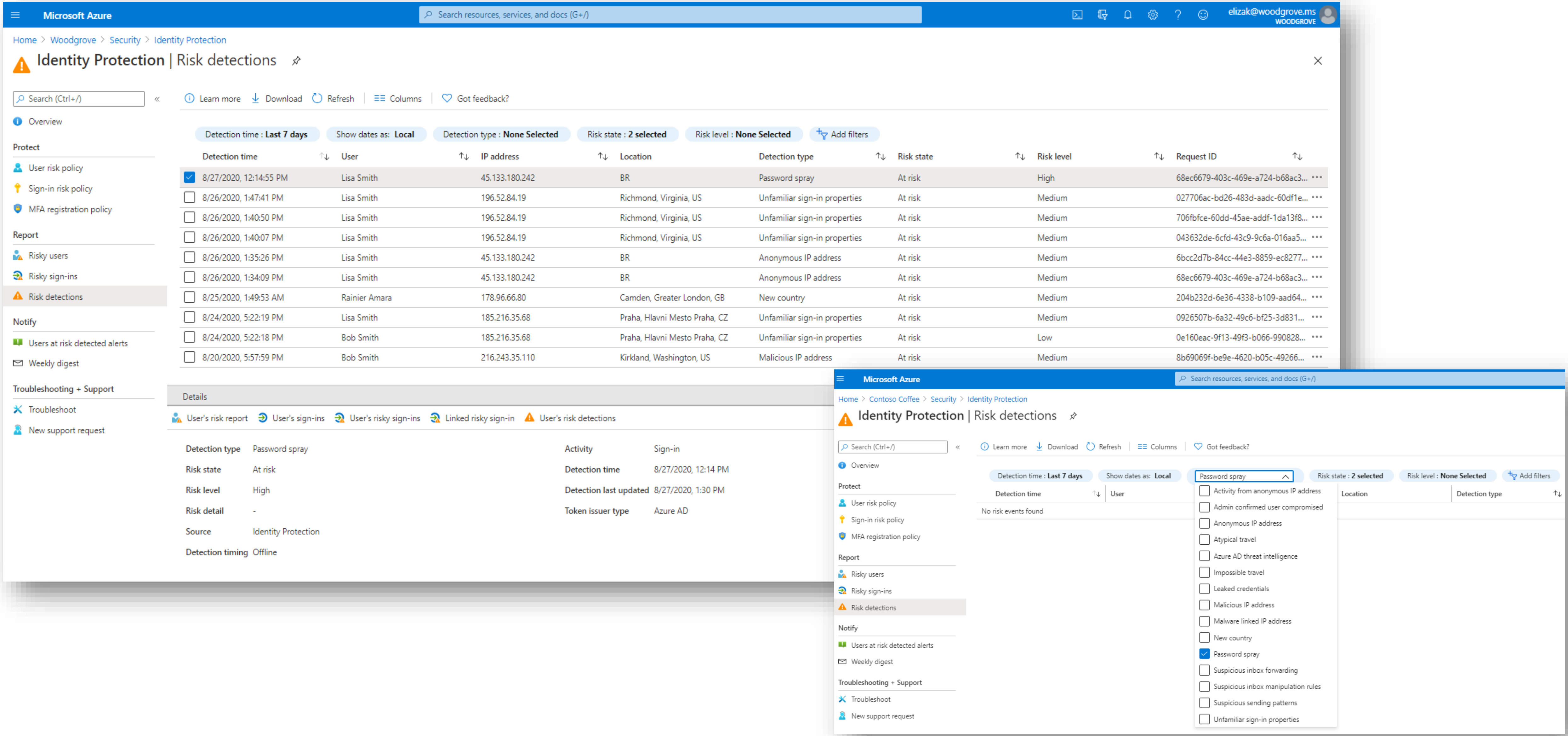
```
GET /riskDetections?$filter=riskEventType eq
microsoft.graph.riskEventType ‘passwordSpray'
{
    "value": [
     "id": "259ba87d-3f99-47b2-b8ff-22365927b36a",
     "isProcessing": false,
     "riskLevel": "high",
     "riskEventType": "passwordSpray",
     "riskState": "atRisk",
     "riskDetail":"none":
     "riskLastUpdatedDateTime": "2020-08
      22T22:18:18.2781812Z",
     "userDisplayName": "Helpdesk Admin",
     "userPrincipalName":
     "dan@contosocoffee1.onmicrosoft.com"
    ]
}

POST identity/conditionalAccess/policies
 {
    "displayName":"Block EXO for non-trusted regions",
    "state": "enabled",
     "conditions": {},
}


POST /riskyUsers/confirmCompromised
{
  "userIds": [
     "259ba87d-3f99-47b2-b9ff-22365927b46a"]
}
```

Password Spray detection





Home > Woodgrove > Security > Identity Protection

Identity Protection | Risk detections

Detection time : **Last 7 days** | Show dates as: **Local** | Detection type : **None Selected** | Risk state : **2 selected** | Risk level : **None Selected** | Add filters

	Detection time	User	IP address	Location	Detection type	Risk state	Risk level	Request ID	
☑	8/27/2020, 12:14:55 PM	Lisa Smith	45.133.180.242	BR	Password spray	At risk	High	68ec6679-403c-469e-a724-b68ac3...	•••
☐	8/26/2020, 1:47:41 PM	Lisa Smith	196.52.84.19	Richmond, Virginia, US	Unfamiliar sign-in properties	At risk	Medium	027706ac-bd26-483d-aadc-60df1e...	•••
☐	8/26/2020, 1:40:50 PM	Lisa Smith	196.52.84.19	Richmond, Virginia, US	Unfamiliar sign-in properties	At risk	Medium	706fbfce-60dd-45ae-addf-1da13f8...	•••
☐	8/26/2020, 1:40:07 PM	Lisa Smith	196.52.84.19	Richmond, Virginia, US	Unfamiliar sign-in properties	At risk	Medium	043632de-6cfd-43c9-9c6a-016aa5...	•••
☐	8/26/2020, 1:35:26 PM	Lisa Smith	45.133.180.242	BR	Anonymous IP address	At risk	Medium	6bcc2d7b-84cc-44e3-8859-ec8277...	•••
☐	8/26/2020, 1:34:09 PM	Lisa Smith	45.133.180.242	BR	Anonymous IP address	At risk	Medium	68ec6679-403c-469e-a724-b68ac3...	•••
☐	8/25/2020, 1:49:53 AM	Rainier Amara	178.96.66.80	Camden, Greater London, GB	New country	At risk	Medium	204b232d-6e36-4338-b109-aad64...	•••
☐	8/24/2020, 5:22:19 PM	Lisa Smith	185.216.35.68	Praha, Hlavni Mesto Praha, CZ	Unfamiliar sign-in properties	At risk	Medium	0926507b-6a32-49c6-bf25-3d831...	•••
☐	8/24/2020, 5:22:18 PM	Bob Smith	185.216.35.68	Praha, Hlavni Mesto Praha, CZ	Unfamiliar sign-in properties	At risk	Low	0e160eac-9f13-49f3-b066-990828...	•••
☐	8/20/2020, 5:57:59 PM	Bob Smith	216.243.35.110	Kirkland, Washington, US	Malicious IP address	At risk	Medium	8b69069f-be9e-4620-b05c-49266...	•••

Details

Detection type	Password spray	Activity	Sign-in
Risk state	At risk	Detection time	8/27/2020, 12:14 PM
Risk level	High	Detection last updated	8/27/2020, 1:30 PM
Risk detail	-	Token issuer type	Azure AD
Source	Identity Protection		
Detection timing	Offline		

Home > Contoso Coffee > Security > Identity Protection

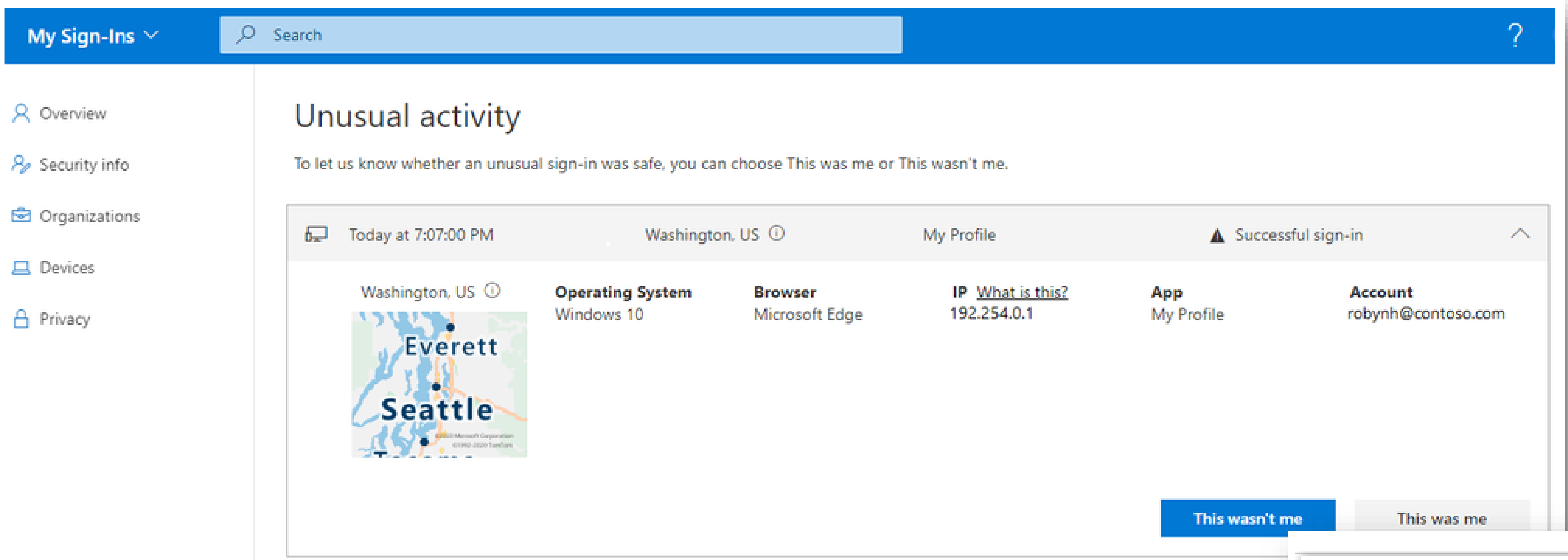
Identity Protection | Risk detections

Detection time : **Last 7 days** | Show dates as: **Local** | Password spray | Risk state : **2 selected** | Risk level : **None Selected** | Add filters

- ☐ Activity from anonymous IP address
- ☐ Admin confirmed user compromised
- ☐ Anonymous IP address
- ☐ Atypical travel
- ☐ Azure AD threat intelligence
- ☐ Impossible travel
- ☐ Leaked credentials
- ☐ Malicious IP address
- ☐ Malware linked IP address
- ☐ New country
- ☑ Password spray
- ☐ Suspicious inbox forwarding
- ☐ Suspicious inbox manipulation rules
- ☐ Suspicious sending patterns
- ☐ Unfamiliar sign-in properties

Detection time	User	Location	Detection type
No risk events found			

My sign-ins with “This wasn’t me” functionality



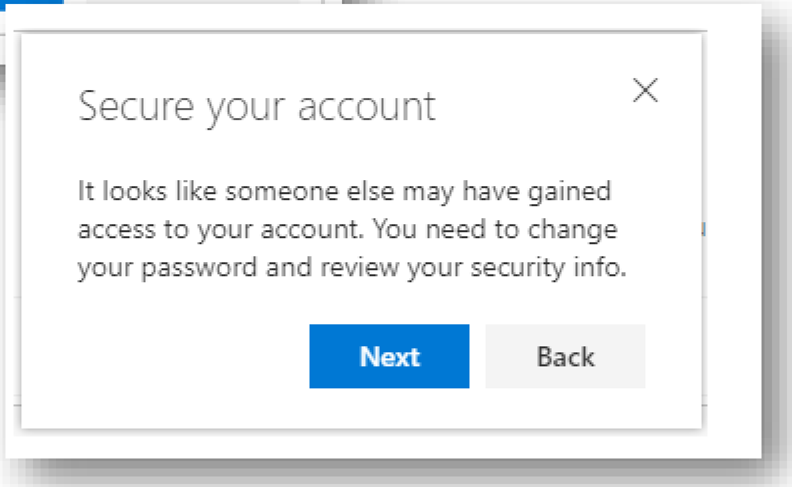
Unusual activity

To let us know whether an unusual sign-in was safe, you can choose This was me or This wasn't me.

Today at 7:07:00 PM | Washington, US | My Profile | Successful sign-in

Washington, US

Operating System	Browser	IP What is this?	App	Account
Windows 10	Microsoft Edge	192.254.0.1	My Profile	robynh@contoso.com



Secure your account

It looks like someone else may have gained access to your account. You need to change your password and review your security info.

My Sign-Ins now shows unusual activity and you can report “This wasn’t me” via end user feedback. If a risky sign-in was automatically detected, it surfaces as “Unusual activity”.

What should you do now?

- Enable Identity Protection on your tenant and review the Identity Protection reports
- Generate CA (Conditional Access) User and Session Risk policies in Report only mode
- Turn on MFA for all users
- Enable Password Hash Sync
- Use Conditional Access to block legacy authentication

https://aka.ms/enableMFA
https://aka.ms/zerotrust

CLOUD IDENTITY SUMMIT ‘20

Your Feedback is important!

http://feedback.identitysummit.cloud/

Thanks to our sponsors!

DICE
DEBEKA
INNOVATION
CENTER

yubico