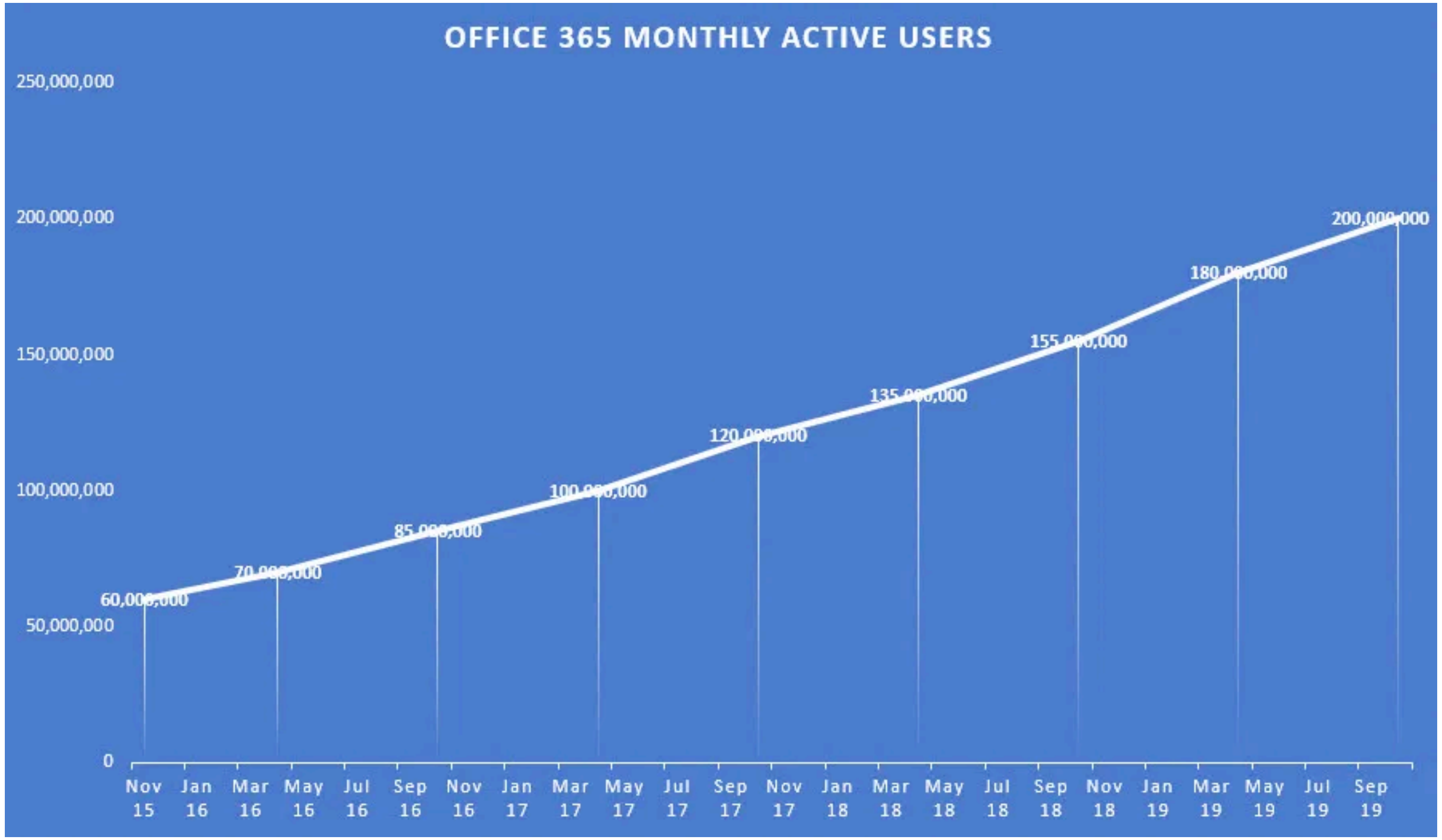
VECTRA®

Practicing “Safe SaaS” for Microsoft Office 365

Marc Drouvé, Security Engineer Manager DACH/EE
mdrouve@vectra.ai
+49 179 5090040

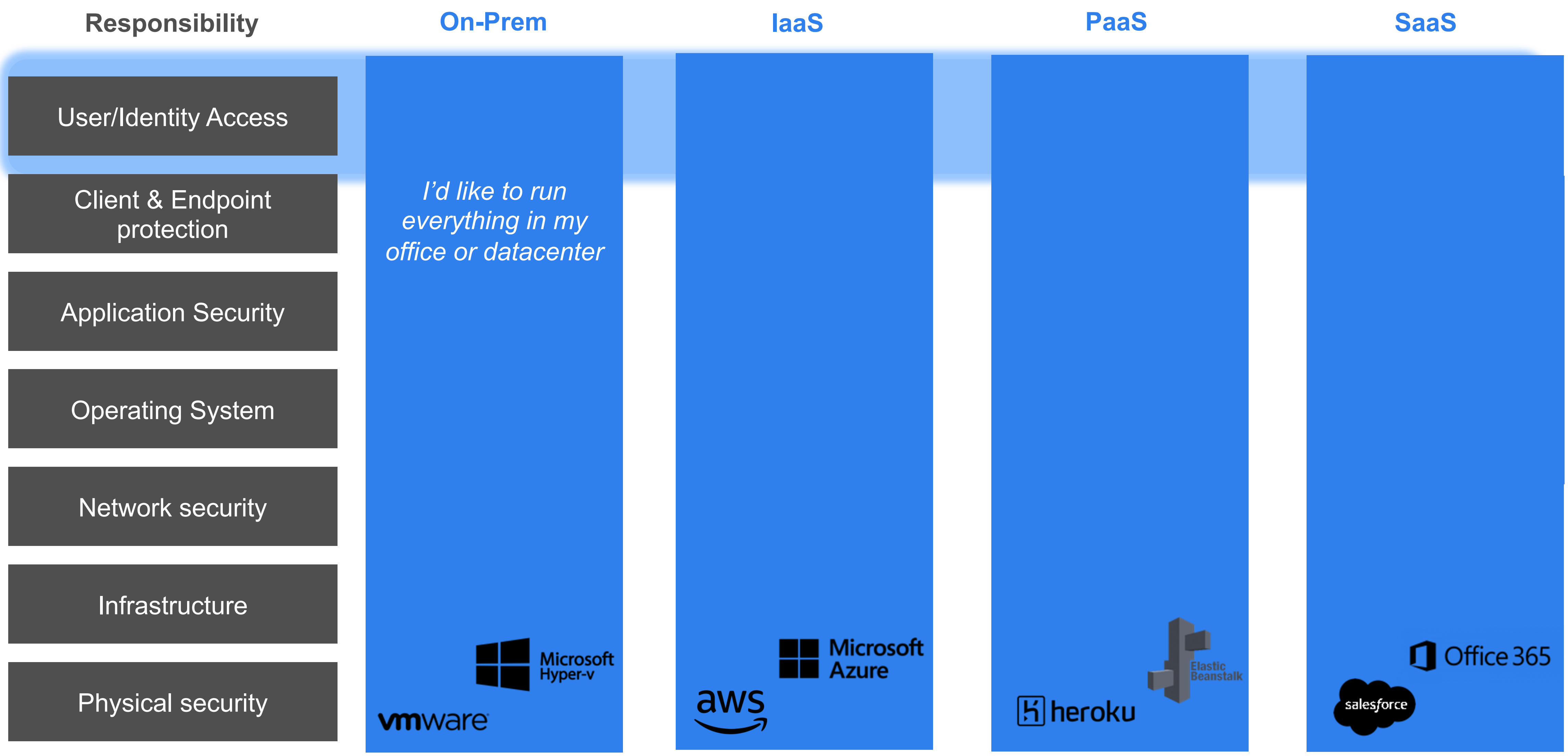
No surprises, Office 365 is widely used

>200,000,000 active users each month



office365itpros.com/2019/10/24/office-365-hits-200-million-monthly-active-users/

Cloud is a shared risk / responsibility model



I'd like to run everything in my office or datacenter

🟦 You ⬛ Cloud Provider

Cloud security expertise is hard to find

Cloud security is complex to configure

Focus is on prevention, not detection

Cloud security implementations are siloed

Legacy on-prem tools don’t work in the cloud

No consistency across Cloud Service Providers

Current cloud security solutions are inefficient

VECTRA®

Office 365 is a high-value attack target

Valuable business data + repeatable tactics make Microsoft 365 an attractive target

- IP and trade secrets
- Plans and project data
- Financial data
- Customer and employee data

Consequences

- Subversion
- Espionage
- Ransom
- Theft

Microsoft
Office 365
S
O
E
T
W
P
Y
S
X

Understanding Office 365 attacks

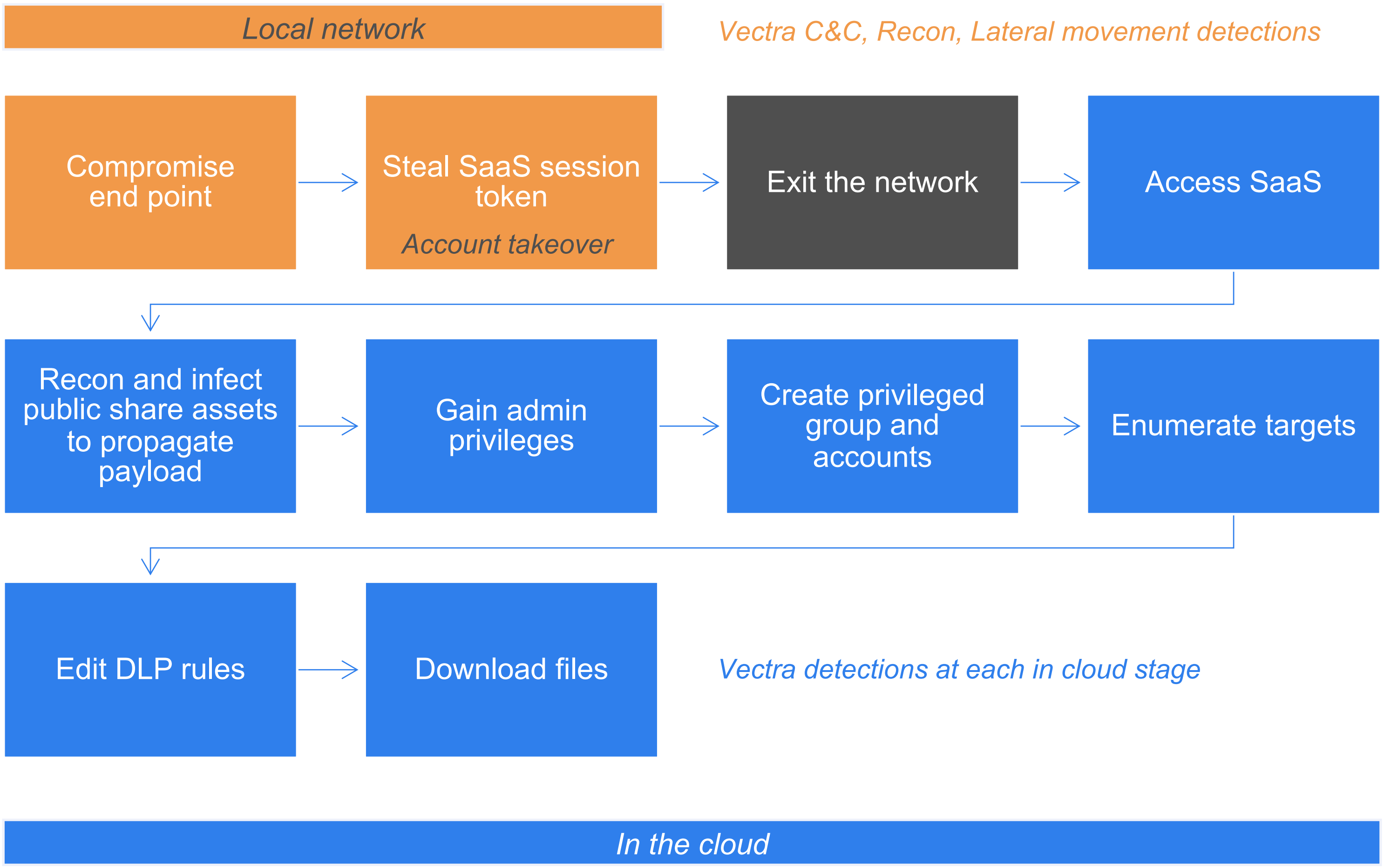
Account Takeover in Office 365 has become the largest threat vector in the cloud

SaaS attacks have deeper impact, as they make it easy to move around laterally

Even with the rising adoption of incremental security approaches like multi-factor authentication, access controls continue to be circumvented.

40%
2018
2019

Visibility into MFA bypass SaaS attack



Local network

Vectra C&C, Recon, Lateral movement detections

Compromise end point → Steal SaaS session token *Account takeover* → Exit the network → Access SaaS

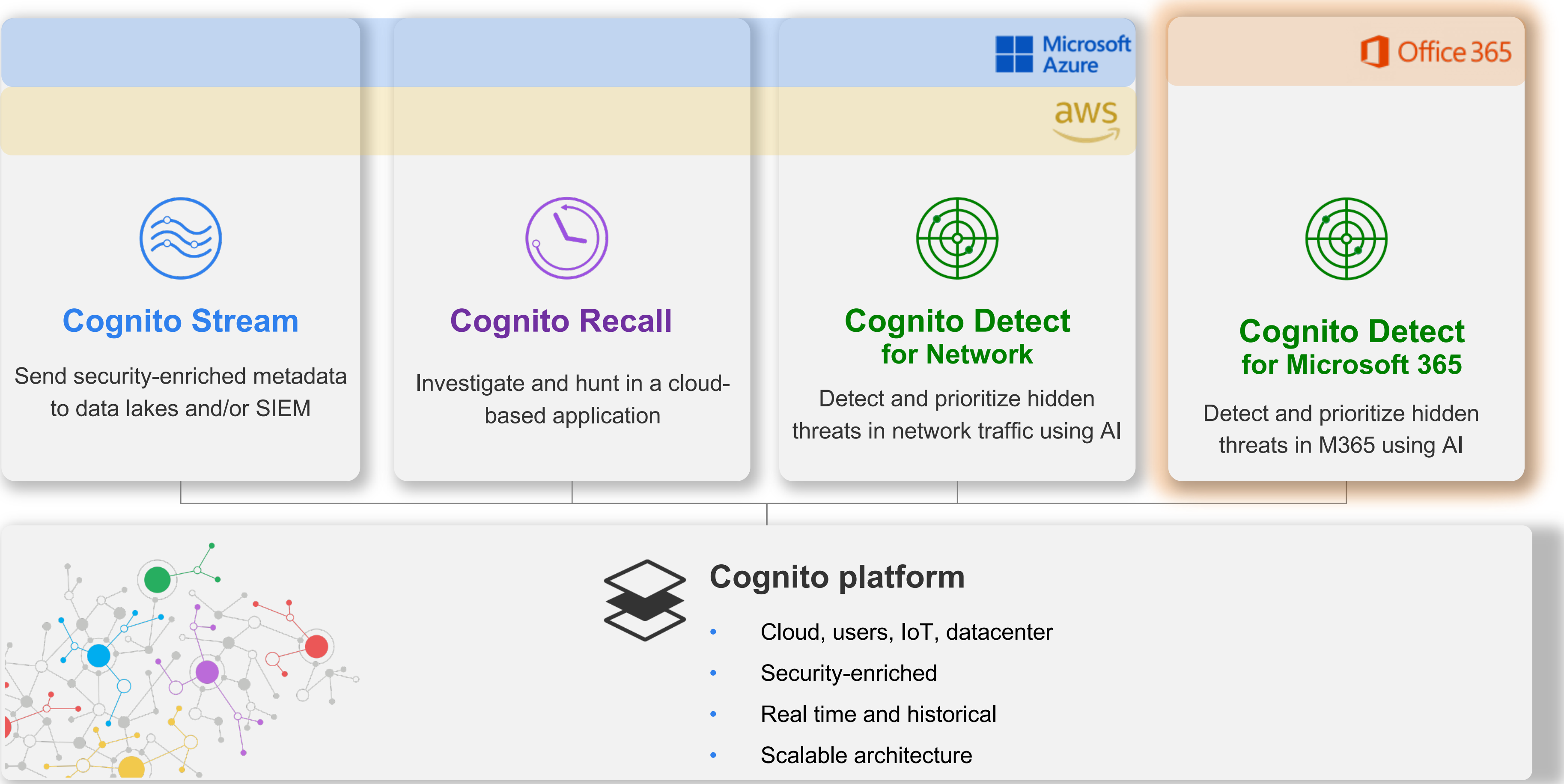
Recon and infect public share assets to propagate payload → Gain admin privileges → Create privileged group and accounts → Enumerate targets

Edit DLP rules → Download files

Vectra detections at each in cloud stage

In the cloud

Cognito, the AI-powered network detection and response (NDR) platform



Cognito Stream

Send security-enriched metadata to data lakes and/or SIEM

Cognito Recall

Investigate and hunt in a cloud-based application

Cognito Detect for Network

Detect and prioritize hidden threats in network traffic using AI

Cognito Detect for Microsoft 365

Detect and prioritize hidden threats in M365 using AI

Cognito platform

- Cloud, users, IoT, datacenter
- Security-enriched
- Real time and historical
- Scalable architecture

Ask yourself…

If I had a compromised Microsoft Office 365 account right now, *(how)* **would I know**?

Get answers with Cognito Detect for Office 365

Find post-compromise attacker behaviors in Office 365 before it too late

- **Infiltration and elevation:** Brute force, adding users and privileges to groups, staging malware, etc.
- **Reconnaissance:** accessing files in unusual ways; listing users, files, and shares, etc.
- **Persistence and evasion:** installing apps to keep access, changing policy and logging, turning off DLP, etc.
- **Exfil and destruction:** creating mail sinks, sharing and downloading files, etc.

Covering key areas of the MITRE ATT&CK matrix for Office 365

MITRE ATT&CK®

TTP	Tactic covered by =>1 Cognito model
TTP	Addressed via integrations

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
Spear phishing Link	Account Manipulation	Valid Accounts	App Access Token	Account Manipulation	Account Discovery	App Access Token	Email Collection
Valid Accounts	Create Account		Redundant Access	Brute Force	Cloud Service Dashboard	Internal Spear phishing	
	Office Application Start		Valid Accounts	**Steal App Access Token**	Cloud Service Discovery	**Web Session Cookie**	
	Redundant Access		**Web Session Cookie**	**Steal Web Session Cookie**	Permission Groups		
	Valid Accounts						

attack.mitre.org/matrices/enterprise/cloud/office365/

25+ Attacker Behavior models optimized for Microsoft 365

VECTRA®

Keeping your Office 365 deployments safe

Stop the largest attack vector in Microsoft 365

30% of organisations suffer account takeovers every month. Vectra understands attacker behavior and account privilege in SaaS applications, allowing you to put an end to breaches.

Attackers don’t operate in silos, your security solution shouldn’t either

Track attacker activity pivoting between on-premise, data center, IaaS and SaaS. All from a single place.

Microsoft security telemetry can be overwhelming and feel disjointed. Vectra’s AI models put it all together

Triage and enrich the security data from Microsoft 365 without having to deploy sensors. Make your business safe in the cloud in minutes.

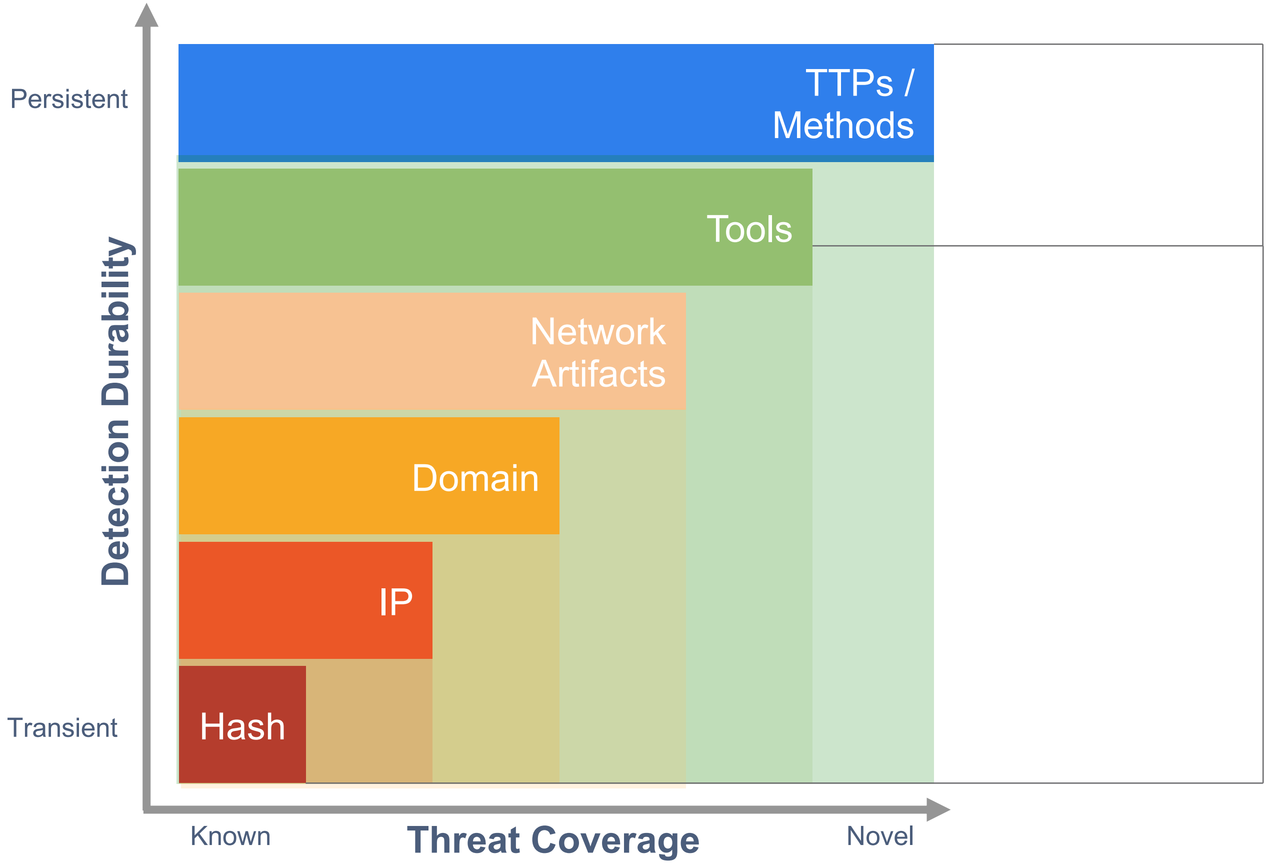
What makes Vectra uniquely valuable?

Correlate across hybrid, multi-cloud and on-prem

Automated deployment with a rich integration ecosystem

High-Fidelity, low noise alerts with enriched metadata for threat hunting and investigation

Looking for what the threat does



Durable coverage

- Both novel and known attacks
- Difficult and expensive to evade

Fast, labeled coverage of known threats

- Tools
- Exploits
- Known attacker infrastructure
- Environment-specific indicators

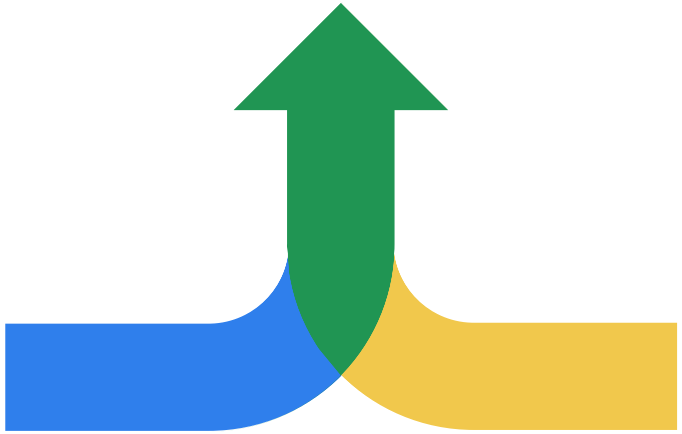
Combine data science and security research

Attacker Behavior models

- High-fidelity detection of things attackers must do
- Find known and unknown

Security Research

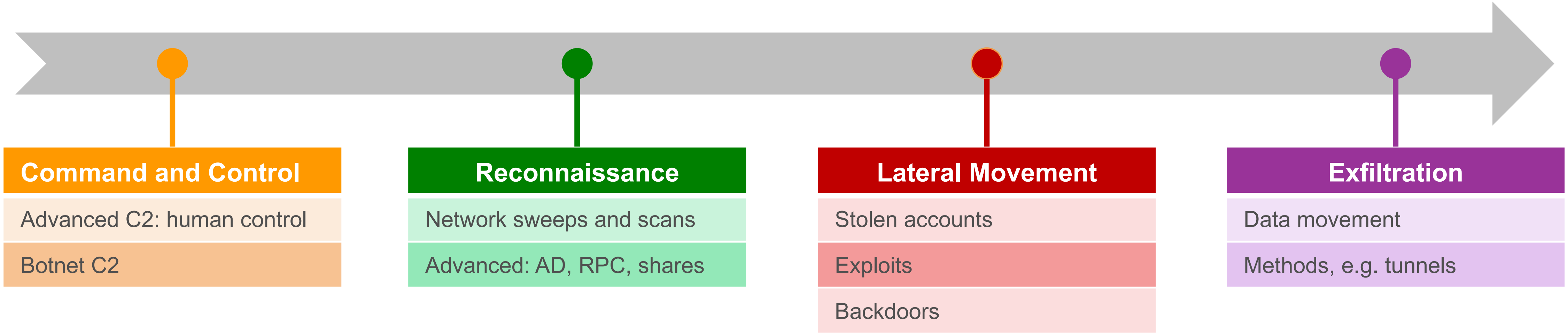
- Identify, prioritize, and characterize fundamental attacker behaviors
- Validate models



Data Science

- Determine best approach to identify behavior
- Develop and tune models

To automate detecting attacker behaviors



Command and Control

- Advanced C2: human control
- Botnet C2

Reconnaissance

- Network sweeps and scans
- Advanced: AD, RPC, shares

Lateral Movement

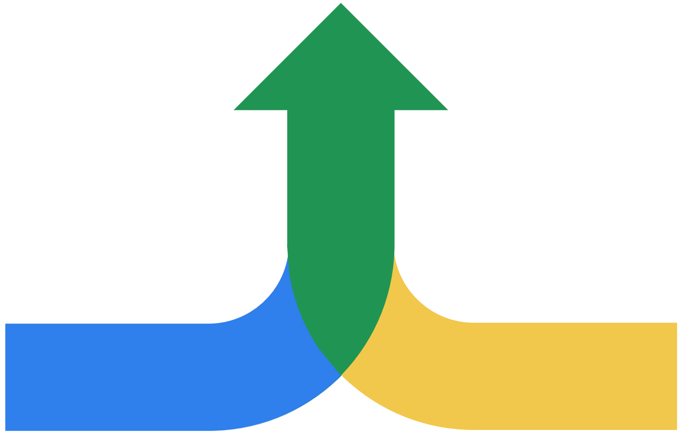
- Stolen accounts
- Exploits
- Backdoors

Exfiltration

- Data movement
- Methods, e.g. tunnels

Security Research

- Identify, prioritize, and characterize fundamental attacker behaviors
- Validate models

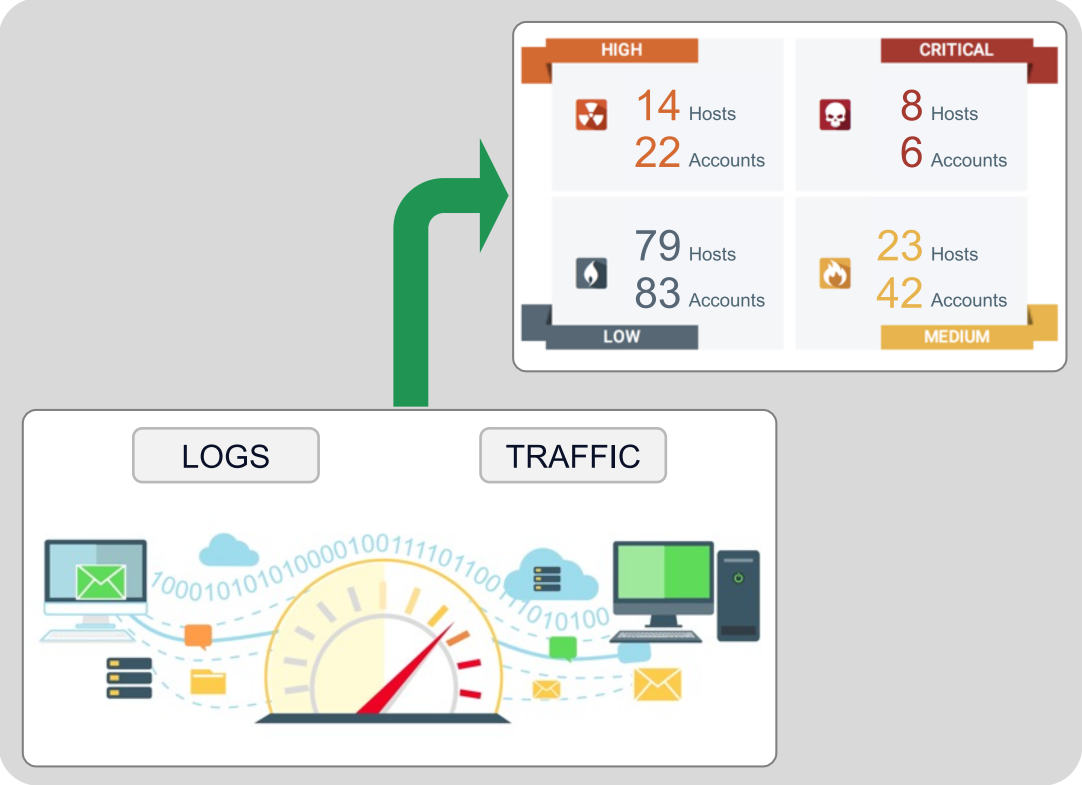


Data Science

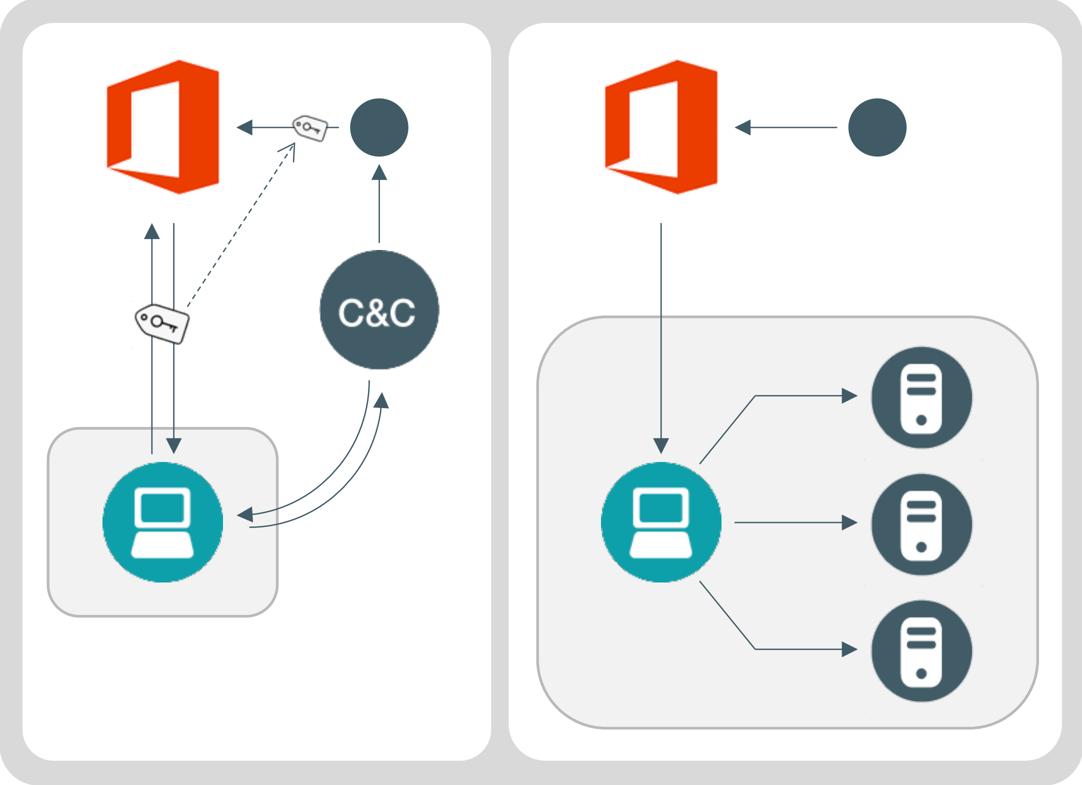
- Determine best approach to identify behavior
- Develop and tune models

The Vectra difference

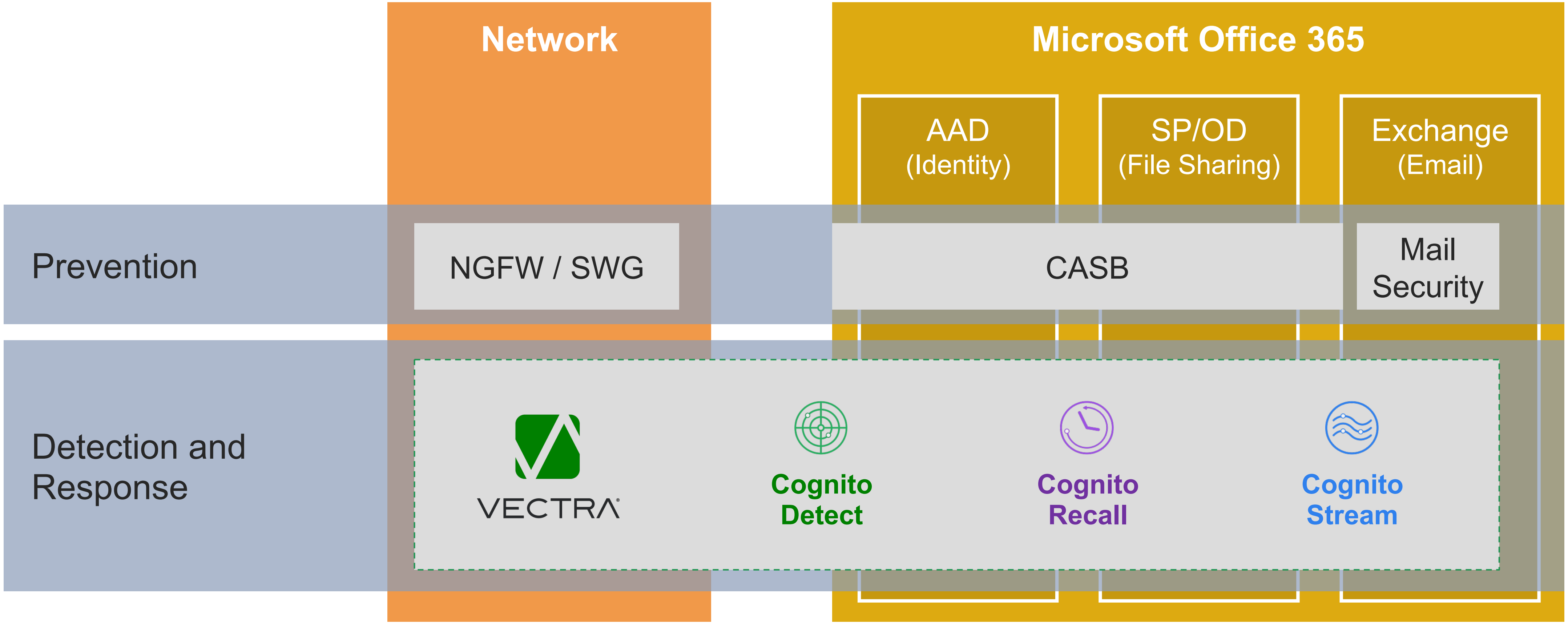
Low Noise / High Signal



LAN-Cloud Pivots

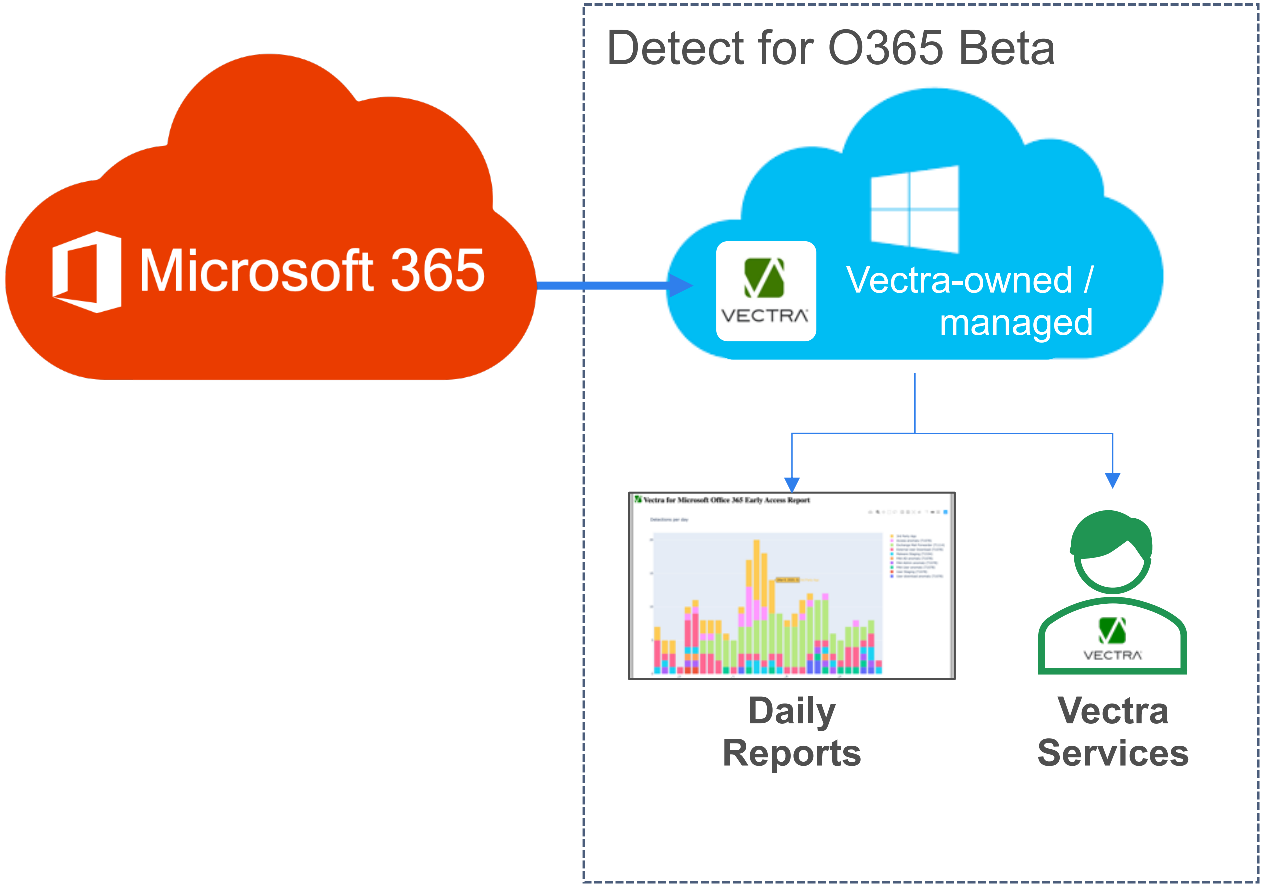


Vectra and Office 365



Access Vectra services for free

Cognito Detect for Microsoft Office 365 Beta program



Easy to start:

- 15-minute onboarding

Gain insight quickly:

- Regular reports
- Help from Vectra consulting analysts

Simple onboarding process

Cognito Detect for Microsoft Office 365 Early Access program

Information we need

- Choice of cloud location
  - EU
  - USA
- Domain of the Microsoft 365 Admin who will authorize Vectra access

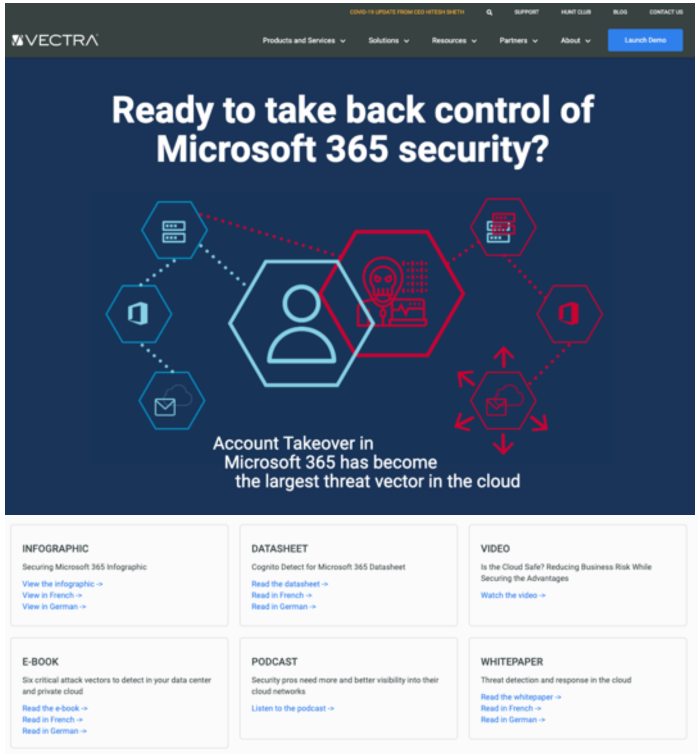
Vectra provided URL to sensor App

Actions for Microsoft 365 Admin

- Follow the URL to install Vectra Microsoft 365 sensor App
- Authenticate to Microsoft 365
- Grant consent to Vectra for 2 privileges
  - ActivityFeed.Read
  - ActivityFeed.ReadDLP

To find out more…

Solution materials



Ready to take back control of Microsoft 365 security?

Account Takeover in Microsoft 365 has become the largest threat vector in the cloud

INFOGRAPHIC

Securing Microsoft 365 Infographic

View the infographic ->
View in French ->
View in German ->

DATASHEET

Cognito Detect for Microsoft 365 Datasheet

Read the datasheet ->
Read in French ->
Read in German ->

VIDEO

Is the Cloud Safe? Reducing Business Risk While Securing the Advantages

Watch the video ->

E-BOOK

Six critical attack vectors to detect in your data center and private cloud

Read the e-book ->
Read in French ->
Read in German ->

PODCAST

Security pros need more and better visibility into their cloud networks

Listen to the podcast ->

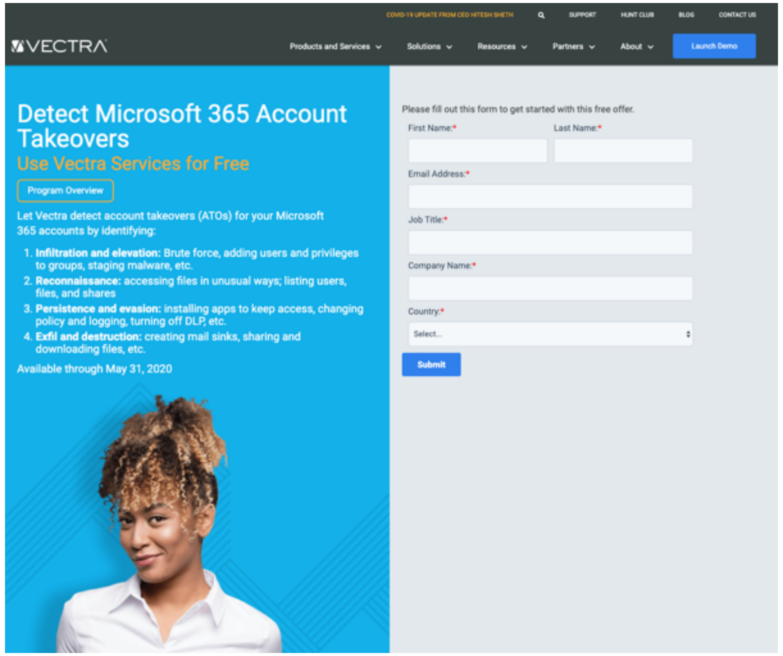
WHITEPAPER

Threat detection and response in the cloud

Read the whitepaper ->
Read in French ->
Read in German ->

www.vectra.ai/microsoft365

Early access program requests



Detect Microsoft 365 Account Takeovers

Use Vectra Services for Free

Let Vectra detect account takeovers (ATOs) for your Microsoft 365 accounts by identifying:

1. **Infiltration and elevation:** Brute force, adding users and privileges to groups, staging malware, etc.
2. **Reconnaissance:** accessing files in unusual ways; listing users, files, and shares
3. **Persistence and evasion:** installing apps to keep access, changing policy and logging, turning off DLP, etc.
4. **Exfil and destruction:** creating mail sinks, sharing and downloading files, etc.

Available through May 31, 2020

Please fill out this form to get started with this free offer.

First Name:* Last Name:*

Email Address:*

Job Title:*

Company Name:*

Country:*

Select...

www.vectra.ai/microsoft365-program

VECTRA

VECTRA®

Q&A

VECTRA®

Thank you