EBOOK

Is Your SOC Hybrid Attack Ready?

As hybrid attacks cause new challenges for SOCs, there are three key areas defenders can focus on to see, keep pace and stop attackers.

VECTRA®

Security teams have no shortage of responsibilities. Yet in between all of the patching and managing vulnerabilities, responding to alerts, meetings with leadership, reporting, ensuring compliance, educating employees and managing an array of other internal risks and beyond — they still have to stop actual cyberattacks.

However, today when that time comes it means a compromise has already happened — an attacker is inside your environment working to progress. So, what is actually needed to make sure your SOC is ready to stop a post compromise hybrid attack?

Here, we'll take a close look at what makes today's hybrid attacks so difficult to detect and stop by looking through the lens of a SOC analyst. You'll see:

1. What's makes prioritizing attacks in today's hybrid environments so difficult.
2. How attackers move beyond preventative security and progress inside a hybrid environment.
3. Three areas defenders can focus efforts to detect and prioritize today's attacks.

A majority of SOC analysts say these have significantly increased in the past three years[1]:

↑ **63%** size of organization's attack surface

↑ **70%** number of security tools

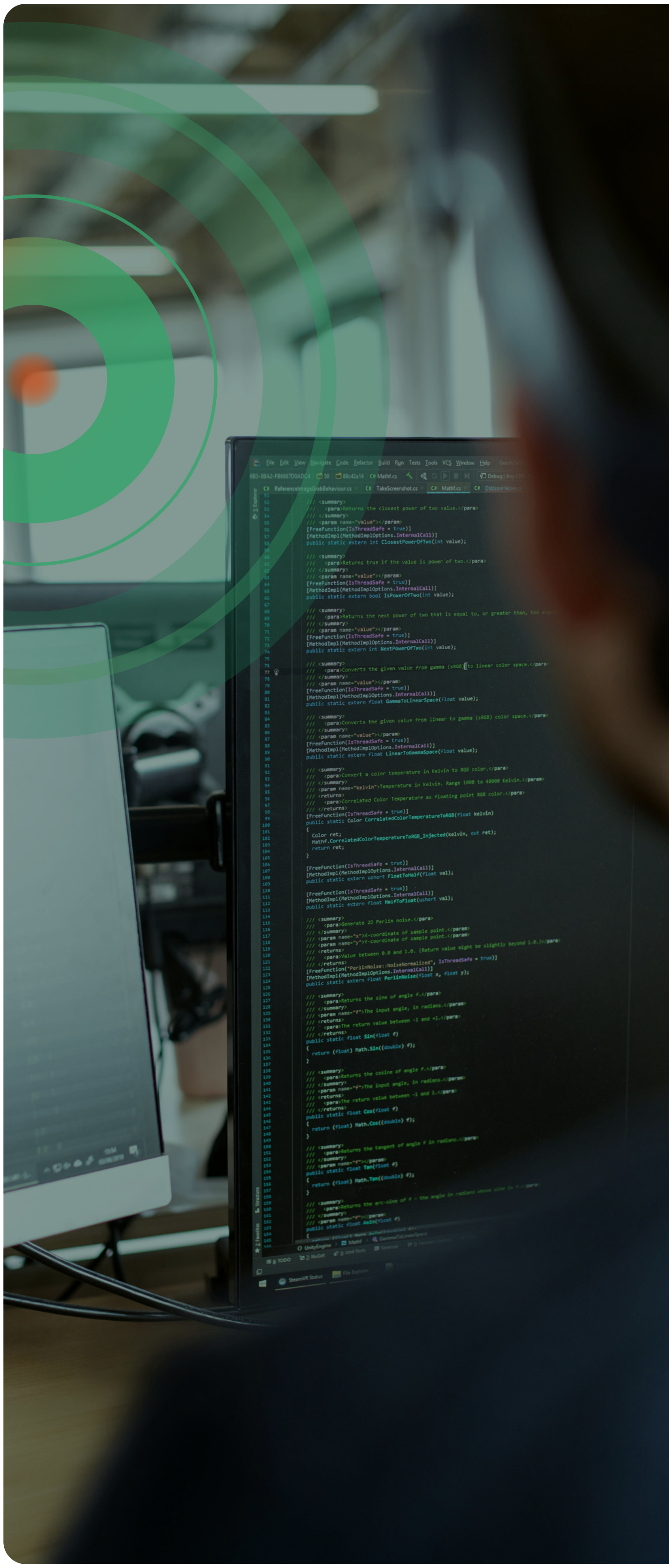
↑ **66%** alerts managed

[1] 2023 State of Threat Detection Report: The Defenders' Dilemma

Table of Contents

What is a hybrid attack?

Hybrid attacks can start with anyone or anything, move anywhere at any time at speed to disrupt business operations at scale, despite having every preventative measure in place.



Why is it so difficult to defend against a hybrid attack?

They're like finding THE NEEDLE in a stack of needles because of three things:

1. **Exposure**
   Getting integrated real-time coverage across the hybrid attack surface is complex.
2. **Latency**
   Correlating individual alert streams to get accurate threat signal is highly manual.
3. **Noise**
   Gaining control of attacks hidden in a mess of alert noise is close to impossible.

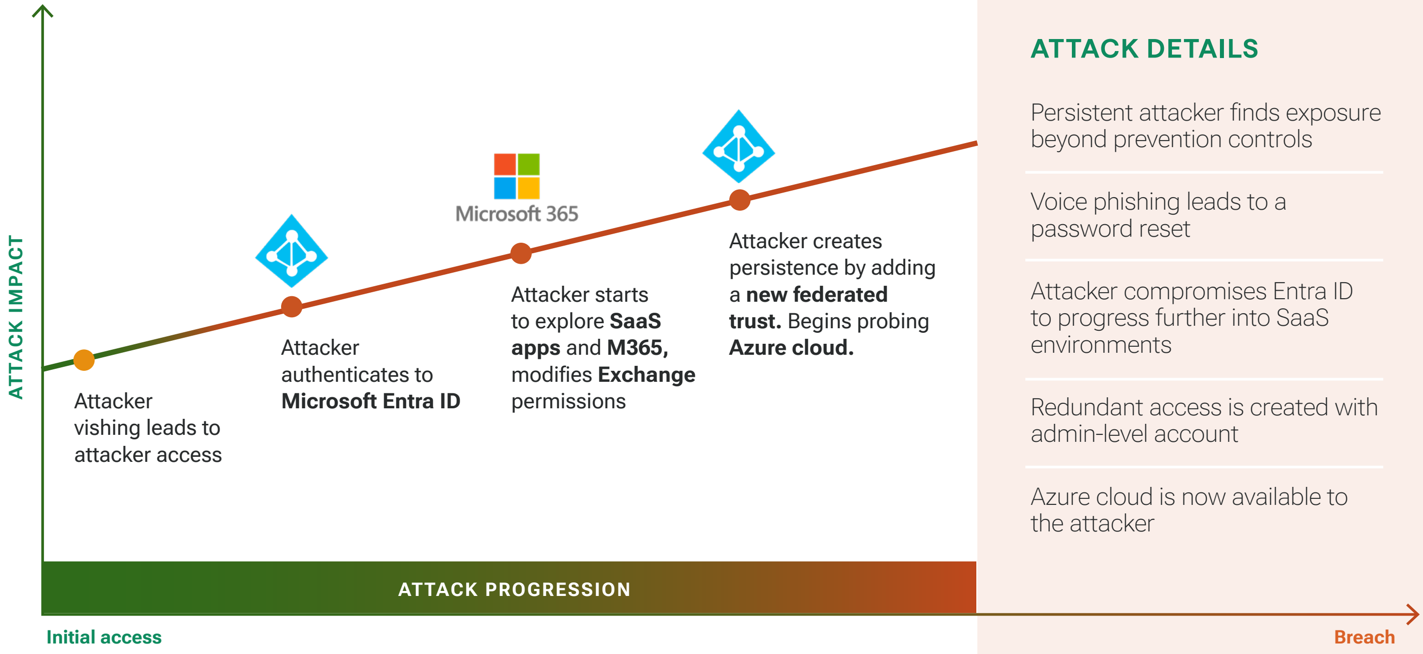
In addition, the lack of people and resources available in many of today's SOCs further compound the challenge.

SECTION 1:
Coverage

Let's take a look at a hybrid attack progression where the attackers use a compromised identity to move throughout an environment to access cloud resources. These tactics are attributable to recent attacks by Scattered Spider.

Hybrid attacker exposes path to the cloud

Scenario: IT desk resets MFA for admin account, allowing attack access to the cloud and where they move to add persistence.



Attacker vishing leads to attacker access

Attacker authenticates to **Microsoft Entra ID**

Attacker starts to explore **SaaS apps** and **M365,** modifies **Exchange** permissions

Attacker creates persistence by adding a **new federated trust.** Begins probing **Azure cloud.**

ATTACK DETAILS

Persistent attacker finds exposure beyond prevention controls

Voice phishing leads to a password reset

Attacker compromises Entra ID to progress further into SaaS environments

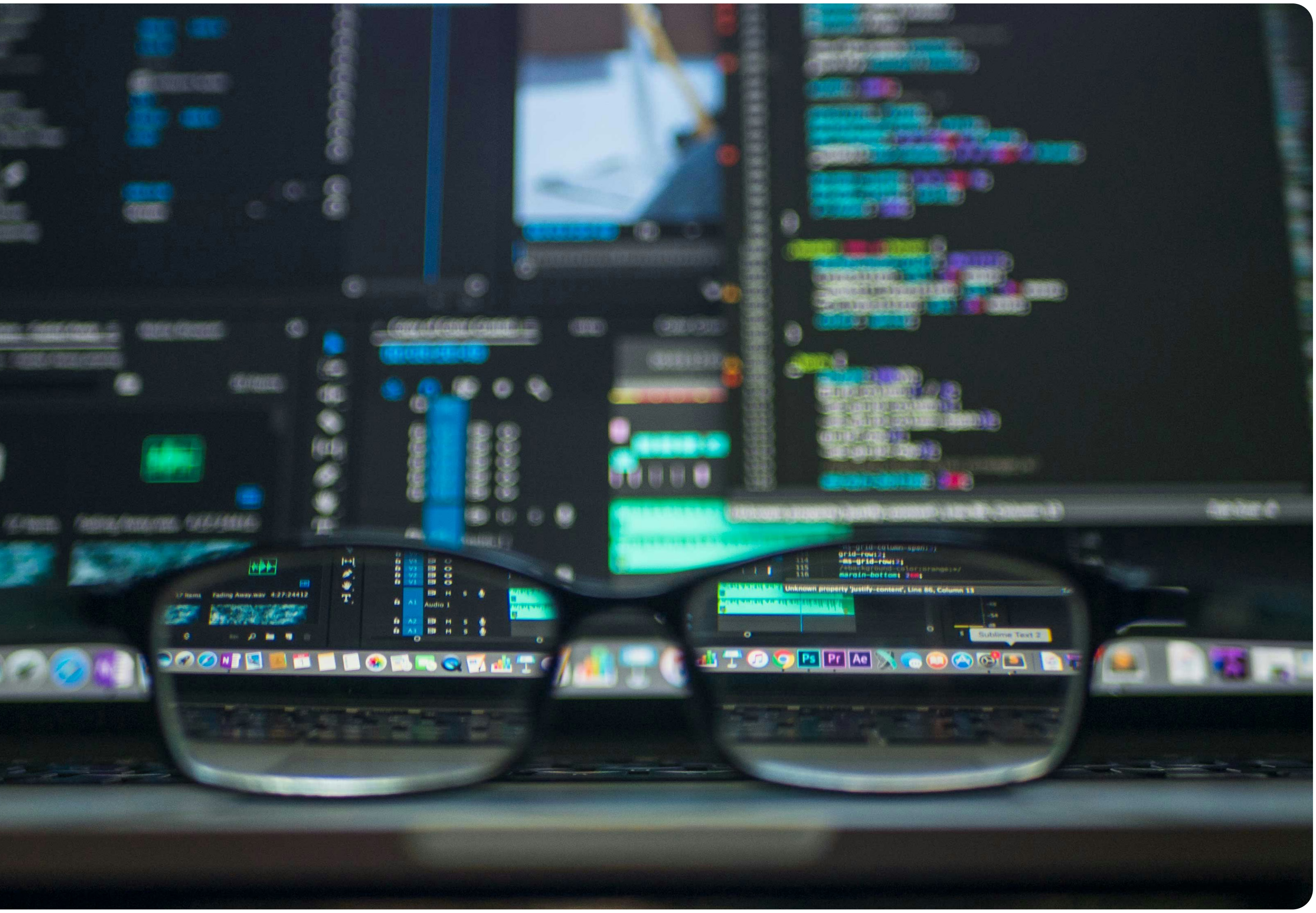
Redundant access is created with admin-level account

Azure cloud is now available to the attacker

Where is your exposure?

In this attack, the actors found exposure beyond prevention controls with the compromised identity. Attackers typically don't just use one tactic, which was the case here as they moved through SaaS apps and then added persistence to start probing Microsoft Azure. Even with prevention controls in place such as MFA or endpoint security, attackers will always work to find additional exposure. In this instance, a compromised identity provided the attacker with everything they needed to bypass any preventative security measures.

Each tactic and technique provide an opportunity for defenders to detect the activity, however, the first piece to the puzzle is having coverage to do so wherever the attacker moves — here that's across identity, SaaS and cloud surfaces. In other attacks, that can also mean data center, IoT, endpoint, email, etc.



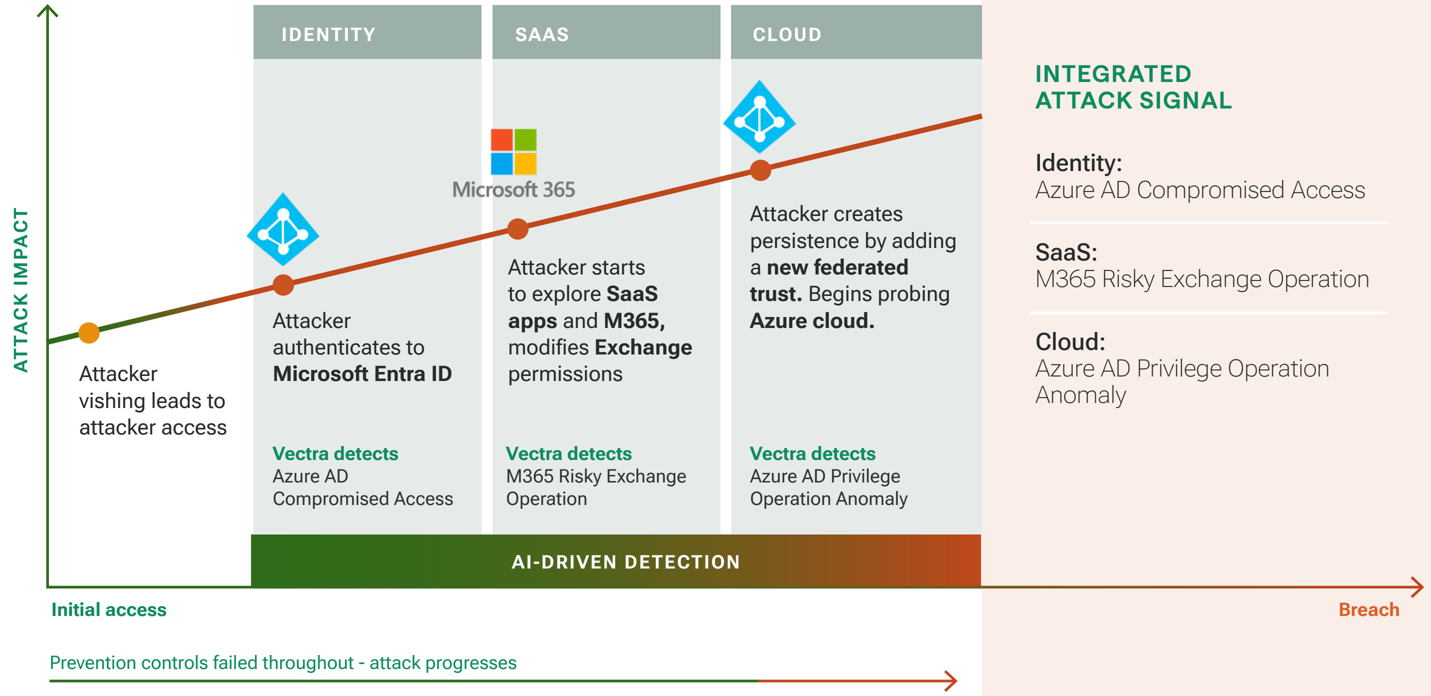
SECTION 2:

Clarity

Now that we've seen what the attackers are doing and where they're moving, how do we detect them? Here's another image of the attack where the defending organization uses AI-driven detection to detect the attacker behavior across the different hybrid surfaces that the attacker targets.

Threat activity detected across identity, SaaS and Cloud

Scenario: No part of the hybrid environment is off limits as the attacker moves across identity, SaaS and cloud surfaces. Defenders need coverage across each surface along with an attack signal that maps to each tactic and technique.


ATTACK IMPACT
IDENTITY
SAAS
CLOUD
Microsoft 365
Attacker vishing leads to attacker access
Attacker authenticates to Microsoft Entra ID
Attacker starts to explore SaaS apps and M365, modifies Exchange permissions
Attacker creates persistence by adding a new federated trust. Begins probing Azure cloud.
Vectra detects Azure AD Compromised Access
Vectra detects M365 Risky Exchange Operation
Vectra detects Azure AD Privilege Operation Anomaly
AI-DRIVEN DETECTION
Initial access
Breach
Prevention controls failed throughout - attack progresses

INTEGRATED ATTACK SIGNAL

Identity:
Azure AD Compromised Access

SaaS:
M365 Risky Exchange Operation

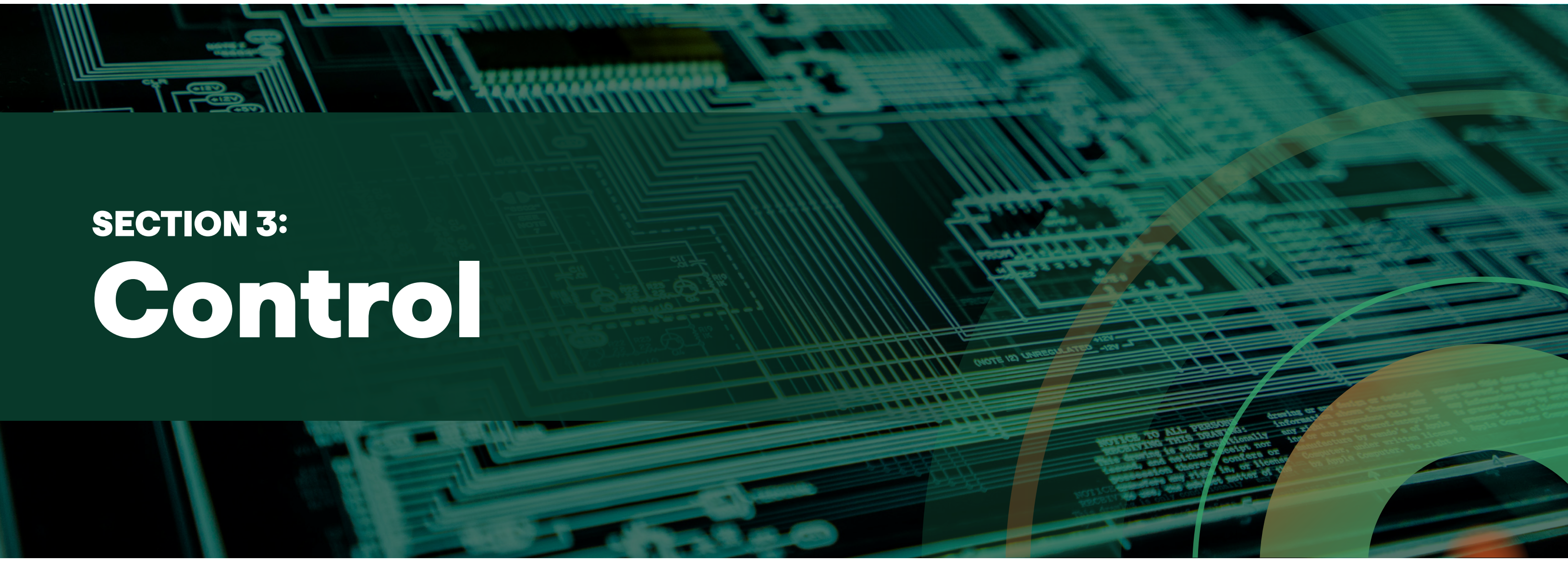
Cloud:
Azure AD Privilege Operation Anomaly

Is your attack signal integrated?

As the attacker moves from one surface to another (identity, SaaS and cloud), you can see that there is a detection mapped to each tactic. One of the common challenges defenders face is the latency that comes from correlating security alert streams from different tools, which can be highly manual and result in missed events.

The right AI can automate this process and give defenders time back to investigate and respond. While it can be a big help to have everything in one place, SOCs still receive an average of 4,484 alerts per day[1], which is why to successfully defend against a hybrid attack, there's more to it than just getting more detections as there's no possible way an analyst can evaluate that many alerts in a day.

[1] 2023 State of Threat Detection Report: The Defenders' Dilemma



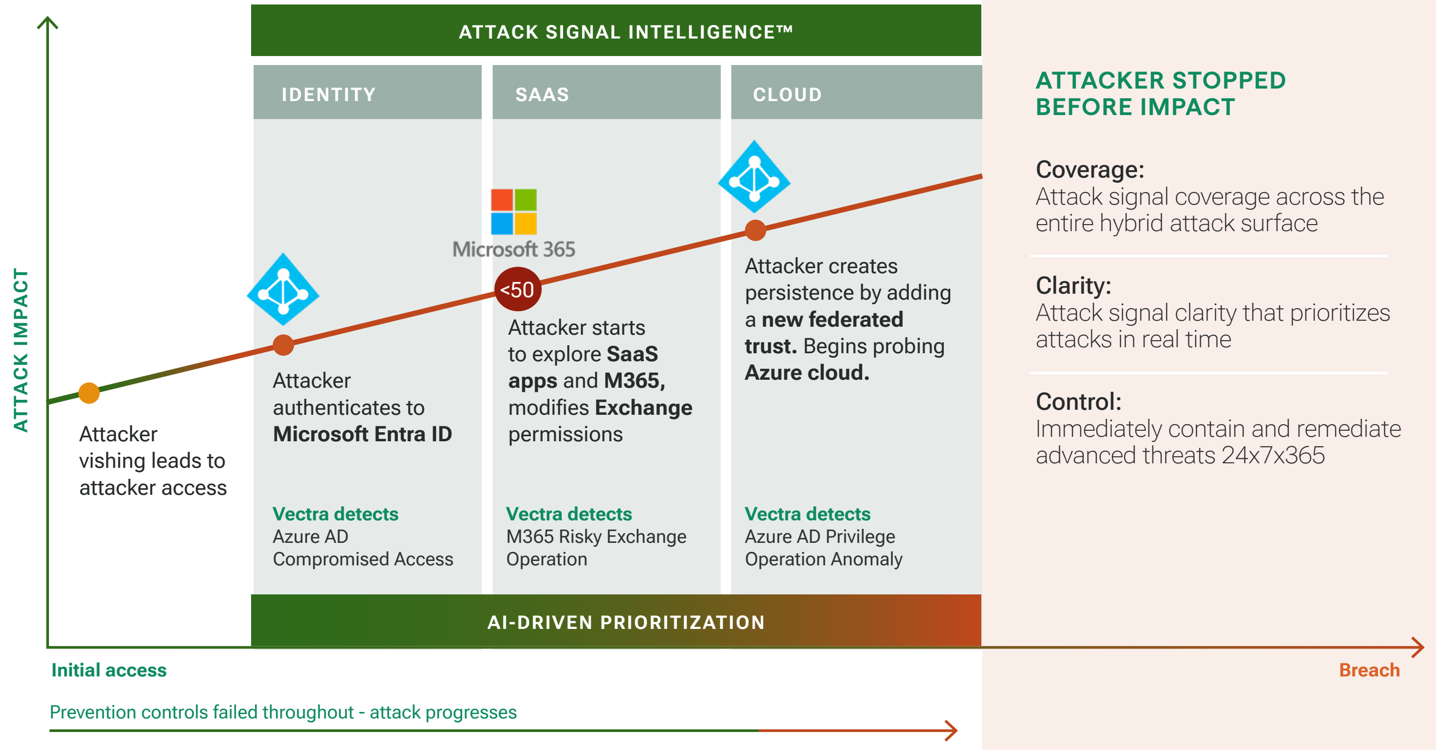
SECTION 3:

Control

Beyond just another security alert, a detection is the opportunity for a defender to stop a real attack. So how do they know when an alert is an urgent matter? Let's take another look at the attack where the detections are prioritized.

Controlling the attack means more than just "more" detections

Scenario: Technology that automatically prioritizes the detections and presents defenders with an urgency rating will give SOCs and/or managed services teams the control needed to stop the attack.



ATTACK SIGNAL INTELLIGENCE™

IDENTITY | SAAS | CLOUD

Attacker vishing leads to attacker access

Attacker authenticates to **Microsoft Entra ID**

Vectra detects
Azure AD Compromised Access

Attacker starts to explore **SaaS apps** and **M365,** modifies **Exchange** permissions

Vectra detects
M365 Risky Exchange Operation

Attacker creates persistence by adding a **new federated trust.** Begins probing **Azure cloud.**

Vectra detects
Azure AD Privilege Operation Anomaly

AI-DRIVEN PRIORITIZATION

Initial access

Breach

Prevention controls failed throughout - attack progresses

ATTACKER STOPPED BEFORE IMPACT

Coverage:
Attack signal coverage across the entire hybrid attack surface

Clarity:
Attack signal clarity that prioritizes attacks in real time

Control:
Immediately contain and remediate advanced threats 24x7x365

Knowing what matters

Not only can the right AI detect attacker activity across the hybrid attack surface, defenders can use it to prioritize what detections really matter so they can focus on urgent security events rather than wasting efforts on false positive alert noise. Using Vectra's Attack Signal Intelligence as the AI example here, the technology utilizes ML to automatically analyze detection patterns, then it scores relevant events to distinguish malicious from benign activity. In addition, defenders receive detections that are automatically correlated across all of their attack surfaces and evaluated against globally observed attack profiles to create an urgency rating, so they know which alerts need attention.

The image above shows this in action. You can see how the attack progression builds in urgency until it reaches a level that requires action (signified by the red dot on in center column). In the SOC, this information is clearly displayed so the analyst knows there's an urgent matter. Whether the analyst work is carried out by an internal team member or by Vectra MXDR, the full attack context is provided for immediate investigation with the option for automated or manual response actions to isolate and contain the attack.

Vectra MXDR customers gain 24×7×365 service and expertise with MXDR specialists who are dedicated to investigating malicious activity surfaced by the Vectra AI Platform

1. Attack Signal Intelligence
2. 24x7x365 service and expertise
3. Full end-to-end attack coverage
4. Remote response and remediation
5. Full adaptability based on your SOC's maturity
6. Managed security policy configuration

SECTION 4:

Key Takeaways

Defending against hybrid attacks starts with the right focus.

The hybrid attack example we've discussed here certainly poses challenges for defenders — compromised identities, hiding in privileges, lateral movement across domains in search of a target — this attacker activity highlights the importance of being able to prioritize post compromise attacker methods. And as you can see in the last example of the attack, it's possible with the right approach even when you're dealing with the exposure, latency and noise that makes stopping today's attackers so difficult in the first place. If you look to the right side of the image, there are three areas of focus that you can use in your strategy.

Coverage:

Having coverage for today's hybrid environments can be done by utilizing an integrated attack signal that spans all hybrid surfaces (identity, cloud, SaaS, data center, IoT, endpoint, etc.). Attackers will always be working to uncover exposure beyond where you already have prevention controls making it critical to be able to detect every surface.

Clarity:

Having clarity today into post compromise attacker methods is accomplished with an integrated AI-driven attack signal that knows what's malicious and prioritizes urgent threats in real-time. This removes the latency around event correlation so your team knows what threats are real and if they are critical so they know what to do next.

Control:

Successful investigation and response control for hybrid attacks means that defenders have the full attack context along with automated and manual response actions to empower their skills and expertise. Gaining coverage and clarity helps your team maximize its talent so they aren't wasting time on alert noise, but rather know what real threat to address and what actions to take with the controls to do it.

Building SOC confidence and competence

It’s easy to blame attackers for diminished confidence and competence in the SOC, but what if we didn’t have to contend with the added exposure, latency and noise present across hybrid environments? Would we still have 97% of analysts worried they’ll miss a relevant security event because it was buried in a flood of security alerts? Or 71% of analysts admitting the organization they work in may have been compromised and they don’t know about it yet?[1]

While attackers will always pose new challenges, they now operate in a hybrid world — just like us. So, we should ask:

1. COVERAGE
   Can we see them?
2. CLARITY
   Can we keep pace with them?
3. CONTROL
   Can we stop them?

With an AI-driven XDR platform and MXDR services SOCs gain the coverage, clarity and control needed to stop today’s hybrid attacks.

About Vectra AI

Vectra AI is the leader in hybrid attack detection, investigation and response. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single platform. Vectra AI's patented Attack Signal Intelligence empowers security teams to rapidly detect, prioritize, investigate and stop the most advanced hybrid cyber-attacks. With 35 patents in AI-driven detection and the most vendor references in MITRE D3FEND, organizations worldwide rely on the Vectra AI Platform and MXDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.