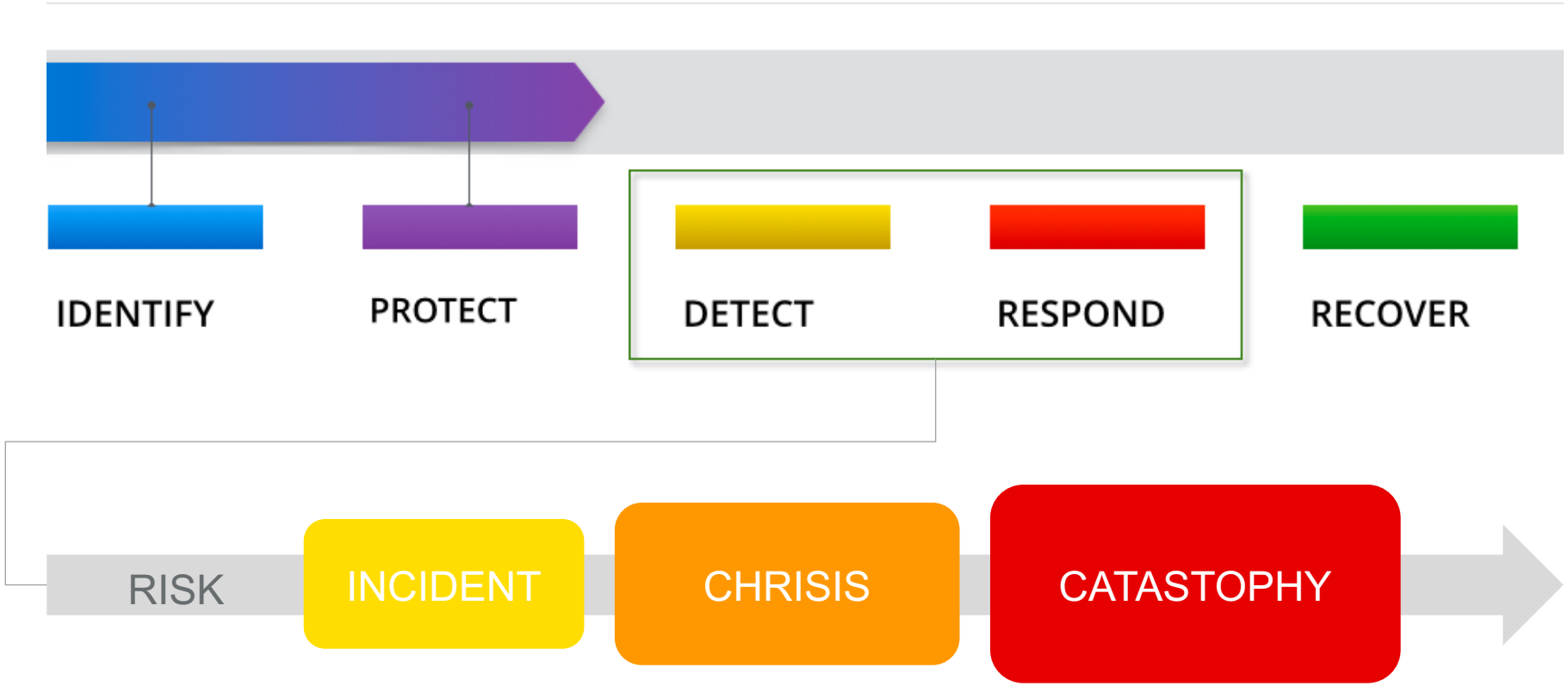
VECTRA®
SECURITY THAT THINKS.®

What is Extended Detection & Response (XDR)?

And why should we care…

When Prevention fails, efficient Threat **Detection & Response** is key.



Source: NIST Cyber Security Framework

The **challenge** from an organizations' point of view…

"

We don't know how to keep pace with **modern attacks.**

***83%** of security leaders think traditional approaches don't work for modern threats*

"

We don't know if we are being **compromised right now.**

***72%** of security leaders think they may have been breached but don't know it*

"

We don't know how to prioritize the threats **that matter most.**

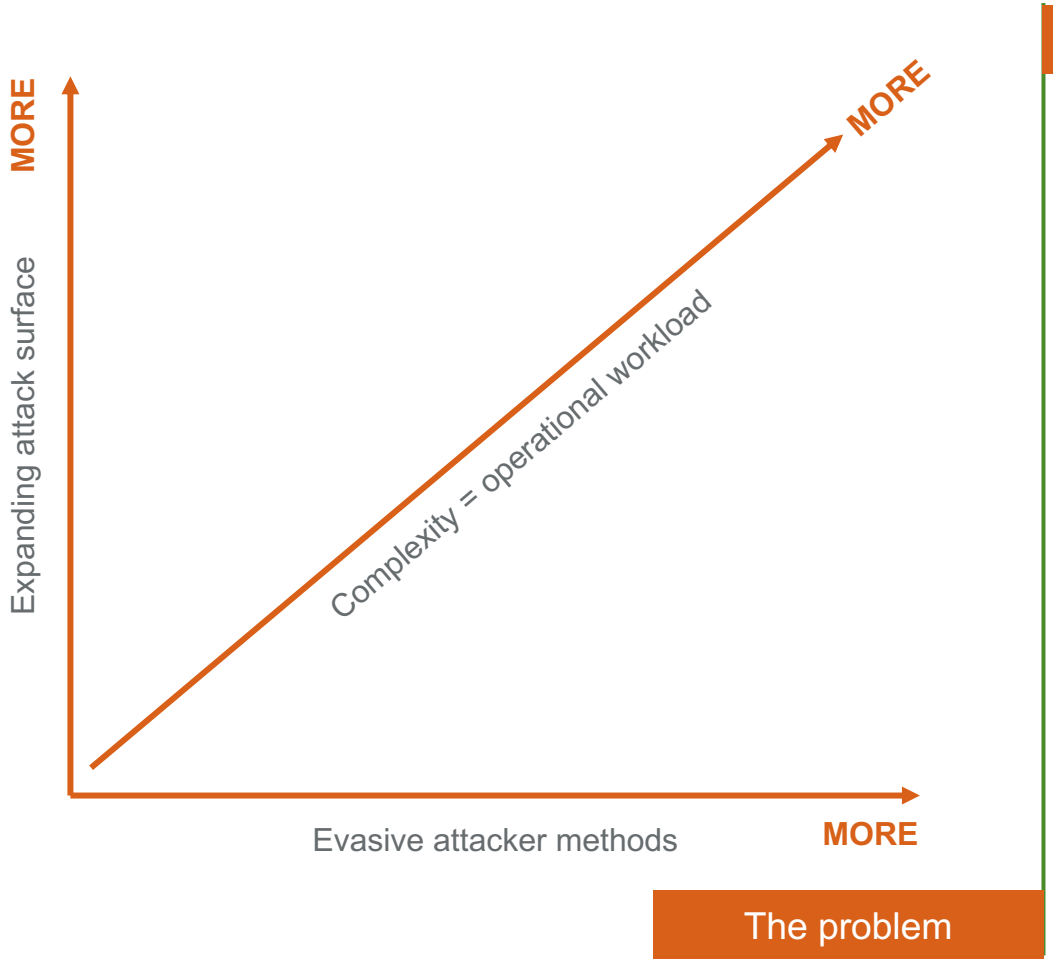
79% of security leaders say vendor tools fail to live up to their promise

The unknown

Source: Vectra Research Study | Global : Fit for Purpose or Behind the Curve? - January 2022 - Based on interviews of 1800 IT security decision makers working at organizations with more than 1,000 employees across France, Italy, Spain, Germany, Sweden, Saudi Arabia and the US, and more than 500 employees across the Netherlands and Australia & New Zealand.

The unknown is rooted in MORE

How can security take on more without more complexity, noise and burnout

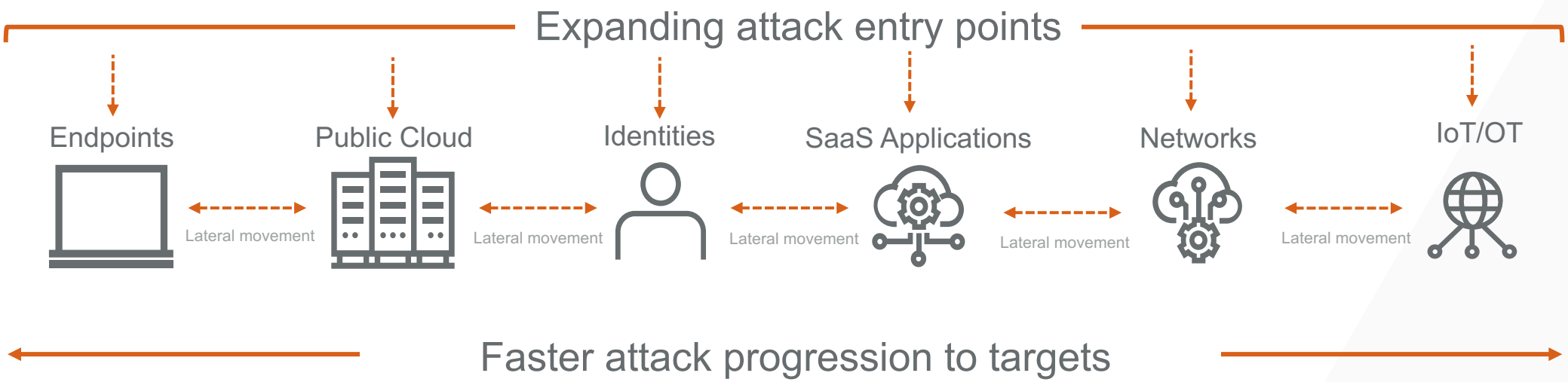


The challenges

- **More attack surface to cover**
  without adding more complexity
- **More evasive attackers to detect**
  without creating more noise
- **More skilled defenders to keep pace**
  without burning analysts out

Attackers feed on the **unknown**.

How can you detect the earliest signs of a breach?



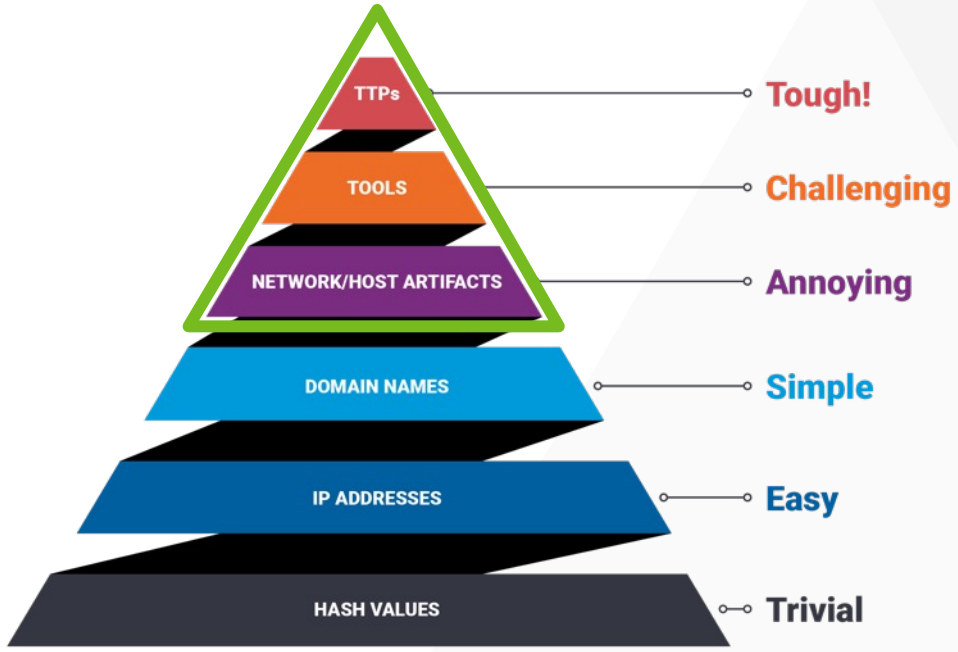
Attackers feed on the **unknown**.

How can you detect the very latest attack techniques?

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

brute ratel

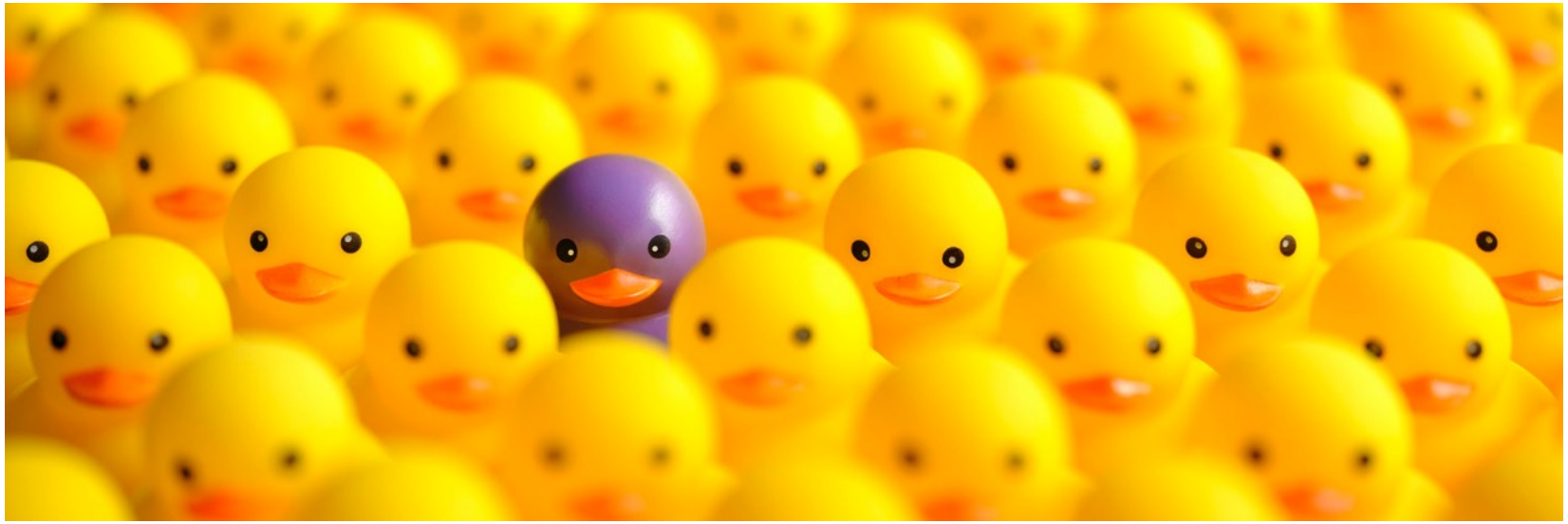
SLIVER
FRAMEWORK



The Pyramid of Pain

If only it was this easy…

Different ≠ Bad



Bad ≠ Different

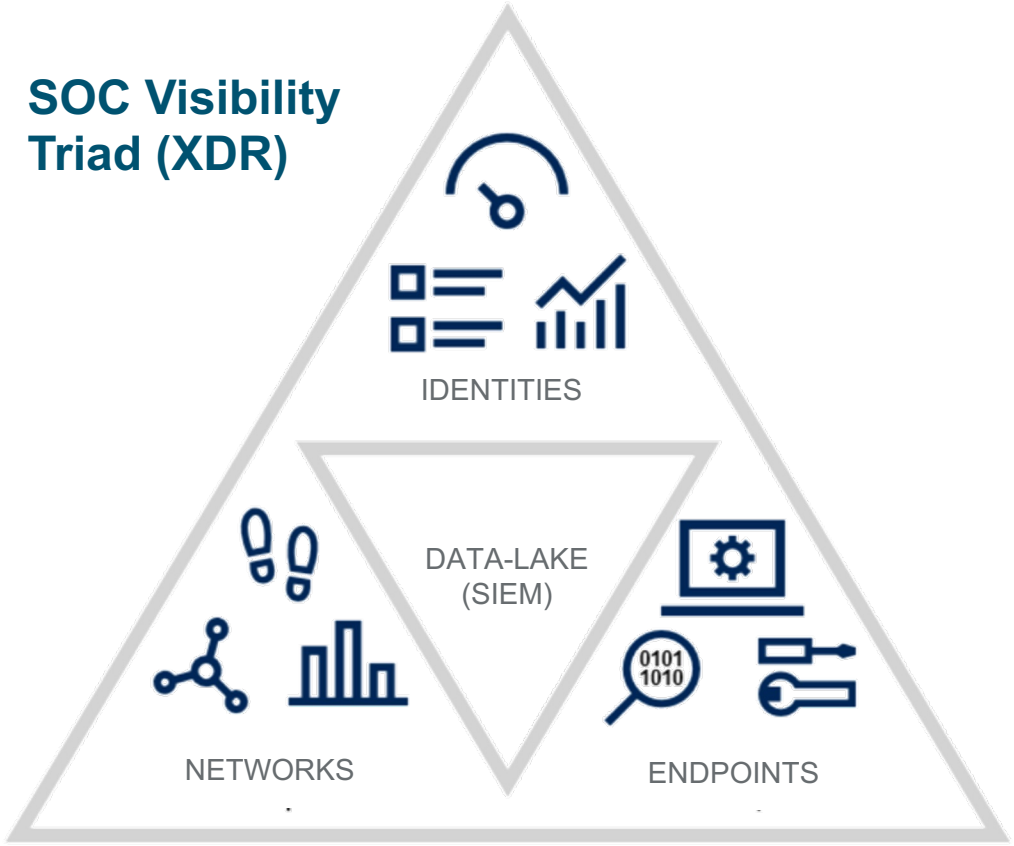
Modern **SecOps** is anchored to monitoring endpoints, networks & identities

Gartner

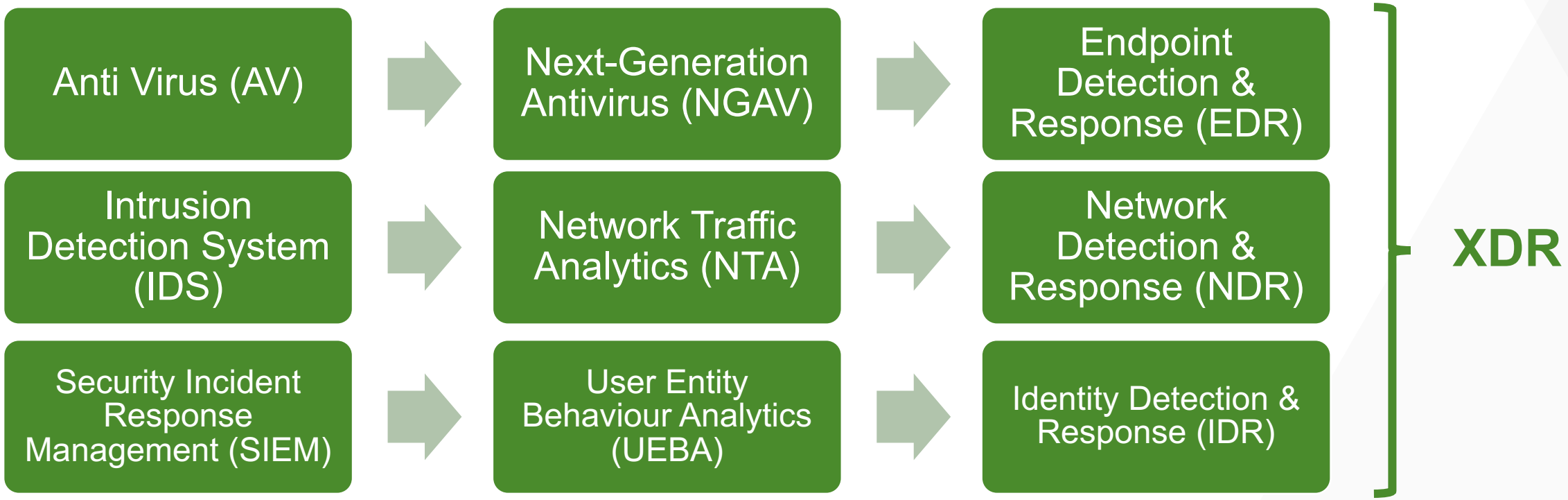
> Network-based technologies enable technical professionals to obtain quick threat visibility across an entire environment without using agents.

Source: Applying Network-Centric Approaches for Threat Detection and Response March, 2019, ID Number: G00373460

SOC Visibility Triad (XDR)



The Evolution of **Threat Detection** Tools



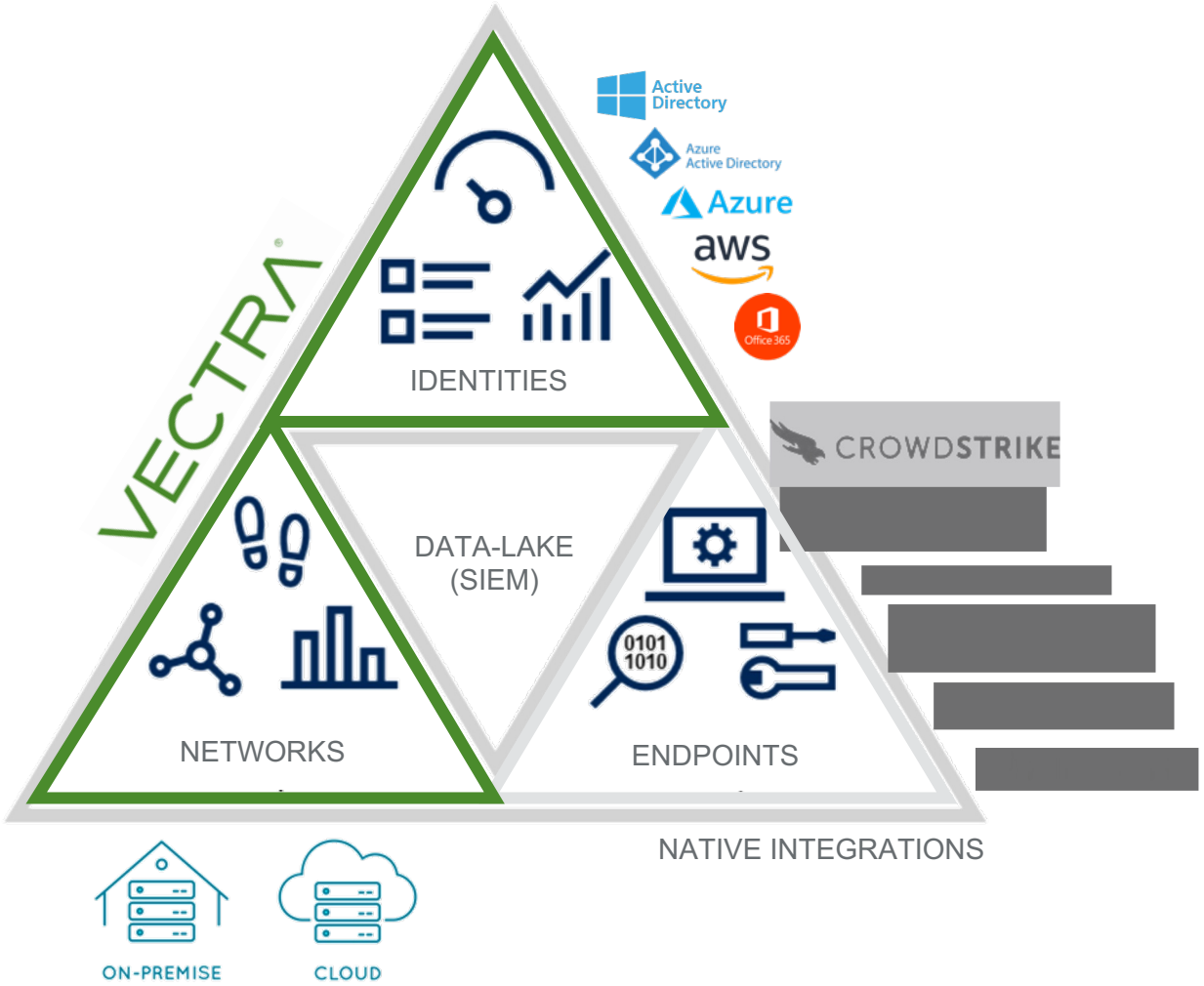
Example - **SolarWinds** - The Sunburst attacks

8 Controls to Thwart Sunburst and Other Supply Chain Attacks

By Thomas Lintemuth, Gartner | February 19, 2021

Step	Purpose	Activity to Detect	Control	
1	Download software update			Endpoint
2	12-14 days after download SUNBURST activates	New programs running	EDR/Whitelisting	Endpoint
3	DNS lookups to avsvmcloud.com	DNS lookup to new domain	Sanitized DNS	Network
4	C2 outbound HTTPS tunnel	HTTPS tunnel to new domain	NDR, SWG, FW	Network
5	Fully functional HTTPS tunnel	HTTPS non-standard activity	NDR	Network
6	Domain reconnaissance	Suspicious traffic LDAP Query / RPC	NDR, IDsegmentation	Network
7	Access other systems on network	Suspicious remote execution Privilege access anomalies	NDR, IDsegmentation Deception	Identity
8	Move to ADFS server to obtain SAML signing certificate	Suspicious remote execution Privilege access anomalies	NDR, IDsegmentation Deception	Identity
9	Login to Azure AD	Suspicious login	NDR	Identity
10	Attackers add trusted domains to Azure AD	Suspicious Azure AD activity	Azure tool	Identity
11	Update credentials with access to O365	Suspicious O365 activity - Oauth permission changes eDiscovery searches, "Power Automate" flows via HTTPs or external storage	O365 monitoring	Identity
12	Access Email	Suspicious O365 activity - sign-on, forwarding, transport rule eDiscovery	O365 monitoring	Identity

Vectra AI – **Extended Detection & Response** platform



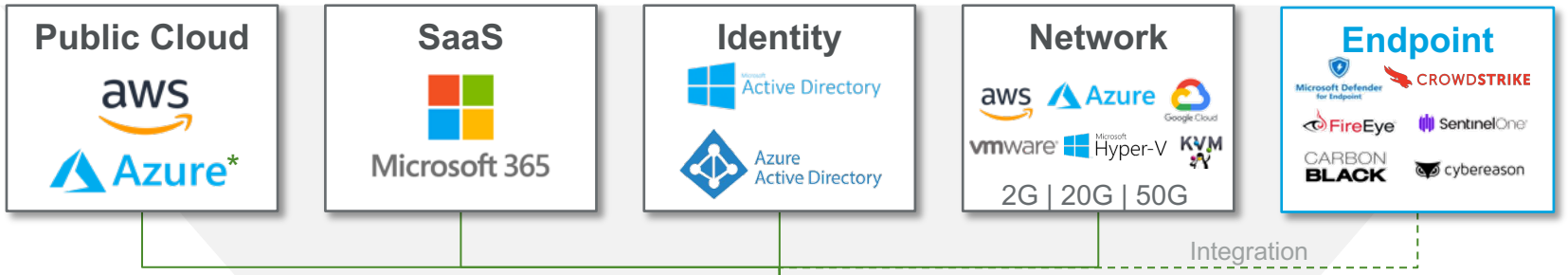
Vectra AI - Integrated **Attack Signal Intelligence™**

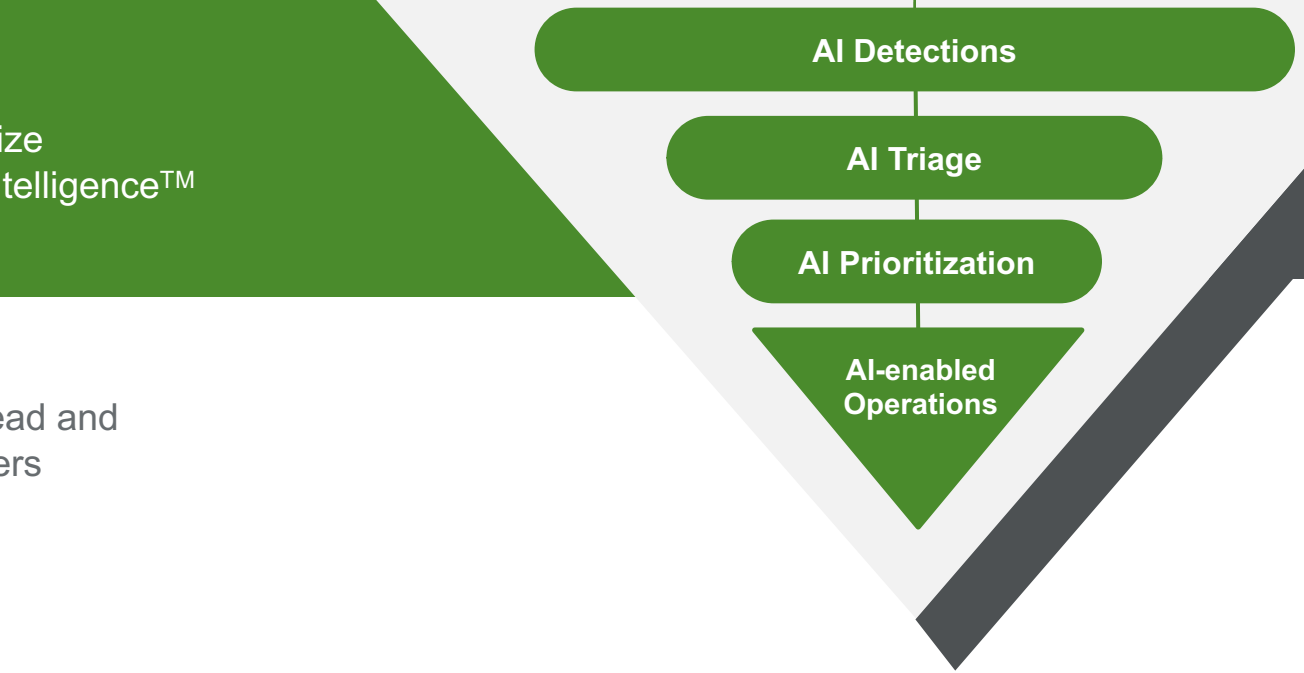
The coverage, clarity and control we defenders deserve

Coverage
Know where you are compromised right now

Clarity
Know what to prioritize with Attack Signal Intelligence™

Control
Know how to get ahead and stay ahead of attackers





24/7 Services
Managed detection, response and training provide the skills and reinforcements defenders need

Orange Cyberdefense

* Early Access Q3 2023

VECTRA SECURITY THAT THINKS®