ANM
TECH DAY

# Platforms vs Specialized Tools

# Chris Hammer

Cybersecurity Architect

- 25+ Years of IT and Security Experience
- Security, Network, Cloud, and Data Center background
- Built and managed Red / Blue Teams
- I like fast things…If it has an engine, I will drive, ride, or fly it

**Key Skills:**

- Cybersecurity Risk Management and Program Development
- Aligning security objectives to risk and outcomes
- Validation Services (Red & Blue Team Exercises)
- Enterprise Security Architecture
- Wading through the fluff

# What We Will Cover

Agenda

- Cybersecurity Platforms vs Specialized Tools
- The Debate
- What do Platforms Have to Offer?
- Where do Specialized Tools Fit?
- The End Game
- Q & A

# What?

Platforms vs Specialized Cybersecurity Tools


# It’s Still a Common Debate


- Breadth vs. Depth Trade-off
- Operational Simplicity vs. Flexibility
- Speed of Innovation
- Cost & Procurement Dynamics
- Risk Appetite & Architecture Philosophy

# Security Platforms

# What do Platforms Have to Offer?





- **Reduce risk** through integration
- **Simplify operations** and staffing
- **Predictable (maybe lower) long-term costs**
- **Improve detection and response**
- **Scale** with the business
- **Strengthen compliance and governance**
- **Increase accountability**
- Deliver **clearer executive insight**


TOP 10 REASONS
Organizations Choose
CYBERSECURITY PLATFORMS
1 Reducing Risk
2 Operational Efficiency
3 Lower TCO
4 Stronger Outcomes
5 Scalability
6 Accountability
7 Alignment
8 Better Exec Metrics
9 Faster Time to Value
10 Improved Governance
Strengthen. Simplify. Secure.

# Why Organizations Choose Platforms

Vs Tool Sprawl


**Risk Reduction Through Integrated Coverage**
**Executive takeaway:** Fewer security gaps, fewer blind spots.

- Reduce fragmentation by covering multiple threat vectors (identity, endpoint, network, cloud)
- Fewer integration failures between tools → lower likelihood of missed alerts or misconfigured controls
- Security posture becomes architectural, not point-solution dependent

**Operational Efficiency & SOC Simplification**
**Executive takeaway:** Do more with the same—or fewer—people.

- Unified consoles, shared telemetry, and correlated alerts reduce alert fatigue
- SOC analysts spend less time switching tools and reconciling data
- Automation and shared context shorten Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)

# Why Organizations Choose Platforms

Continued…


**Scalability & Future-Proofing**
**Executive takeaway:** Security that grows with the business.

- Platforms scale more easily across users, devices, locations, and clouds
- Easier adoption of new capabilities (e.g., Zero Trust, AI , post-quantum readiness)
- Reduces the risk of re-platforming every 3–5 years

**Vendor Accountability & Clear Ownership**
**Executive takeaway:** One throat to choke.

- Clear accountability for security outcomes and roadmap alignment
- Fewer finger-pointing scenarios between tool vendors
- Simplified escalation, support, and executive alignment

# Why Organizations Choose Platforms

From Chaos to Control

- "Platforms are a necessary condition to optimize."
- Add capabilities as needs evolve and time allows
- Shrinking the attack window
- Better efficacy, decision making, and business value


Prioritization in Action, white paper. IBM-PAN, 2025

"Studies show three out of four organizations are looking at security vendor consolidation today. Compared to only 29% in 2021 is a large shift in five years."

Tim Can Den Heedee, VP Global Sales, Cybersecurity Services - IBM Consulting

https://www.youtube.com/watch?v=aFdXXviDiu0

# Platforms

## A Case Study in Optimization

**Problem**: SecOps Tools where too difficult to manage, lacked threat hunting capabilities, struggled to maintain CJIS compliance with hot and cold storage. Staff was challenged to maintain security stack.

**Approach**: Workshop, gaps, tools rationalization measured effectiveness and ops supportability, cost analysis

**Solution**: Replaced SOC tools with a platform based MDR matching their primary security and NGFW vendor for optimization.

# Gaps? Where Platforms Leave off.

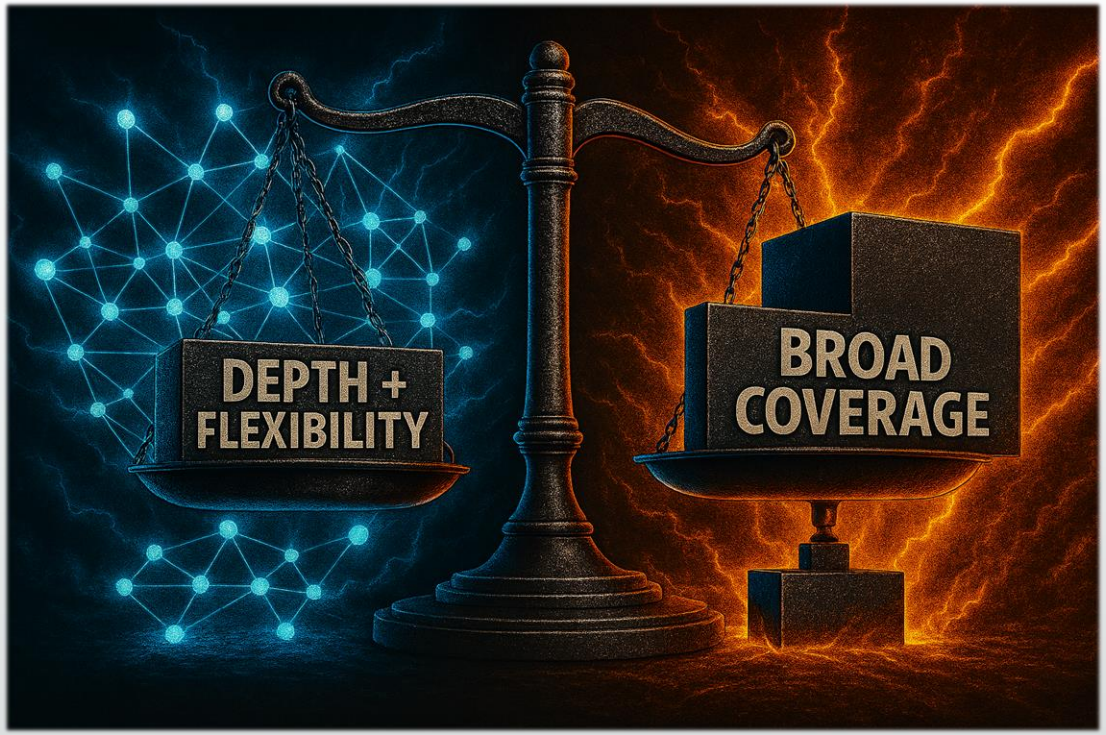
Specialized Tools Begin

# Why Specialized Tools?

# Why Specialized Tools in 2026?

Where Specialized Makes Sense in a Platform-Dominated World

- Platforms offer simplicity & breadth
- Specialized tools deliver targeted depth, agility, and innovation
- Many mature orgs choose hybrid: Platform core + strategic specialized extensions



# Breadth vs. Depth + Flexibility

- **Depth**: Specialized often beats "good enough" (e.g., top Email Security, IOT / OT, deception / anomaly tech, VA, or data classification tools typically outperform platform modules)

- **Flexibility**: Independent upgrades → new capabilities quickly

- Avoids platform stagnation or forced feature creep

# Faster Innovation + Smarter Cost


- **Innovation Speed**: Specialized solutions respond and adapt to threats quickly

- **Cost Efficiency**: Pay for excellence only — no subsidizing bundled capabilities you might not need

- **ROI** can be larger in high-impact areas (e.g., BEC prevention, data classification, IOT/OT, etc.. )

# Risk Appetite & True Mesh Architecture

Supports composable, vendor-agnostic mesh (Gartner Cybersecurity Mesh Architecture --CSMA vision)

Reduces single point of failure — if one vendor has a major outage, others compensate

Fits high-risk orgs (finance, critical infrastructure, healthcare) that prioritize defense-in-depth

# Critical Decision-Maker Considerations (Reality Check)

Another Tool Doesn't Always Solve the Problem

- **Integration Maturity & Debt** — Can your Team/XDR/SIEM/SOAR handle multi-vendor orchestration?
- **Current Tool Sprawl** — Already fragmented? Adding more tools can increase risk without strong governance.
- **Acquisition targets** — What happens if your favorite solution gets acquired or begins to expand their solution set?
- **Vendor Ecosystem Readiness** — Choose API-first, integration-friendly solutions.
- **Incident Impact Tolerance** — If a gap in one area could be catastrophic, depth > simplicity.

**Complexity vs. RISK**

# Expanding and Filling Gaps

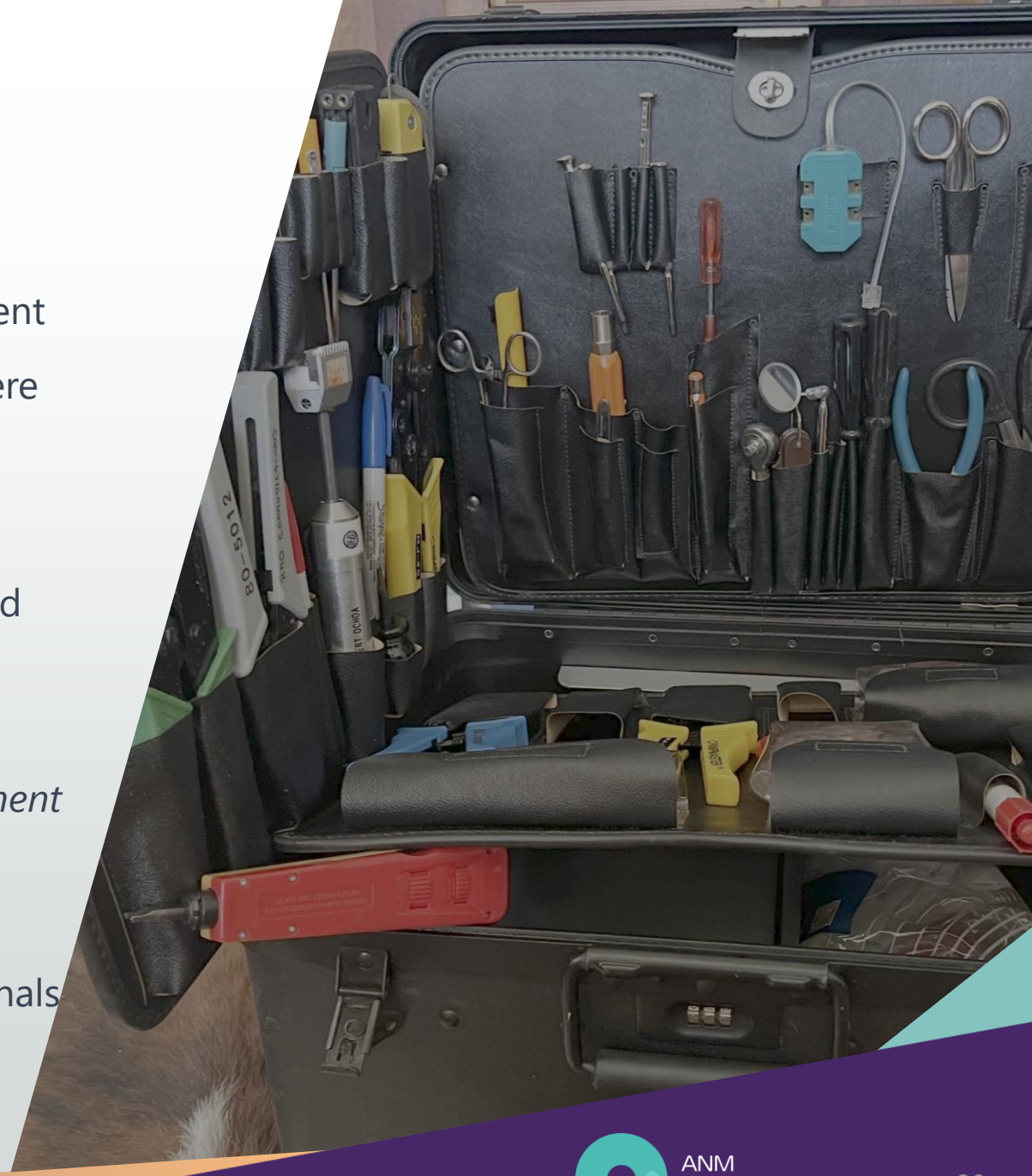
A Case Study in Specialty Tools

**Problem**: platform provided strong foundational coverage, the client continued to experience risk in human-centric attack vectors—specifically email-based threats and insider risk scenarios—that were not adequately mitigated by platform-native capabilities alone.

- Persistent phishing and BEC
- Limited detection depth for insider threats
- Operational strain on the security team, which lacked specialized workflows for investigating human-driven threats

**Approach**: Stakeholder cybersecurity workshop, use-case-driven security capability assessment. *Tuned / optimized existing environment before recommending additional tools.*

**Solution**: Stack expansion with supportable workflows, UBA, BEC protections, Context-aware risk scoring tied to identity and HR signals



# Wrapping it Up!

Who Wins?

# Typical Client Scenarios

A Common Thread


- Organizations with **mature security teams**, and **larger budgets** tend to lean on **hybrid** approaches

- Organizations with **less mature** and/or **smaller security budgets** tend to find more value in the **platform** approach to security

- Organizations may blend the platform and best of specialized tools approach to achieve the outcome they're looking to complete

# Choose Based on Maturity & Risk

What are your Threats & Risks?

**Platforms → Operational simplicity, unified visibility, lower overhead**

**Specialized → Depth, innovation, flexibility, true mesh alignment**

**2026 Reality: Hybrid model dominates mature orgs**

**Evaluate: Risk profile + SecOps capability + integration readiness**

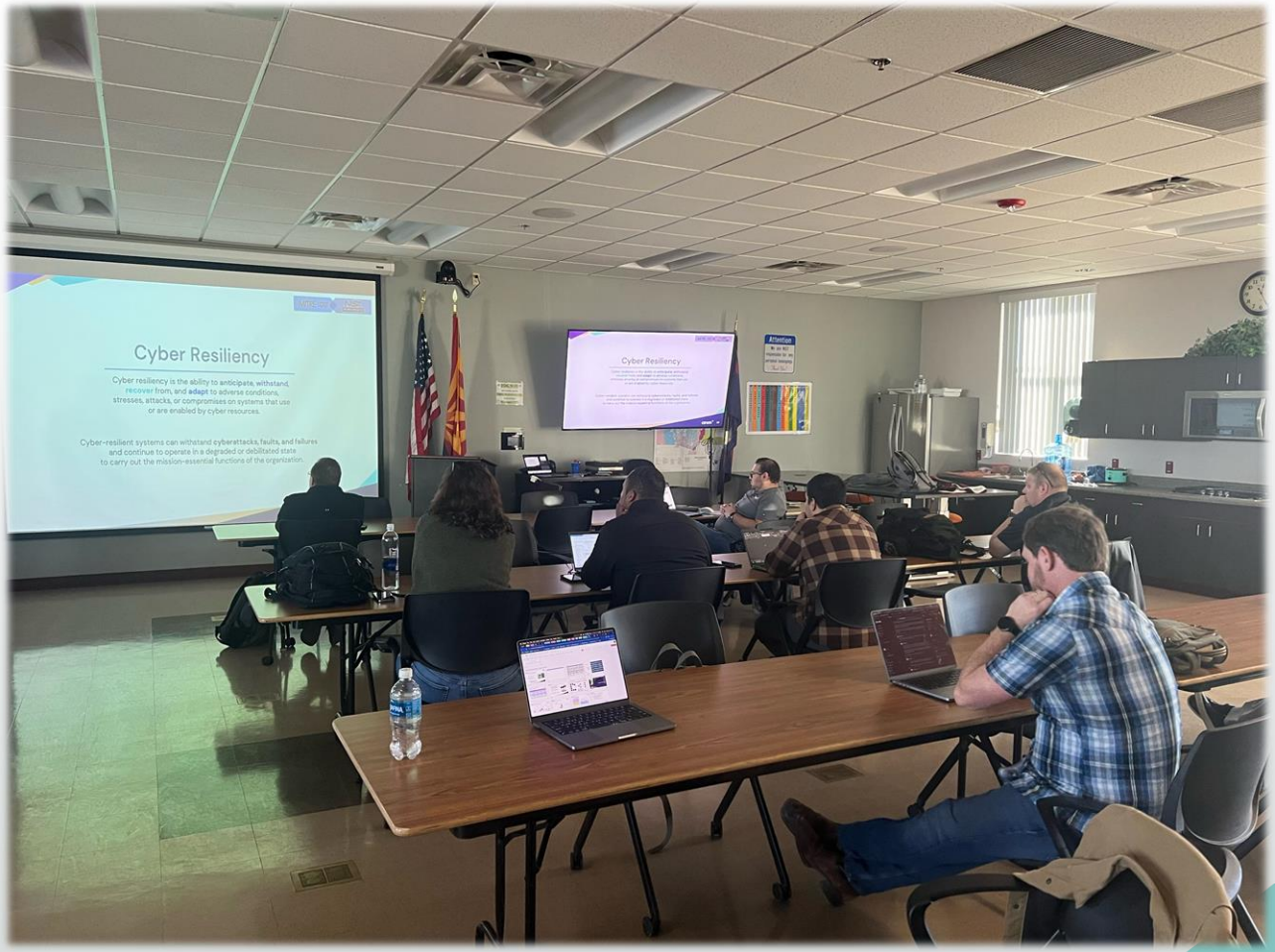
**Risk & Governance**

# How ANM Can Help?

- **Workshops**: Understand your environment with key stakeholders

- **Tools Rationalization**: Inventory, heat map, analysis

- **Cost Analysis**: Help analyze Opex vs Capex, ROI and TCO of current and potential changes



Thank you!

# Questions?