

THE UNSEEN WORKFORCE

TRUST NOTHING. **VERIFY EVERYTHING.**

THREATS

DETECTED

START →



CONTENTS

Welcome from Ignition.....	1
Vendor contribution	2
The threat landscape.....	3
The new AI attack surface	4
AI for the defenders	5
Identity as the AI control plane	6
Project Quiltworks	7
The market opportunity.....	9
Starting the conversation toolkit	13
Resources	14
Credentials	15



Welcome to your guide into the UNSEEN WORKFORCE



"I'm excited to bring you this toolkit at a time when the AI threat landscape is evolving at an unprecedented pace."

I'm excited to bring you this toolkit at a time when the AI threat landscape is evolving at an unprecedented pace.

This year, I've watched identity security shift from an IT security stack conversation to become a Board table priority. Why? Because as organisations roll out AI agents to operate across their environments, using systems, processing data, and making decisions, the access, permission and privilege of these machine identities are largely ungoverned. They don't carry a badge. They don't respond to MFA. Nobody offboards them when they're no longer needed. We're calling this the unseen workforce, a population of identities operating in your customers' names, whose access is often not fully accounted for. In this environment, it's unclear who is responsible when these agents cause a breach.

The adversaries already know this. They're not breaking in anymore. They're logging in, using stolen credentials, valid sessions, and the same AI tools businesses are adopting. This is why the significance of this conversation has been elevated. As the power of these tools grows, it's becoming ever more urgent.

We've built this document to ensure you have everything you need regarding the current AI threat landscape at your fingertips. The shape of the new attack surface, and the role

identity governance plays in defending against it. Use it as a tool to prepare for new business conversations and to approach existing customers once more. We've collected the current market data, real-time context, and proof points that can act as conversation starters. This helps move things beyond product features, creating the broader case for why this matters now. Why any legacy security stack must be revisited. And why this is now a leadership governance conversation.

Here at Ignition, our curated portfolio only carries what works, so you can be confident that every vendor in our collective solves a piece of the AI identity challenge. We've created and collated this content and data to get your customers' attention. There is plenty more to come in future editions, as well as via our website and LinkedIn channels.

If you want to talk through how to get the most from it, for your team or for the partners you're working with, get in touch with your Ignition contact.

I look forward to seeing you soon.

Sean Remnant

Co-Founder & CSO, Ignition Technology

Thank you to our Vendors

Abnormal

 BeyondTrust

 CROWDSTRIKE

digicert®

EXTRAHOP®

 illumio

 SailPoint®

 SENDMARC

 Synack®



THE SCALE OF THE CHALLENGE*



82%

of detections in 2025 were malware-free

27 SEC

is the fastest recorded eCrime breakout

70%

reduction in eCrime breakout over the last five years

89%

increase in AI-enabled adversary activity

35%

of cloud incidents involve valid account abuse

61%

of BEC is supply chain partner compromise

23%

of large-enterprise BEC incidents involve lateral attacks

\$4.91M

is the average cost of a supply-chain/vendor compromise

44%

of organisations have implemented governance policies for AI agents

Huge benefits are emerging from the development of AI. Industries from healthcare to climate to biology are revolutionising, while every industry is feeling the impact of generative and agentic AI.

This represents huge opportunities for many organisations, yet the unprecedented speed of change signals a significant security risk too. Those scaling agentic AI must look again at their identity security stack.

As organisations compete to realise the potential of AI, identity is moving from a layer of the security stack to become the critical component of cyber risk management.

The Ignition curated portfolio offers solutions to every aspect of the AI identity challenge, enabling customers to scale AI without security risk while ensuring their people and their customers, stay protected.

Sources*

CrowdStrike 2026 Threat Report,
Abnormal 2026 Attack Landscape Report
SailPoint, AI agents: The new attack surface

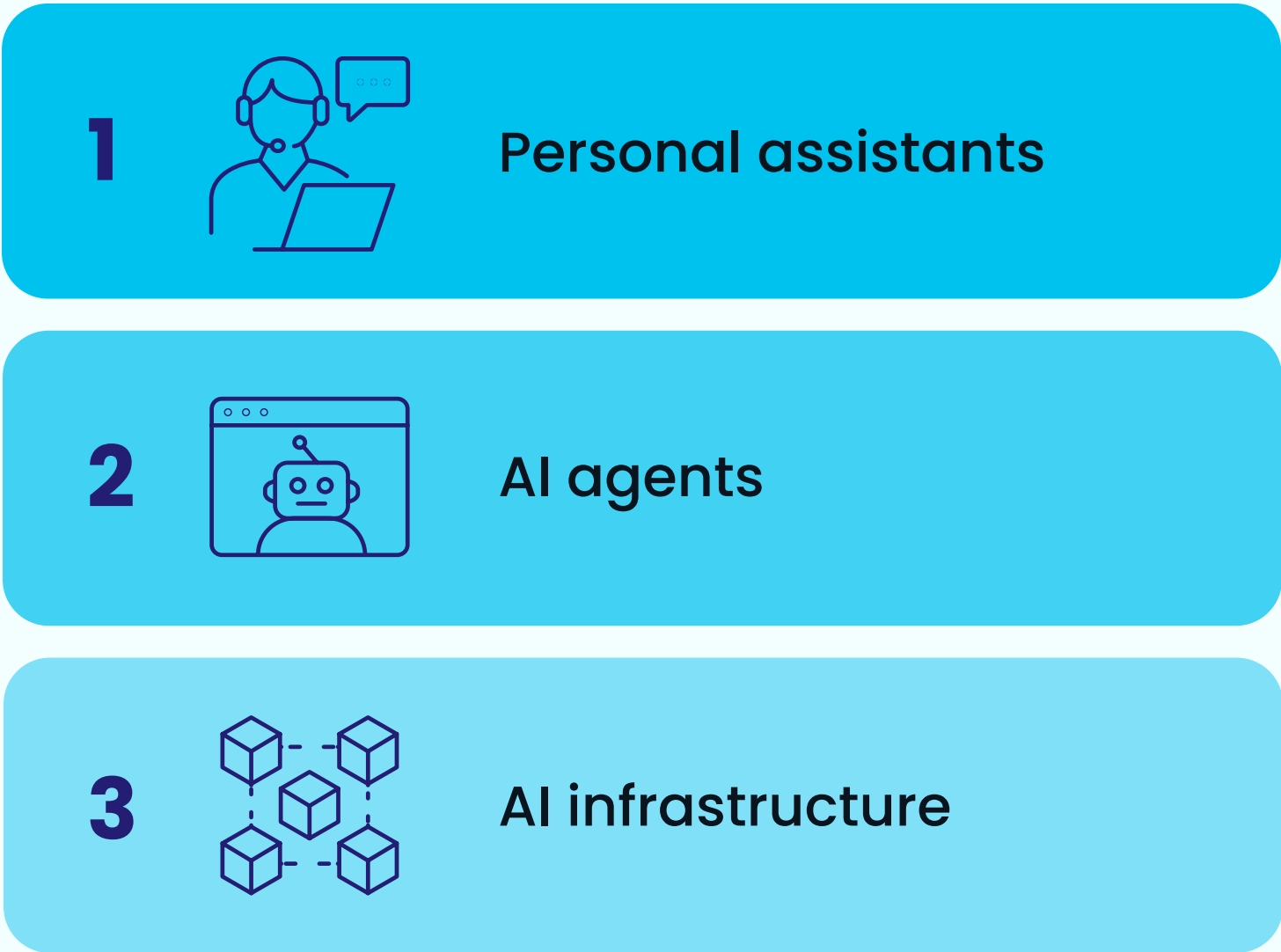


GLOBAL AI ADOPTION IS SCALING FASTER THAN THE INTERNET DID

GLOBAL AI ADOPTION IN FIGURES

- * from 700m to 900m active users are reported for OpenAI ChatGPT
- * 89% of organisations now use AI
- * 70-85% of AI initiatives reported to be failing
- * 88% of organisations reported a confirmed or suspected AI-agent security incident
- * 55% of AI users now pay for at least one AI product in 2026
- * 18.8% of the world's working-age population use generative AI

THREE LAYERS OF AI IDENTITY THREAT



This new level of threat opens the door to partner conversations with not just new but also existing customers. Every organisation with ambitions to scale agentic and autonomous AI must now reconsider their AI identity security stack in line with these ambitions. A legacy stack from 2020 is no longer sufficient.

Sources:
1. TechCrunch. 2. McKinsey State of AI 2026. 3. Gartner. 4. Gravitee The State of AI Agent Security, 2026. 5. Menlo Ventures The State of Consumer AI, 2026. 6. Microsoft AI Economy Institute, Global AI Diffusion Report 2026.

Let's get the conversation started

When was the last time you asked your customers:

- ? Do you have an inventory of all AI applications and tools in use?
- ? How do you control what a user can do with personal assistants like Claude, ChatGPT and Copilot?
- ? Do you have any controls in place to protect against prompt injection?
- ? Have you thought about how you control access to AI infrastructure?
- ? How do you treat agent and human traffic and access differently?
- ? How are you governing agents' access?

Anyone who can't answer these questions confidently needs to reassess at their AI identity stack.

DEFENSIVE DOMAINS WHERE IGNITION'S PORTFOLIO OPERATES:

When attackers and defenders have access to the same models, the advantage goes to whoever applies them fastest and most intelligently.

Legacy tools are not enough. Customers need education on both the threat and the tools and technology available to help defend against the modern AI threat.

The Ignition portfolio offers the capability to scale AI with the confidence that the right governance is in place.

Together, we can take back control from the bad actors, ensuring customers have an intuitive security stack that keeps them one step ahead of any cyber risk.



Let's get the conversation started

Have you asked your customers:

- ? How many different security vendors do you have in your environment?
- ? Are you looking to consolidate your tech stack?
- ? Have you seen an increase in phishing emails?
- ? Can you trust that all employees are not a threat?
- ? Are you looking at automation to help reduce risk?
- ? How do you handle cross domain attacks?



Project Glasswing, Anthropic’s initiative to secure critical software using Claude Mythos Preview, has already identified more than 10,000 high and critical severity vulnerabilities. The evidence is clear: AI is accelerating vulnerability discovery faster than organisations can remediate it. The challenge is no longer finding security flaws, it’s fixing them quickly enough.

This is a problem keeping many CEOs awake at night.

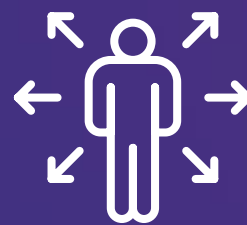
And that’s why we’re recommending identity as the AI control plane.

IDENTITY HELPS GOVERN THREE KEY AREAS OF BUSINESS OPERATIONS



Access

Who and what can connect, and when?



Privilege

What actions are permitted, at what level, for how long?



Traceability

The audit trail of who did what, when and why?

THIS OFFERS BOARD CONFIDENCE



Control

Governance on what AI can and can’t do in your environment



Accountability

Evidence to demonstrate accountability



Resilience

The ability to detect, isolate, and recover when things go wrong

Let’s get the conversation started

Can your customers confidently answer these questions?

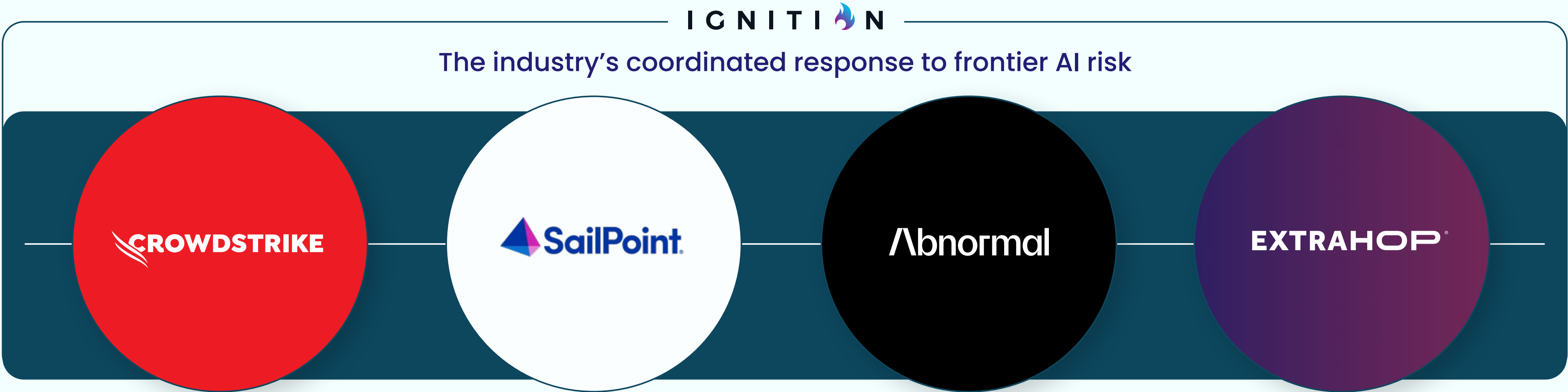
- ? Are you confident you haven’t got an insider threat?
- ? Do you have visibility of non-human identities?
- ? How are you managing non-human identities?
- ? Can you differentiate between agents and humans?
- ? How many identities do you have in your environment?
- ? How do your agents authenticate?

PROJECT QUILTWORKS

Frontier AI is creating new vulnerabilities faster than organisations can identify, prioritise and remediate them. Project QuiltWorks brings together leading security providers to help customers close that gap.

[Project QuiltWorks](#) brings together Ignition Technology, CrowdStrike and members of our wider vendor ecosystem, including Abnormal, ExtraHop and SailPoint, to help organisations address the growing risks created by frontier AI.

As AI accelerates the speed at which vulnerabilities can be discovered and exploited, Project QuiltWorks combines expertise across threat intelligence, identity security and visibility to help partners and customers identify, prioritise and reduce cyber risk before it becomes a breach.



Helping organisations move from AI risk exposure to AI readiness and resilience





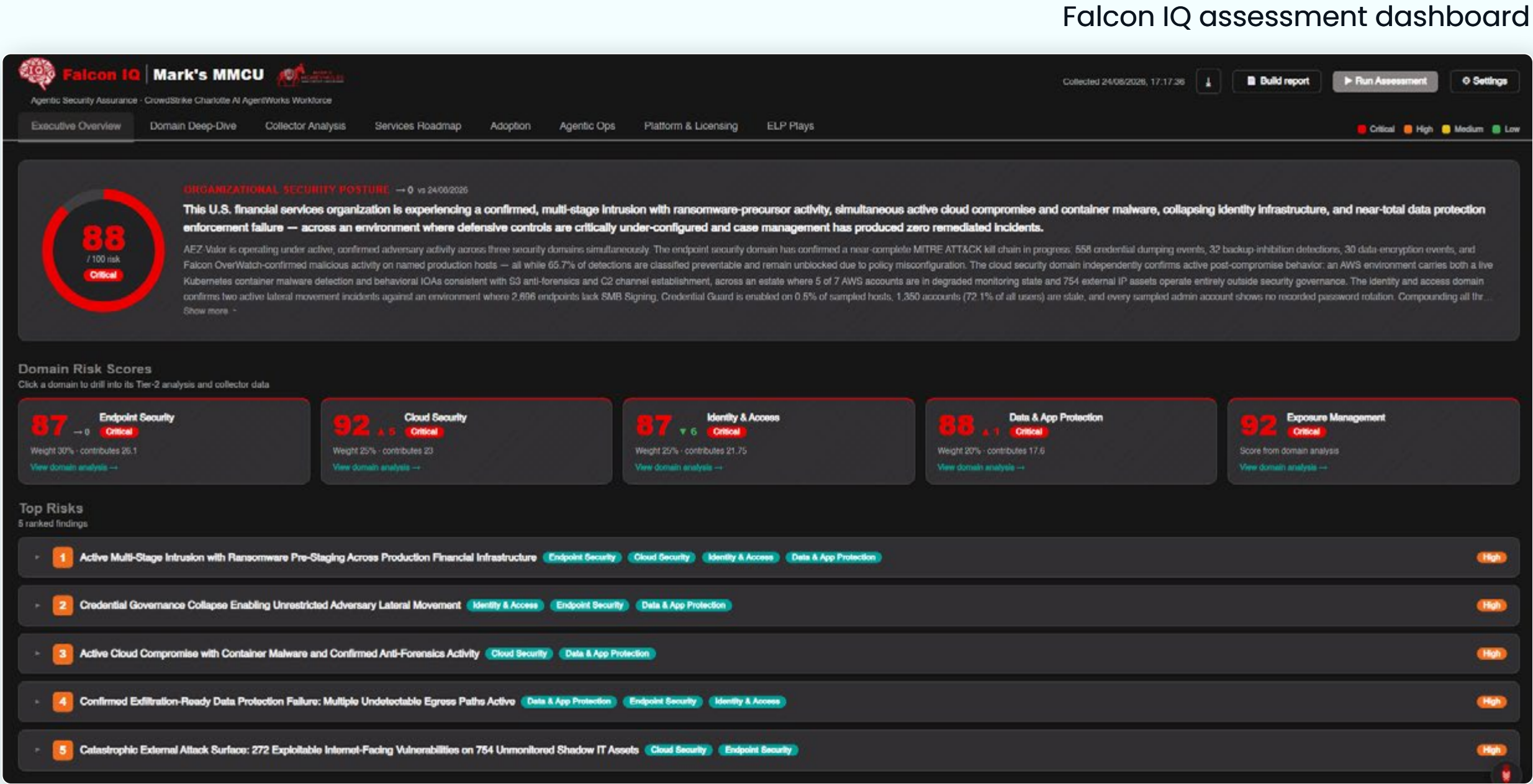
PROJECT QUILTWORKS

Falcon IQ Assessment

Operationalising Project QuiltWorks at machine speed.

Falcon IQ is the assessment capability underpinning [Project QuiltWorks](#), helping organisations identify AI-driven vulnerabilities and translate findings into prioritised remediation actions.

By transforming security telemetry into clear, prioritised insights, Falcon IQ enables organisations to understand risk, assess business impact and accelerate remediation through a single AI-powered assessment.



What Customers Receive

- 1 Risk overview**
A clear picture of overall security posture
- 2 Priority findings**
Priority issues ranked by risk and impact
- 3 Executive insights**
Board-ready outputs for senior stakeholders
- 4 Recommended actions**
Clear guidance on remediation priorities



Nearly 45 million vulnerabilities identified within hours, helping organisations uncover risks that had remained hidden for years.

From weeks of analysis to immediate insight

Traditionally, assessing security posture requires multiple tools, spreadsheets and stakeholder workshops.

Falcon IQ automates that process, delivering a comprehensive view of organisational risk through a single assessment.

The assessment automatically identifies priority risks, highlights opportunities for remediation and provides executive-ready reporting, reducing the manual effort traditionally associated with security reviews.

Traditional Assessment	Falcon IQ
Multiple teams	▶ Single streamlined assessment
Manual analysis	▶ Automated identification of risk
Weeks of effort	▶ Results delivered rapidly
Complex reporting	▶ Executive-ready insights
Reactive prioritisation	▶ Recommended next actions

THE IGNITION CURATED PORTFOLIO PROPOSITION

The Ignition curated portfolio provides complementary solutions that work together to prevent identity deception at each stage of any attack chain.

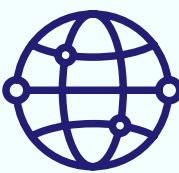
This means our partners can build end-to-end solutions, and end customers have protection before, during and after a compromise.

Attackers don't think in products. They think in attack paths. Your security strategy should too.

Here's how it works...

Together, CrowdStrike, Abnormal and Sendmarc create a layered defence that protects organisations from the moment an attacker impersonates your brand through to the detection and response of any attempted compromise.

[Find out more about this solution stack here.](#)



Protecting only the endpoint isn't enough



Protecting only email isn't enough



Protecting only your domain isn't enough



Establishes trusted email identity and prevents domain impersonation.

Stage:
Before an email arrives

Challenge:
Brand impersonation, spoofing and phishing

Solution:
Sendmarc



Uses behavioural AI to stop sophisticated email attacks that evade traditional secure email gateways.

Stage:
When an email is delivered

Challenge:
AI-powered phishing, BEC, account takeover, malicious payloads

Solution:
Abnormal



Detects, investigates and responds rapidly if an attack reaches the endpoint, with insight into how AI is being used across the environment with Falcon Guardian.

Stage:
If a user is compromised

Challenge:
Endpoint detection, containment and response

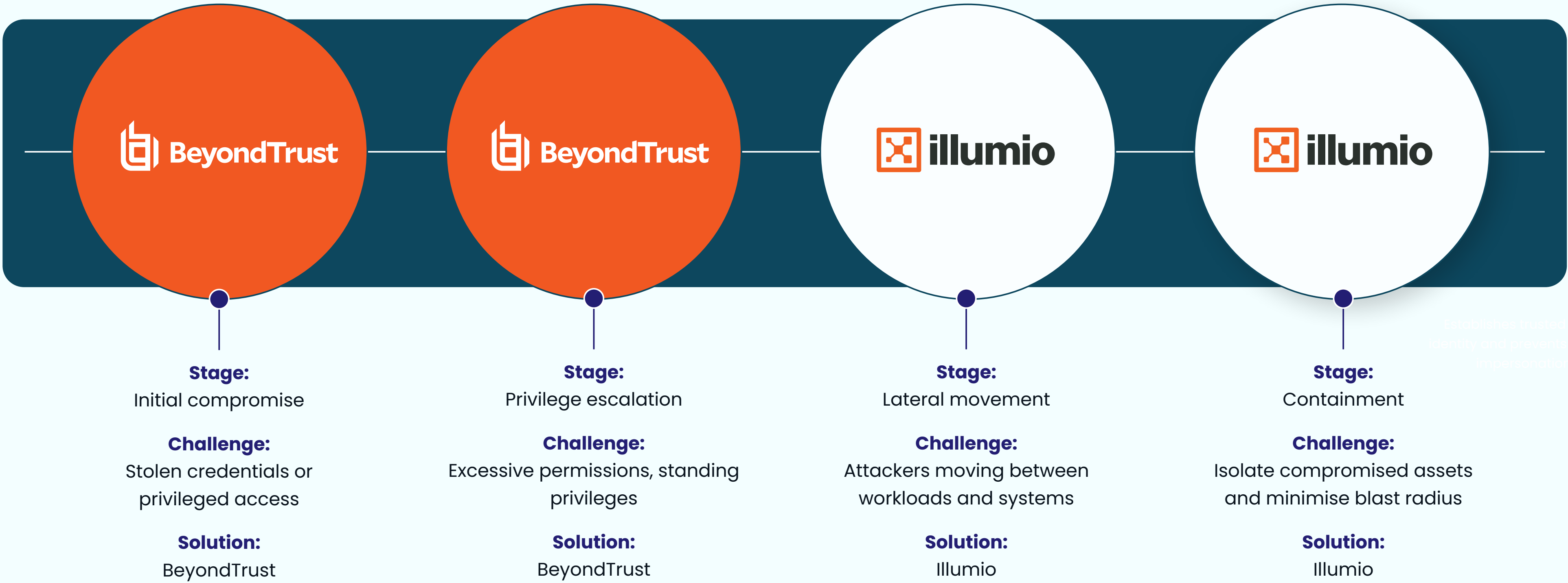
Solution:
CrowdStrike

Email to endpoint

THE IGNITION CURATED PORTFOLIO PROPOSITION

Modern attackers don't break in, they log in. Once inside, they look for privilege and move laterally until they reach critical systems.

Reduce cyber risk by securing privileged identities and containing threats before they spread across your environment. Together, BeyondTrust and Illumio assume attackers will eventually gain access, but ensure they can't escalate privileges or move laterally through your network.



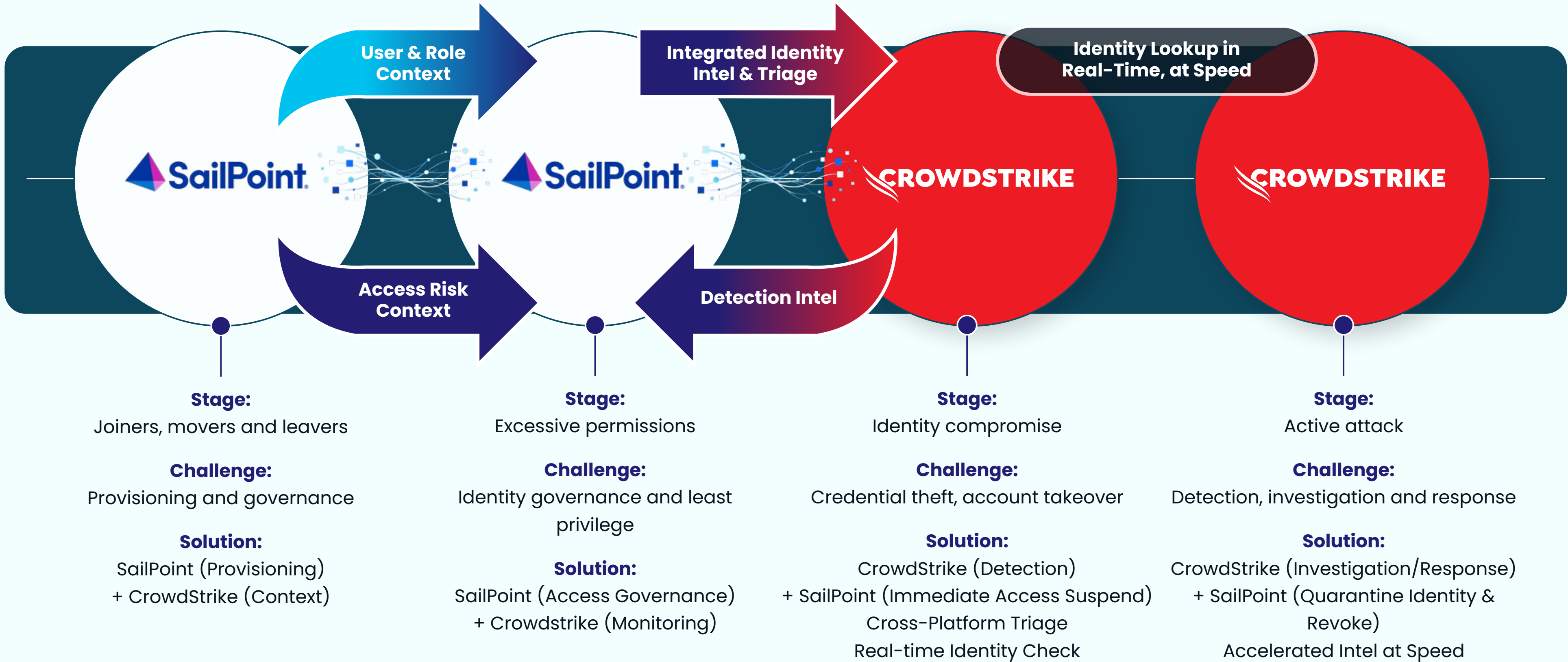
Identity to infrastructure.

THE IGNITION CURATED PORTFOLIO PROPOSITION

Reduce cyber risk by ensuring only the right identities have the right access, while detecting and responding to threats that target users, devices and workloads.

SailPoint and CrowdStrike offer identity security and active threat protection.

SailPoint governs who should have access. CrowdStrike detects when that access is being abused. The combined story is much bigger than IAM or EDR, it becomes Identity Driven Security. This is the modern identity attack journey.



Know every identity. Stop every threat.

AI identity security is much more than an IT issue, let's make sure partners convey the right message for the right audience.

AUDIENCE & MESSAGE MATRIX



CISO

Governance, accountability, board-level risk and regulatory exposure



IT Director

Operational control, visibility gaps, agent integration without oversight



Compliance/Risk

Audit trail, policy coverage, regulatory alignment



Procurement

AI identity control cost Vs incident cost

Let's get the conversation started

Can your customers answer these questions?

- Do you know how many non-human identities are operating in your environment right now?
- Who owns your AI agents' credentials when the person who created them leaves?
- If an AI agent behaved unexpectedly, how quickly would you know?
- What's your current policy for AI agent access provisioning and deprovisioning?
- How would your board answer a question about AI identity governance today?

Handling common objections

- 'We're not using agentic AI yet'**
You may be and not know it. Shadow AI is the practice of using AI without an organisation's knowledge, approval, or oversight.
- 'Our existing IAM covers this'**
Traditional IAM was built for humans. Machine identities operate differently, no MFA, no offboarding, no HR record.
- 'This isn't a board-level issue'**
It becomes one the moment an AI agent causes a data breach, a compliance failure, or a payment fraud.

AI adoption is accelerating faster than governance. Without identity controls, token consumption can spiral unnoticed, turning innovation into unexpected operational cost.



Five checks to discover AI identity opportunities

- 1  Organisation has deployed or is piloting Copilot, ChatGPT or similar personal assistants
- 2  No formal AI usage policy or governance framework in place
- 3  Existing IAM programme hasn't been reviewed since AI agent adoption began
- 4  Recent regulatory scrutiny or compliance activity touching data governance
- 5  Security or IT team expressing concern about shadow AI or unmanaged tool proliferation

Tap to open each report



AI agents: The new attack surface



AI agents: The new attack surface

A global survey of security and IT professionals and executives

→



CrowdStrike Global Threat Report



CrowdStrike 2026 Global Threat Report

27 min: The fastest recorded vCrime breakout time
80% increase in attacks by AI-enabled adversaries
62% of detections in 2025 were malware-free

Download report

Threat Landscape Overview

A definitive look at the cyber threat landscape

- Key adversary activity and events from 2025
- How AI is scaling attacks and lowering barriers to entry
- Expert guidance to defend against threats in the AI era

AI threats have reached a critical turning point

89%↑

→



Attack Landscape Report: How Threat Actors Tailor Tactics to Their Targets



THREAT INTELLIGENCE REPORT

Exposing **VENOM**:
C-Suite Credential Theft Campaign
Weaponizes Live Microsoft Authentication
to Establish Persistent Access

Microsoft Sign in

No account? Create one! Can't access your account?

Next

Sign in options

→



DMARC & The Identity Reckoning



SENDMARC

2026 Cyberthreat Report:
DMARC & The Identity Reckoning

→

Trusted by the industry



“When we were looking for a partner, we were looking for a specialist that was very focused on curating the right brands. So we were very grateful that Ignition took us on as a vendor. We see them as an extension of our business and our go-to-market strategy.”

Sacha Matulovich, Co-founder Sendmarc

With thanks to:

