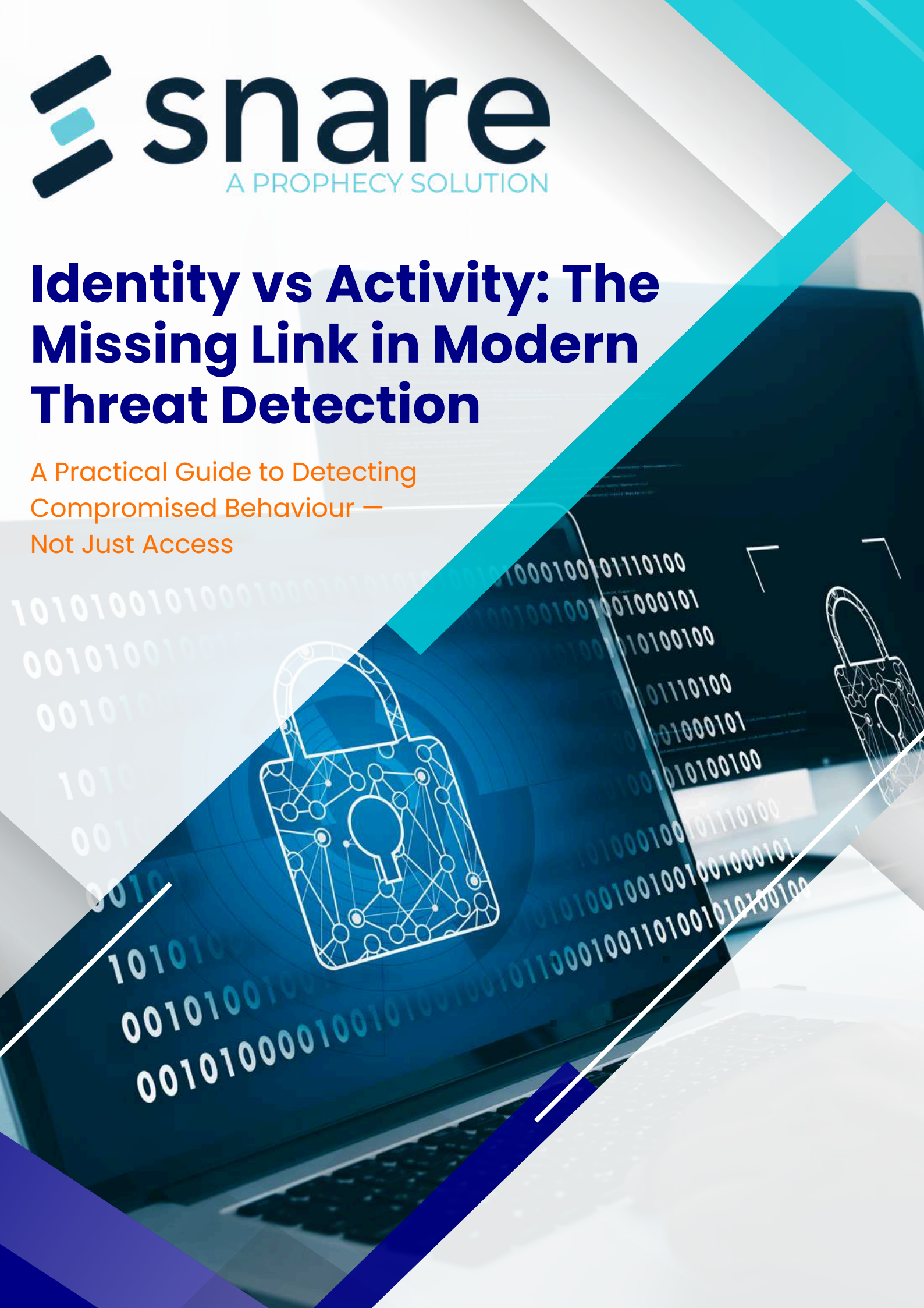
snare
A PROPHECY SOLUTION

Identity vs Activity: The Missing Link in Modern Threat Detection

A Practical Guide to Detecting Compromised Behaviour — Not Just Access



When “Access Granted” Becomes the Problem

For years, cybersecurity strategies have been built around one core principle:

If you control access, you control risk.

Identity became the new perimeter.

Organisations invested heavily in:

- Identity and Access Management (IAM)
- Multi-Factor Authentication (MFA)
- Privileged Access Controls

And for good reason.

Attackers are no longer breaking authentication — they’re passing it.

According to Gartner, identity compromise is now one of the most common entry points for breaches — shifting the focus from who accessed the system to what they did after access was granted.

Identity Is No Longer Enough

Identity tells you:

- Who logged in
- From where
- Using what credentials

But it does not tell you:

- Whether that access was legitimate
- Whether behaviour changed after login
- Whether actions align with expected patterns

The Core Problem

Identity answers "who."
Activity reveals intent.

This aligns closely with principles from Zero Trust Architecture, which emphasises continuous validation — not one-time authentication.

The Rise of Identity-Based Attacks

Modern attackers are targeting identity because:

- It bypasses perimeter controls
- It avoids detection systems
- It provides immediate access to trusted systems

Common Identity Attack Techniques

- Phishing and credential harvesting
- Token theft and session hijacking
- MFA fatigue and push bombing
- Privilege escalation using valid accounts

Why These Work

Once authenticated, attackers inherit trust.

And most systems:

- Do not challenge behaviour
- Do not validate intent
- Do not monitor activity deeply enough

The Blind Spot — Where Identity Fails

Security teams often assume:
"If the user logged in successfully, they are legitimate."
This assumption creates a dangerous blind spot.

Example Scenario

A user logs in from a familiar location.
No alerts are triggered.

But within minutes:

- Multiple systems are accessed
- Privileged commands are executed
- Sensitive data is queried

What Identity Shows

- Valid login
- Expected user
- No anomaly

What Activity Reveals

- Unusual sequence of actions
- Elevated access patterns
- Data access inconsistent with role

Identity confirms access.
Activity exposes compromise.

What Is Identity vs Activity Mapping?

Identity vs Activity Mapping is the process of:

Linking authenticated users to their actual behaviour across systems, over time.

It Answers Critical Questions

- What did the user do after login?
- Did behaviour align with their role?
- Were actions consistent with historical patterns?
- Did activity escalate or change suddenly?

Why This Matters

Without mapping identity to activity:

- You detect access
- But miss intent
- And fail to reconstruct the attack

Where Organisations Struggle

Based on industry insights from Forrester and real-world investigations, most organisations face:

1. Disconnected Data Sources

Identity logs, endpoint logs, and cloud logs exist — but are not linked.

2. Lack of Behavioural Context

Systems track events, not patterns.

3. Short-Term Visibility

Logs are not retained long enough to identify behaviour over time.

4. Over-Reliance on Alerts

Detection depends on thresholds — not investigation.

5. Inability to Reconstruct Events

Teams can see fragments, but not the full story.

You don't just need to know who logged in.
You need to understand what happened next.

What Good Identity vs Activity Mapping Looks Like

Strong organisations move beyond authentication and focus on **continuous behavioural visibility.**

Key Capabilities

1. End-to-End Traceability

Link identity → session → activity → outcome

2. Cross-System Correlation

Connect:

- IAM systems
- Endpoints
- Cloud platforms
- Applications

3. Behavioural Baselines

Understand what "normal" looks like per user or role

4. Full-Fidelity Logging

Capture detailed activity without losing context

5. Investigation Readiness

Enable teams to reconstruct timelines quickly

Key Insight

Identity is the starting point.
Activity is the evidence.

A Simple Mapping Framework

Use this practical model:

Step 1:	**Capture Identity Events**	• Login attempts • Authentication success/failure • MFA events
Step 2:	**Capture Activity Events**	• Commands executed • Files accessed • Systems touched • Privileges used
Step 3:	**Link Identity to Activity**	• Correlate timestamps • Match sessions • Track movement
Step 4:	**Analyse Behaviour**	• Compare to baseline • Identify anomalies in sequence, not just events
Step 5:	**Reconstruct the Narrative**	From login → to action → to impact

Self-Assessment — Are You Mapping Identity to Activity?

Can your team answer:

- What actions did a user perform after login?
- Did their behaviour change during the session?
- Did they access systems outside their role?
- Can you trace their full activity timeline?

Scoring

High Maturity
→ Full traceability across systems

Moderate Maturity
→ Partial visibility, limited correlation

Low Maturity
→ Identity visible, activity unclear

Why This Matters Now

Cybersecurity is shifting from:

- **Access control → Behaviour understanding**
- **Detection → Investigation**
- **Prevention → Proof**

**The future of security isn't knowing who logged in.
It's proving what they did.**

Conclusion

Identity will always be critical.
But on its own, it is no longer enough.

The organisations that detect modern threats are not those that trust identity — but those that verify behaviour.

Ready to see what your users are really doing?

- Identify your investigation gaps
- Benchmark your readiness
- Build a defensible logging strategy

Book a Log Strategy Session

snare
A PROPHECY SOLUTION

Toll Free US: 1(800) 834 1060
Asia/Pacific: +61 8 8213 1200
UK/Europe: +44 (800) 368 7423

AMERsales@prophecyinternational.com
APACsales@prophecyinternational.com
EMEAsales@prophecyinternational.com

snare
A PROPHECY SOLUTION