snare
A PROPHECY SOLUTION

Where Attacks Hide in Your Environment

A Practical Guide to Uncovering Modern Cyber Threats

Introduction: The Visibility Problem No One Talks About

Most organisations believe their security stack is working.

Firewalls are configured.
SIEM is ingesting data.
Alerts are being generated.

But modern cyber incidents are revealing a different truth:

It's not that organisations aren't detecting threats — it's that they can't see what actually happened.

According to Gartner, security teams are increasingly overwhelmed by data volume, yet still lack the context required to investigate incidents effectively. High ingestion does not equal high visibility.

At the same time, attackers have adapted.

They no longer rely on obvious exploits.
They rely on **blending into normal operations.**

Section 1: The Shift — From Breaking In to Blending In

Traditional cybersecurity models were built around **perimeter defence and anomaly detection.**

That model is now outdated.

Modern attackers:

- Use valid credentials
- Operate through trusted tools
- Move laterally without triggering alerts
- Stay undetected for extended periods

This aligns with industry observations from MITRE and its ATT&CK framework, where a growing number of techniques focus on **"living off the land"** — using legitimate system tools for malicious purposes.

What This Means

If your detection strategy relies only on "unusual behaviour," you will miss attacks that look normal.

Section 2: The Five Places Attacks Are Hiding Today

Modern threats don't hide in one place — they hide across your environment.

1. Identity and Access Systems

Attackers increasingly start with:

- Phished credentials
- Token theft
- MFA fatigue attacks

Once inside, they appear as legitimate users.

Why this matters:
Most detection tools trust authenticated users by default.

---

2. Endpoint Activity

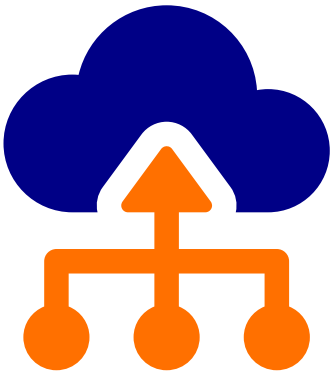
Attackers use:

- PowerShell x
- Command-line tools
- Remote administration utilities

These actions often look like standard IT operations.

Where visibility breaks:
If process-level logging isn't enabled or retained, activity becomes invisible.

3. Cloud and SaaS Environments



Threats hide in:

- Misconfigured permissions
- Unmonitored API calls
- Cross-system integrations

According to Forrester, cloud complexity is a major contributor to reduced visibility across modern enterprises.

---

4. Network Movement

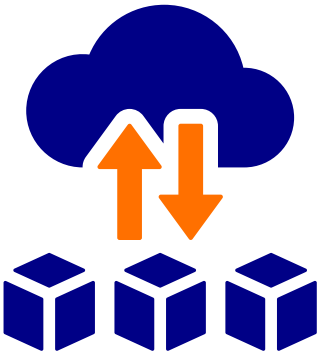
Lateral movement often:

- Uses internal traffic
- Avoids perimeter detection
- Mimics normal communication patterns

Key issue:
East-west traffic is rarely monitored with the same depth as external traffic.

---

5. Data Access and Exfiltration



Attackers:

- Access sensitive data slowly
- Use legitimate tools to extract it
- Avoid triggering volume-based alerts

Reality:
By the time exfiltration is detected, the damage is already done.

Section 3: Why Traditional Detection Is Failing

Security tools are designed to:

- Detect anomalies
- Trigger alerts
- Block known threats

But modern attacks:

- Avoid anomalies
- Generate low signal
- Operate within allowed behaviour

The Core Problem

Detection without context leads to noise.
Noise without visibility leads to missed threats.

According to Gartner, many organisations struggle with:

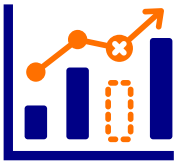
- High false positive rates
- Alert fatigue
- Limited investigation capability

Section 4: The Visibility Gap — Where Organisations Fall Short

Through real-world investigations, five consistent gaps appear:

1. Missing Logs

Critical systems are not logging key events.



2. Incomplete Coverage

Not all environments (cloud, endpoints, APIs) are captured.

3. Short Retention Periods

Logs are deleted before investigations begin.

4. Over-Filtering

Data is reduced before it can be analysed.

5. Lack of Correlation

Logs exist — but cannot be connected into a narrative.

The Result

You don't just miss the attack, you lose the ability to prove it happened.

Section 5: What Good Visibility Actually Looks Like

Strong security visibility is not about collecting more data.

It's about collecting **the right data, at the right fidelity, for the right duration.**

A Modern Visibility Model Includes:

- Full-fidelity log collection (before filtering)
- Coverage across identity, endpoint, cloud, and network
- Long-term retention for investigation
- Searchable and replayable data
- Clear mapping between events and outcomes

Key Insight

Visibility is not a tool.
It's an architecture.

Section 6: A Simple Self-Assessment

Use this to quickly assess your environment:

Can you answer the following within minutes?

- How did a user authenticate?
- What actions did they perform?
- What systems did they access?
- What changed as a result?
- What data was touched or moved?

Scoring Guide

High Confidence

→ You can reconstruct events end-to-end

Moderate Confidence

→ Partial visibility, gaps in timeline

Low Confidence

→ Unable to validate incident scope

Section 7: Why Logs Are the Foundation

Modern security stacks are powerful.
But they rely on one thing:

Accurate, complete, and accessible log data.

Logs are the only source that:

- Records actual activity
- Provides historical truth
- Supports investigation and compliance

Without Logs

- Alerts lack context
- Investigations stall
- Compliance becomes difficult
- Recovery is incomplete

Conclusion: The New Security Reality

Cyber threats are no longer defined by:

- How they enter

But by:

- **How well they can remain unseen**

The organisations that win are not those with the most tools —but those with the clearest visibility.

Not sure where attacks are hiding in your environment?

Start with visibility.

- Identify your logging gaps
- Understand your investigation readiness
- Align to modern frameworks

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