WHITE PAPER

The Detection Gap

Why Access Control Alone Is No Longer Enough to Protect Crown-Jewel Applications.

exeon

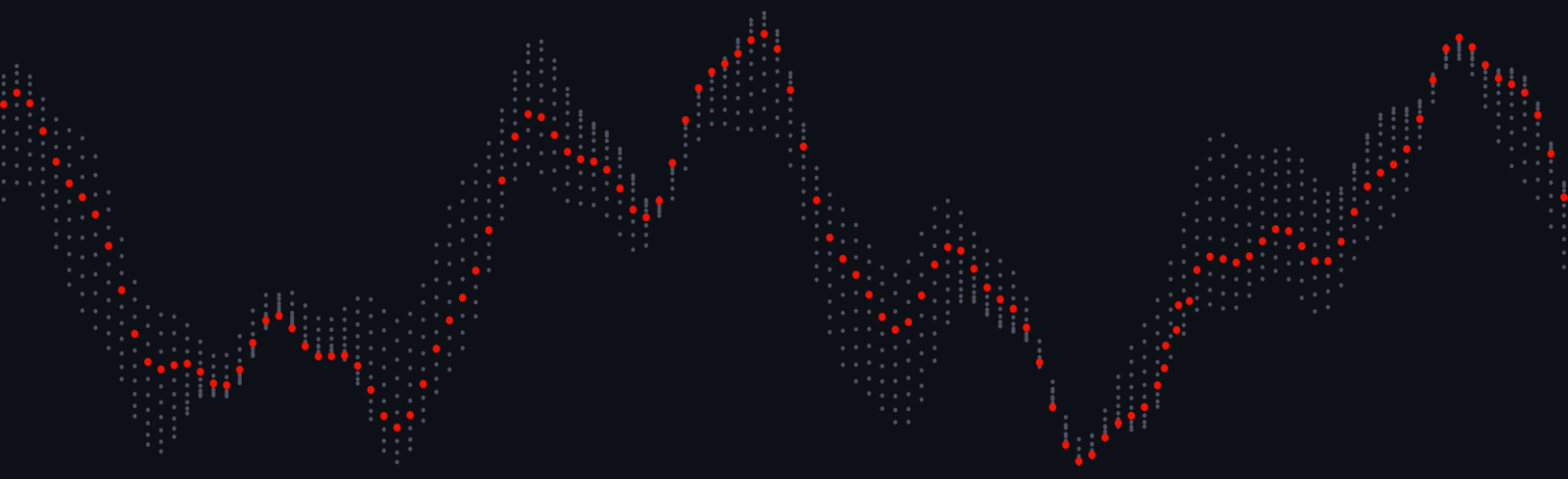
exeon.com

Table of Contents

01

SECTION 01

Executive Summary



For more than two decades, organizations have invested heavily in securing access to their most critical systems.

Identity and Access Management (IAM), Segregation of Duties (SoD), Governance Risk & Compliance (GRC), Privileged Access Management (PAM), multi-factor authentication, audit controls, and regulatory frameworks have significantly improved the way access is governed.

These investments were necessary.
They remain necessary.

Cyber incidents and long dwell times still show how difficult it is to understand what happens after access is granted. Many organizations cannot answer a basic operational question:

> **What are our users, administrators, partners, and service accounts doing right now inside our crown-jewel systems?**

This question sits at the center of what many security leaders increasingly recognize as a growing detection gap.

The challenge is particularly visible in systems that sit at the operational heart of the organization:

- SAP landscapes
- Core banking and wealth management platforms, such as Avaloq
- Clinical Information Systems such as Epic
- Oracle-based business platforms
- Abacus ERP environments
- Manufacturing execution systems
- Energy and utility control platforms
- Industry-specific operational systems

These crown-jewel systems differ by industry, architecture, and vendor.

They share one characteristic:

They contain the organization's most critical business processes, data, and decisions.

The traditional question has been: Who should have access?
The emerging question is: How quickly can we detect when legitimate access is being used in illegitimate ways?

Five findings shaping the detection gap

01 **Identity has become the primary attack surface**

Modern attackers increasingly obtain access through valid credentials rather than technical exploits.

02 **Crown-jewel applications amplify business impact**

Compromise of operational platforms directly affects revenue, operations, customers, patients, citizens, and supply chains.

03 **Traditional controls remain necessary but insufficient**

While access governance explains permissions, it does not necessarily explain behavior.

04 **Security visibility remains fragmented**

Application teams, IAM teams, compliance teams, and SOC teams often observe different parts of the same story.

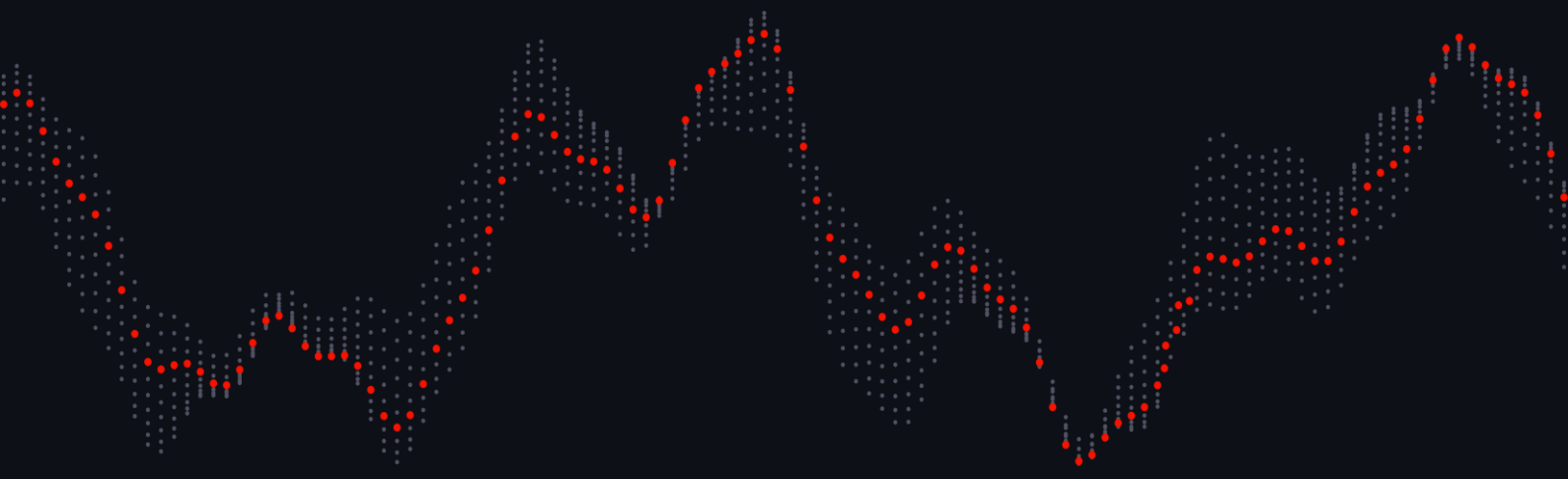
05 **Detection is becoming a resilience requirement**

Regulators increasingly expect organizations not only to prevent incidents, but also to identify them rapidly.

02

SECTION 02

The Threat Model Has Changed



For years, security strategies concentrated on keeping unauthorized users outside the perimeter. Modern attacks increasingly bypass that model because valid credentials can provide the access an attacker needs.

- Phishing
- Social engineering
- Identity theft
- Third-party compromise
- Session hijacking
- Insider abuse
- Misconfigured integrations

Modern attackers don't break in, they log in.

Once authenticated, they often appear indistinguishable from legitimate users.

- The credentials are valid.
- The permissions are valid.
- The transactions are valid.

The challenge is no longer simply granting secure access. It is understanding behavior after access has been granted.

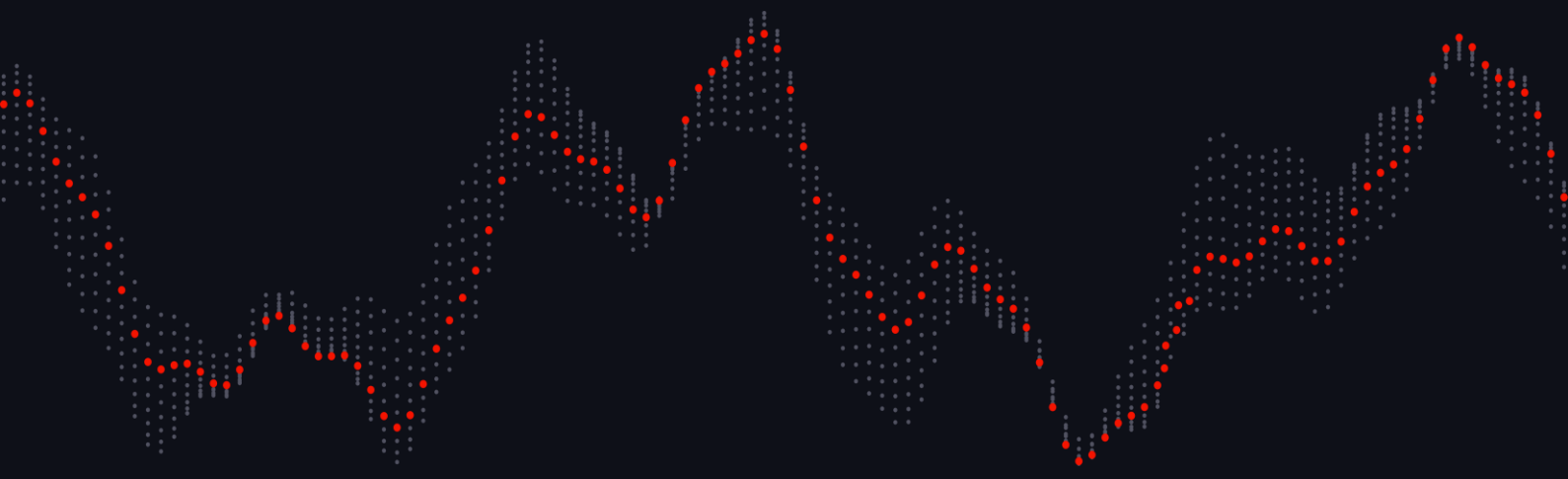
Attackers increasingly operate as legitimate users.

The most damaging cyber incidents increasingly involve valid identities performing illegitimate actions.

03

SECTION 03

Understanding the Three Types of Insiders



Insider risk is no longer limited to malicious employees. Many identity-driven incidents involve people who already have legitimate access to systems, applications and business processes. What distinguishes them is their intent, behavior and circumstances.
Three categories consistently emerge.

The Malicious Insider

The malicious insider intentionally abuses their access for personal, financial, ideological, or competitive gain.

- Theft of sensitive information
- Fraudulent financial transactions
- Sabotage of systems or processes
- Deliberate disclosure of confidential information

Although these incidents often attract significant attention, they represent only one dimension of insider risk.

The malicious insider understands the environment, knows where critical information resides, and frequently understands how to avoid traditional controls.

The Careless Insider

The careless insider has no malicious intent. Risk emerges through mistakes, negligence, or unsafe practices.

Examples include:

- Falling victim to phishing attacks
- Sharing credentials
- Misconfiguring systems
- Sending sensitive information to unintended recipients
- Circumventing controls for convenience such as forgetting to lock the screen
- Using unauthorized applications or cloud services

In many organizations, this category represents the largest source of security incidents.

The challenge is not malicious intent. The challenge is recognizing when routine, careless, or convenience-driven actions create material risk.

The Compromised Insider

The compromised insider has become one of the most important risk categories in modern cybersecurity.

In this scenario, the user is neither malicious nor careless. Instead, an external actor gains control of their identity through:

- Credential theft
- Malware
- Session hijacking
- Social engineering
- Third-party or supply-chain compromise

The attacker then operates using a legitimate identity.

From the perspective of many systems, the activity appears valid:

- Correct username
- Correct authentication
- Approved permissions
- Authorized transactions

The only meaningful difference is the behavior itself.

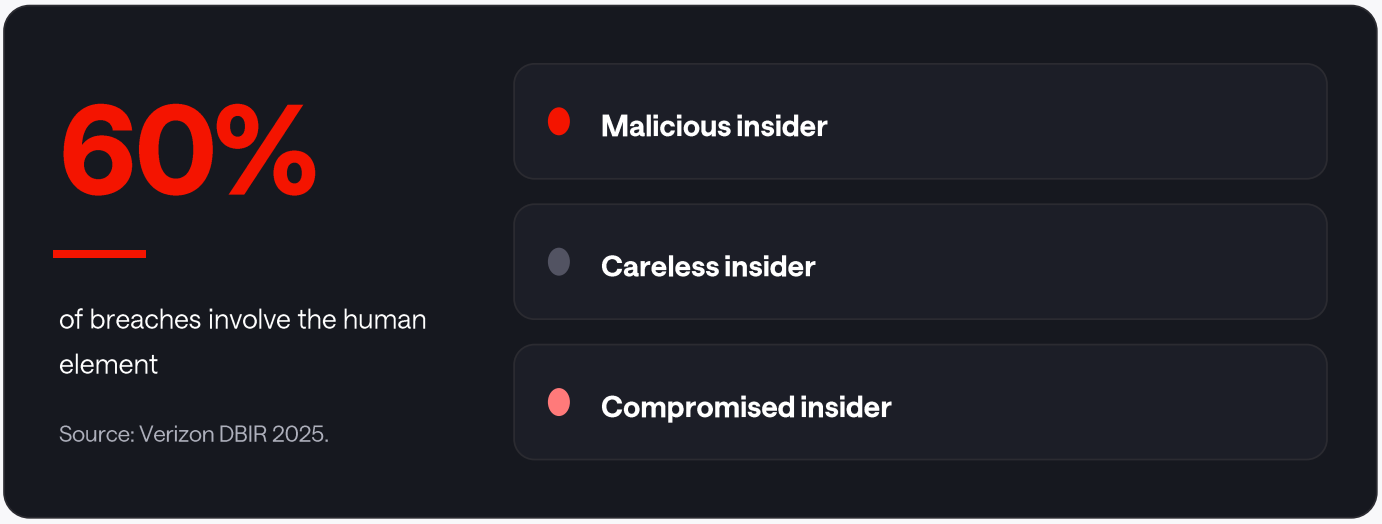


Figure 1. *Although motivations differ significantly, all three categories frequently appear as legitimate users operating within approved systems.*

The Critical Observation

A malicious insider, a careless insider, and a compromised insider may all:

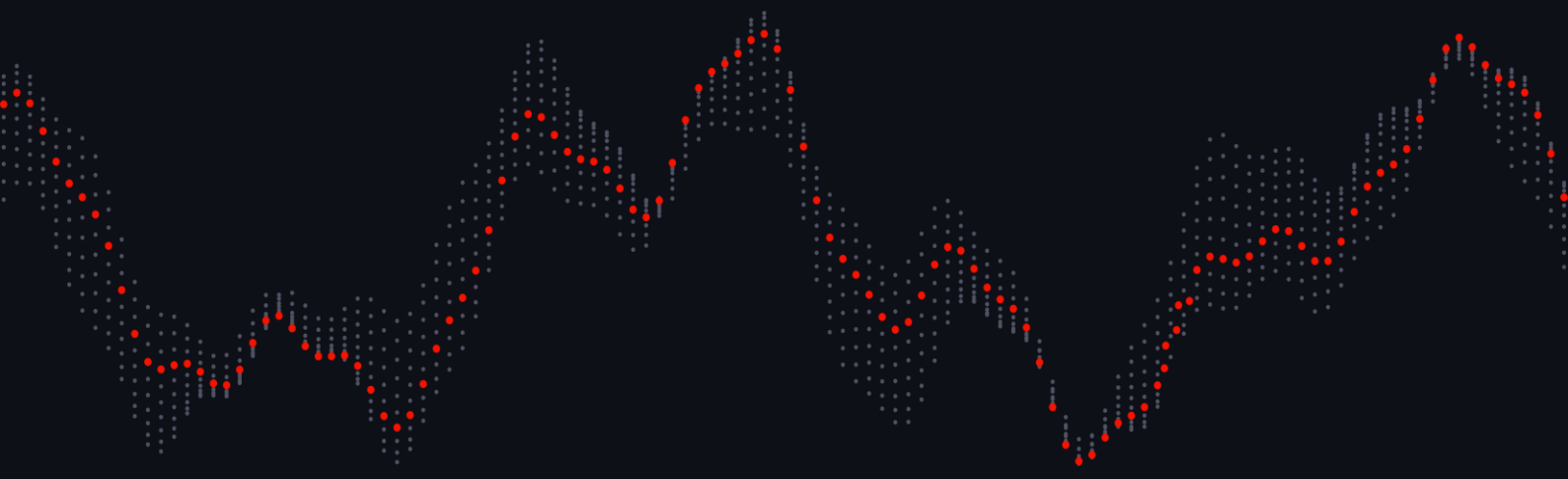
- **Log in successfully**
- **Access approved systems**
- **Use authorized applications**
- **Operate within assigned permissions**

> Access controls are highly effective at determining whether access should exist, but they cannot always show whether the resulting behavior makes sense.
> **This is the line between access governance and threat detection.**

04

SECTION 04

Why Crown-Jewel Applications Matter



Not all systems are equally important. Most organizations possess a small number of platforms whose compromise would create immediate operational consequences.

The specific applications vary by sector.

INDUSTRY	CROWN-JEWEL SYSTEMS
Manufacturing	SAP, MES, Supply Chain Platforms
Financial Services	Core Banking Systems, Avaloq, Payment Platforms
Healthcare	Epic, Clinical Information Systems
Retail	ERP, Logistics Platforms
Energy & Utilities	OT Platforms, Asset Management Systems
Public Sector	Citizen Services Platforms, Financial Systems

Compromise of these systems can result in:

- Financial fraud
- Operational disruption
- Regulatory breaches
- Patient safety risks
- Supply chain interruptions
- Data exfiltration
- Loss of public trust

These systems often contain a unique combination of:

- Sensitive information
- Extensive privileges
- Business process authority
- Cross-system integrations

As a result, attackers increasingly view them as high-value targets.

KEY INSIGHT

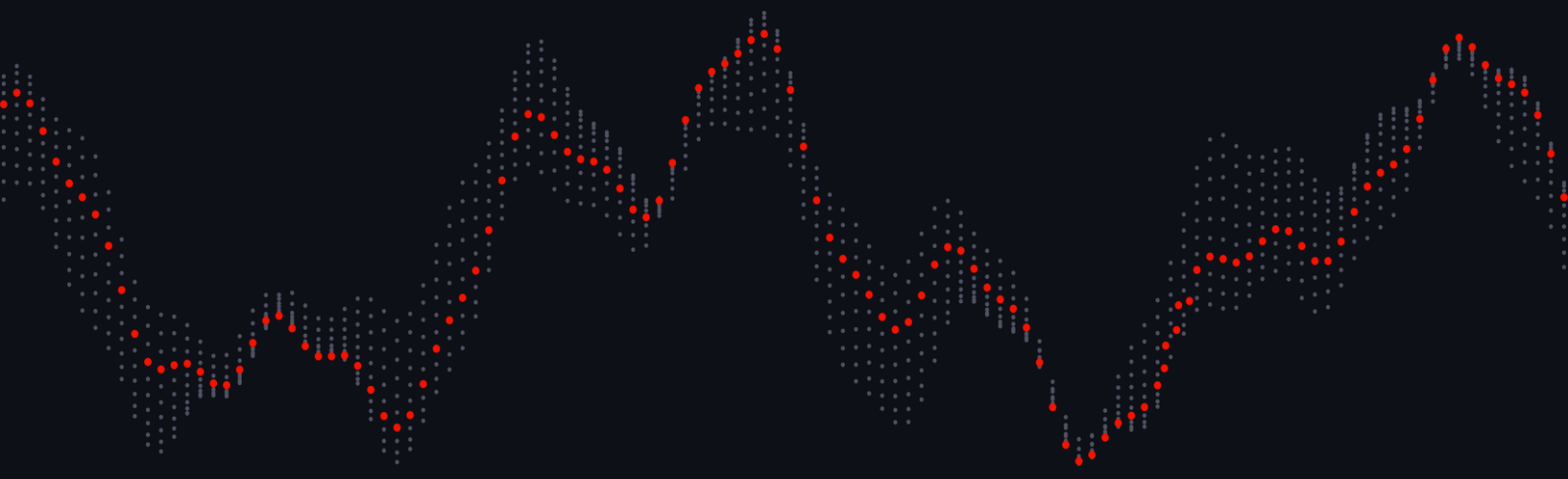
The objective is rarely the application itself.

The objective is the business process, data, or operational leverage that the application controls.

05

SECTION 05

How Enterprise IT Actually Operates Today



The reality of modern enterprise architecture differs significantly from the environments for which many security models were originally designed.

Organizations now operate across:

- Legacy on-premises systems
- Private cloud environments
- Public cloud platforms
- OT and IoT environments
- SaaS applications
- Third-party ecosystems
- Remote workforces

> **Yet one factor increasingly connects them all: Identity.**

A single human or machine identity may interact with dozens of systems across multiple environments.

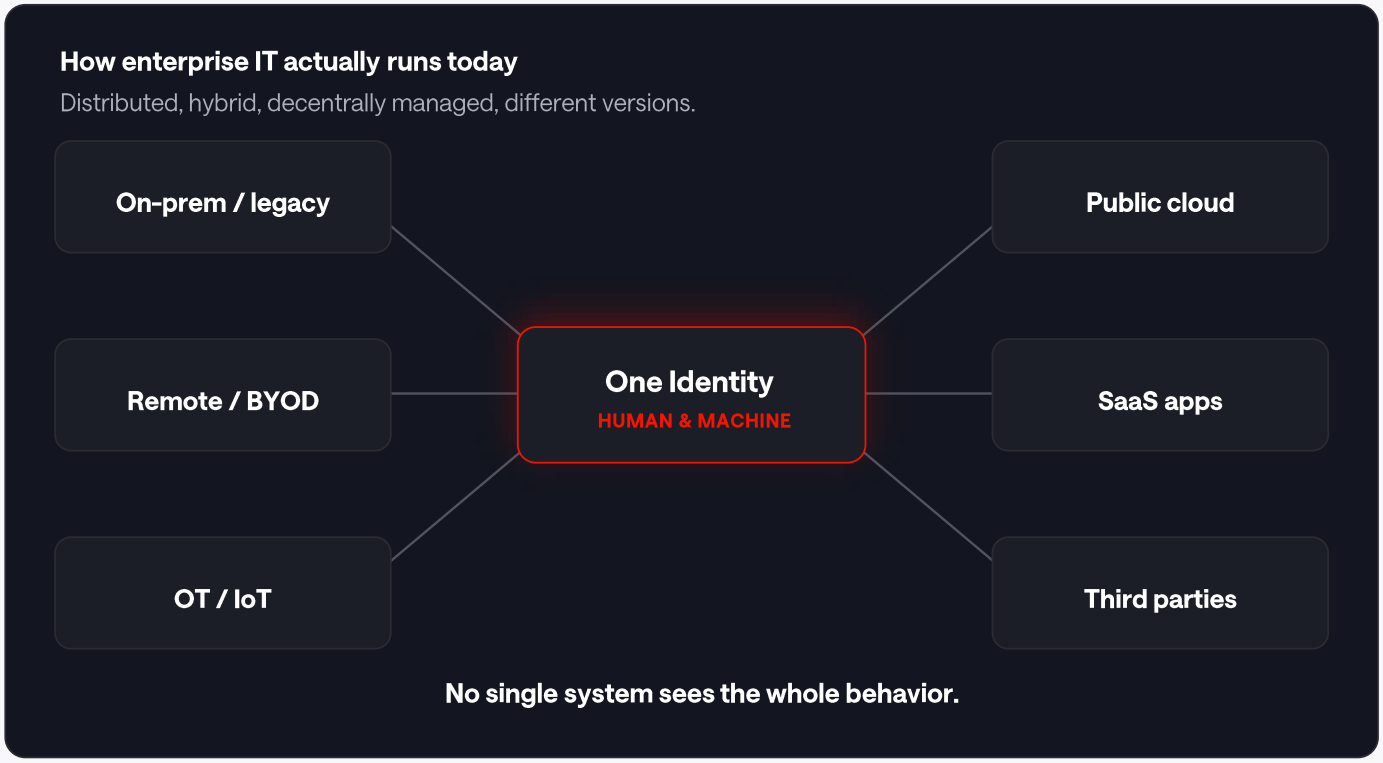


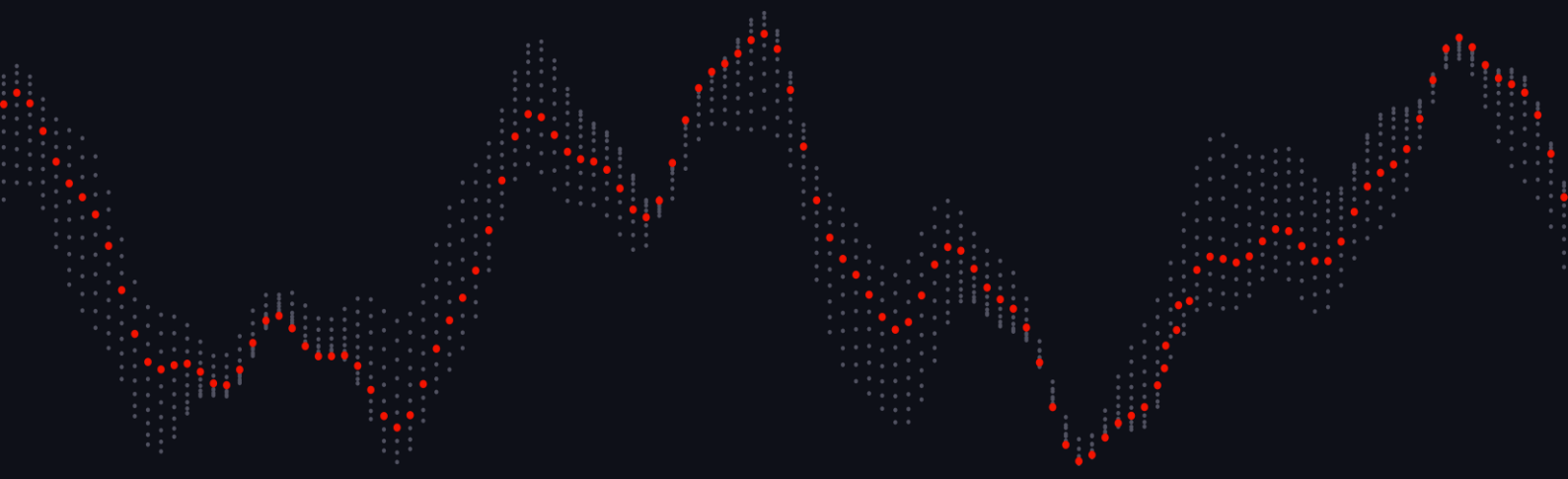
Figure 2. *One identity increasingly spans multiple technology domains. No single system sees the complete behavioral picture.*

As identities move across environments, understanding activity becomes increasingly difficult. What appears normal in one system may look very different when viewed across the broader business context.

06

SECTION 06

The Maturity of Modern Access Control



THE MATURITY OF MODERN ACCESS CONTROL

Organizations have made enormous progress in controlling access.

Across industries, mature programs now include:

- Identity and Access Management (IAM)
- Role-Based Access Control (RBAC)
- Attribute-Based Access Control (ABAC)
- Segregation of Duties (SoD)
- Privileged Access Management (PAM)
- Multi-Factor Authentication (MFA)

Together, these capabilities answer a critical question: who may perform which action?

Strong governance remains the foundation of security, but legitimate permissions do not guarantee legitimate behavior.

A user may possess legitimate permissions and still act in a manner that is:

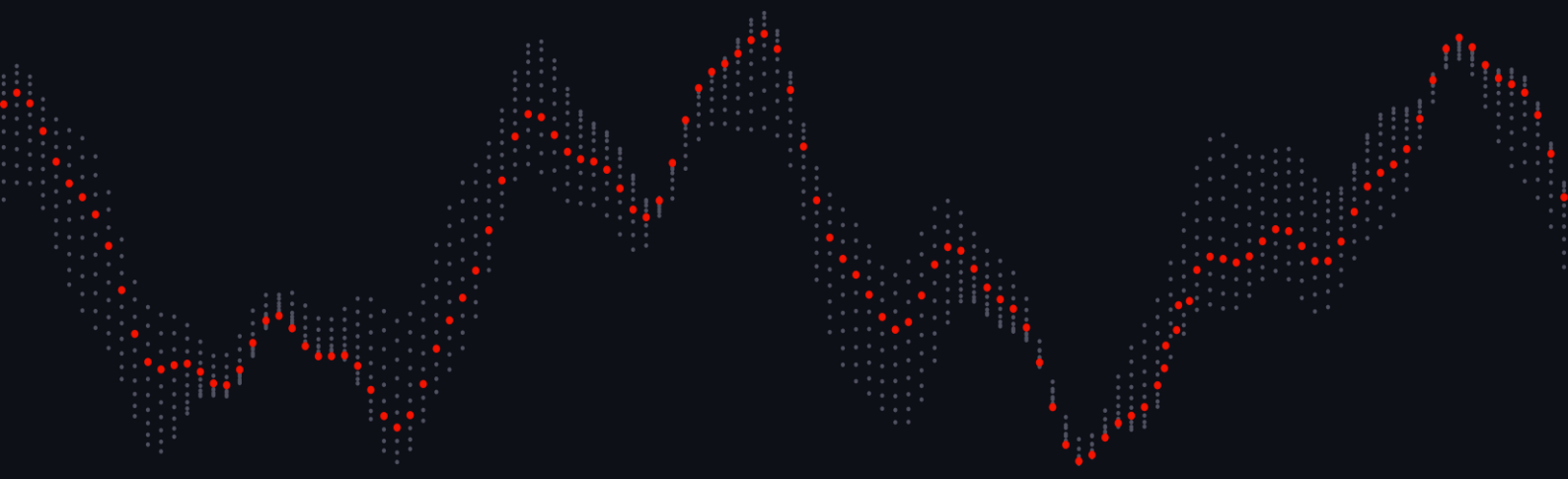
- Unusual
- Risky
- Suspicious
- Malicious

The distinction increasingly matters.

07

SECTION 07

The Detection Gap



Traditional controls generally operate in one of two timeframes.

BEFORE ACTIVITY

Access controls determine:

- Who should have access
- Which privileges they receive
- Which risks must be mitigated

AFTER ACTIVITY

Audits determine:

- What happened
- Whether policies were followed
- Whether violations occurred

Both controls are important, but they describe access before activity and evidence after it. Neither necessarily explains what is happening while the activity is taking place, which creates the detection gap.

Many organizations excel at governing access and documenting activity.

Far fewer excel at understanding behavior while activity is taking place.

The detection gap emerges whenever legitimate activity cannot be distinguished from suspicious activity.

Examples include:

- An administrator using tools they never previously used
- A finance user exporting unusually large datasets
- A service account behaving differently than normal
- A privileged user operating outside expected patterns
- A third-party account accessing unfamiliar systems
- A clinician retrieving patient records unrelated to their role
- A banking administrator making unusual configuration changes

Each action may be authorized in isolation; risk emerges from how the actions relate over time. This is why visibility, rather than another access rule, has become a central challenge in protecting crown-jewel applications.

> **This is where many organizations discover that visibility, rather than access control, has become the next major challenge in protecting crown-jewel applications.**

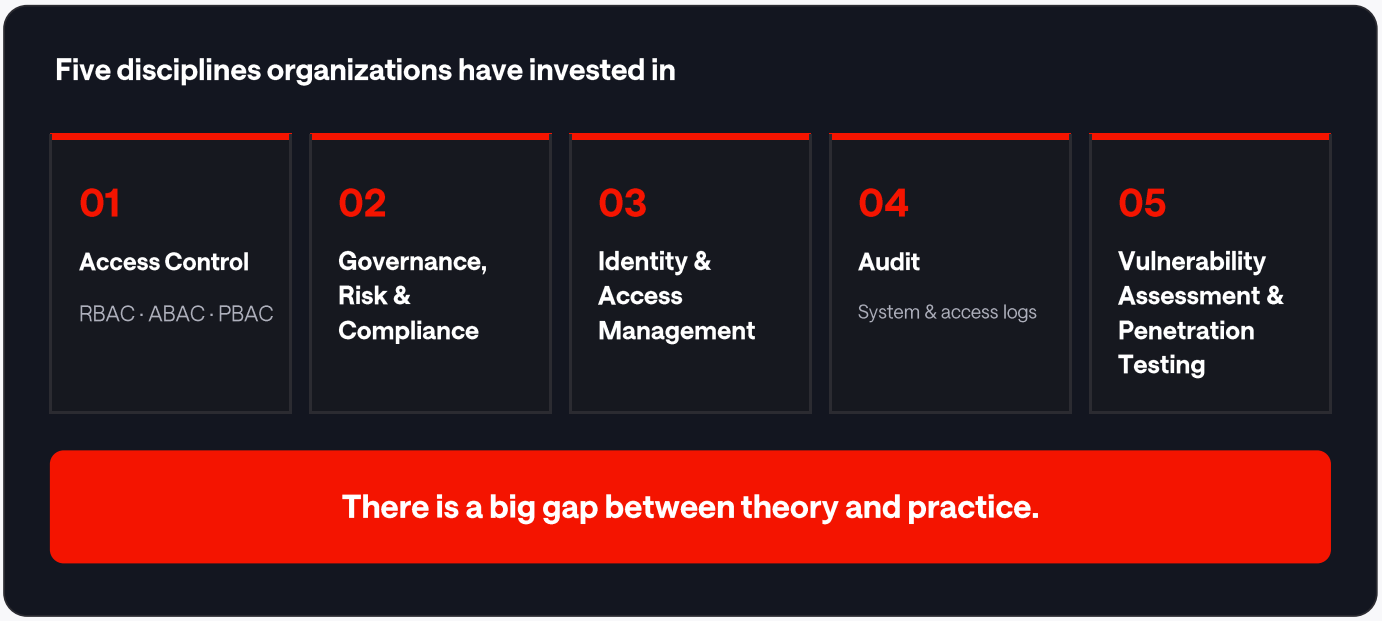
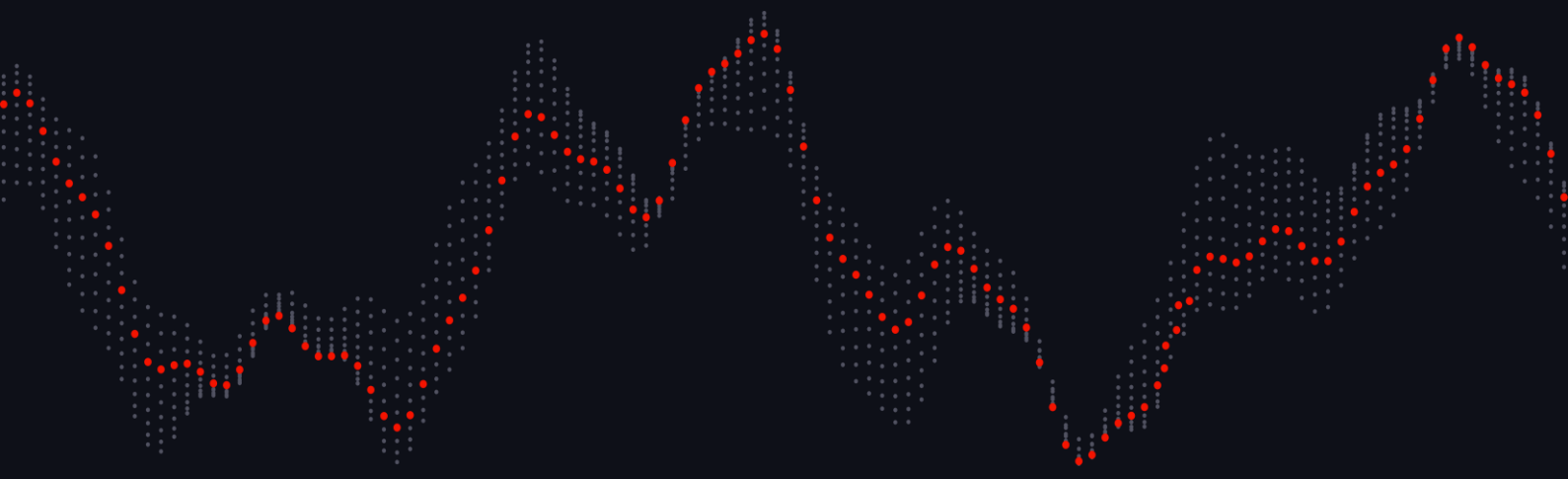


Figure 3. *Organizations have invested heavily in governing access, managing risk, and documenting activity. Yet a critical gap often remains between what identities are permitted to do and what they do in practice.*

08

SECTION 08

Why Event-Based Monitoring Falls Short



Most organizations are not suffering from a lack of security controls.

In fact, many have invested heavily in:

- Identity governance
- Privileged access management
- Security monitoring
- Audit programs
- Security operations centers
- Compliance frameworks

Yet major breaches continue to occur.

This raises an uncomfortable question: How can organizations possess so much security data and still struggle to detect misuse?

The answer often lies in a fundamental distinction:

Collecting activity is not the same as understanding activity.

Many organizations possess:

- Authentication logs
- Audit records
- Transaction histories
- Infrastructure telemetry
- Application logs

When these datasets are reviewed independently**, organizations gain records without context**: they know what happened but cannot easily determine whether it was unusual.

The Difference Between Events and Behavior

Traditional monitoring is largely event-centric. It focuses on questions such as:

- Did a login occur?
- Was a privileged command executed?
- Was a configuration changed?
- Was a file accessed?

These events are important.

However, attackers rarely reveal themselves through a single event.

Instead, risk emerges through a sequence of individually legitimate actions.

For example:

1. A user logs in.
2. The user accesses an administrative function.
3. The user changes a role.
4. The user accesses sensitive data.
5. The user exports information.

Each action may be authorized in isolation, but the sequence changes the assessment.

Behavior gains meaning from context; individual events rarely provide it.

KEY INSIGHT

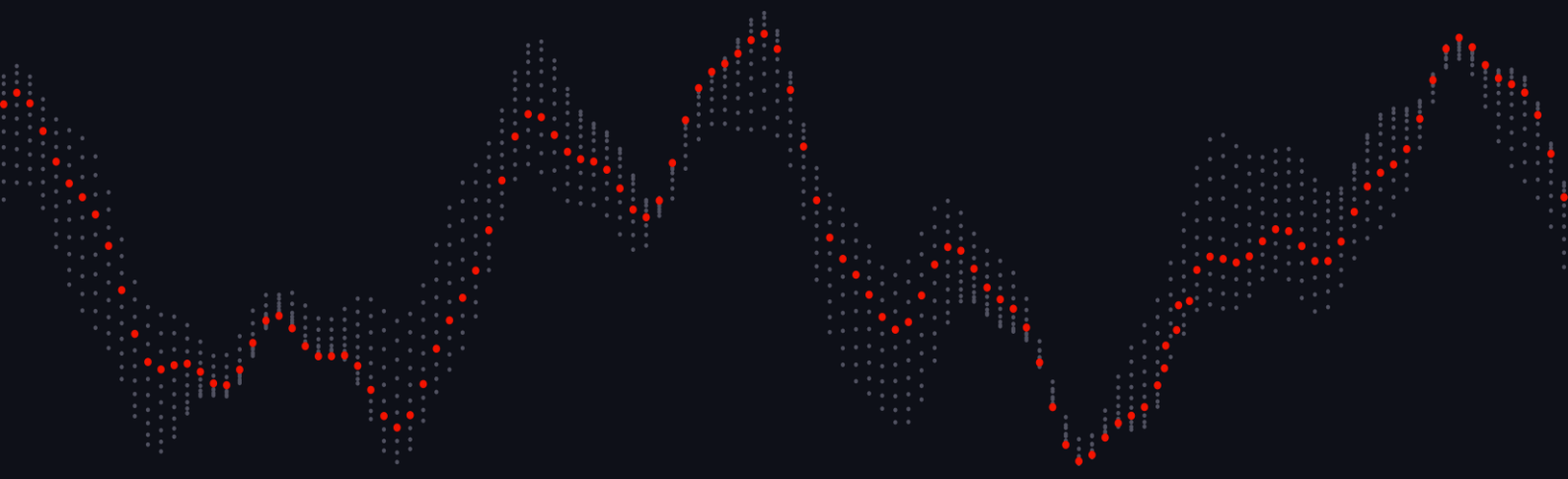
Most incidents are not discovered because a single action looks suspicious.

They are discovered because a sequence of actions tells a different story.

09

SECTION 09

The Visibility Problem



The Organizational Blind Spot

The challenge is not only technological. It is increasingly organizational.

Over time, enterprise security responsibilities have become highly specialized. Different teams focus on different dimensions of risk.

TEAM	PRIMARY FOCUS
IAM	Identity lifecycle and access governance
Application Security	Application controls and configuration
Compliance & Audit	Evidence and policy adherence
Infrastructure Teams	Availability and operations
SOC	Security monitoring and incident response

Each team performs valuable work, but no team sees the complete picture.
In crown-jewel applications, a suspicious sequence can cross business processes, permissions, threat indicators and compliance controls simultaneously, while still appearing benign through any single operational lens.

For example:

- An ERP team may understand business processes.
- An IAM team may understand permissions.
- A SOC may understand indicators of compromise.
- An audit team may understand compliance obligations.

A Common Pattern

Application teams frequently ask:
Is the system operating correctly?

Security teams ask:
Is the environment under attack?

Compliance teams ask:
Is the control functioning?

Executives ask:
Are we resilient?

All are valid questions. None individually explain behavior.

Shared Responsibility and Ecosystem Complexity

Enterprise technology environments have become significantly more distributed.

Historically, organizations owned:

- The infrastructure
- The application
- The data
- The operational processes

Today, responsibilities are frequently shared among:

- Internal IT teams
- Managed service providers
- Software vendors
- Hyperscalers
- SaaS providers
- Third-party partners

The shared-responsibility model improves scalability and flexibility, but it also distributes security context across several stakeholders.
Accountability becomes harder to maintain when no party sees the complete flow of activity.

Crown-Jewel Applications Are Becoming Ecosystems

Many organizations no longer operate critical applications as isolated platforms. Instead, they exist within broader digital ecosystems: interconnected environments that link infrastructure, applications, users, machine identities, data, and external partners across organizational boundaries.

A typical environment may include:

- ERP systems
- Identity providers
- Collaboration platforms
- Cloud services
- Data warehouses
- External integrations
- Managed services

These ecosystems create complex interdependencies that are harder to monitor and secure than standalone systems. The security challenge increasingly lies in understanding how business-critical processes traverse multiple platforms, providers, and identities.

Why Infrastructure-Centric Monitoring Is No Longer Enough

Many security programs were designed around infrastructure.

Servers | **Networks** | **Endpoints** | **Perimeter controls**

Applications were often treated as separate operational domains, but modern attacks increasingly cross that boundary.

An attacker may generate few infrastructure signals while creating substantial risk inside a legitimate business application.

Examples include:

- Fraudulent financial transactions
- Unauthorized data exports
- Privilege escalation
- Administrative abuse
- Configuration manipulation

Because these actions occur inside legitimate business applications, traditional monitoring may observe the session without understanding the business significance of the activity.

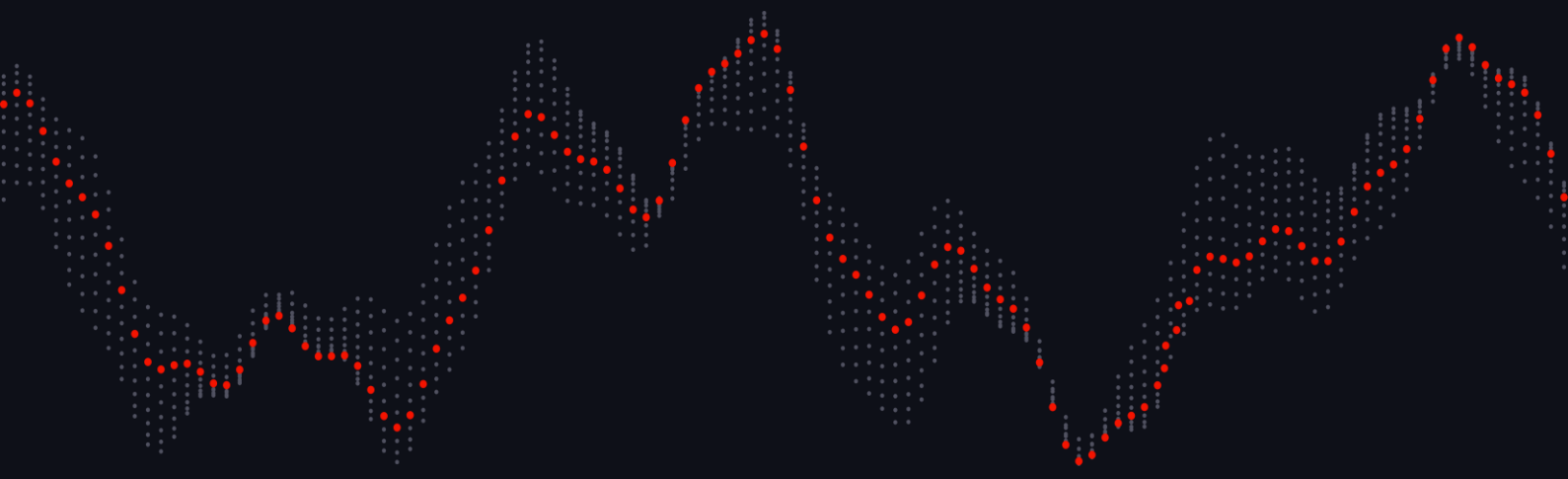
Infrastructure visibility explains where activity occurs.

Behavioral visibility explains why activity matters and when it may indicate misuse.

10

SECTION 10

The Evolution Toward Behavioral Security



Organizations are beginning to recognize that access governance alone cannot answer every security question. A useful way to understand this evolution is through three complementary layers.

LAYER 01

Assignment

Who May?

This layer determines:

- Who receives access
- Which permissions are granted
- Which risks require mitigation

Examples include:

- Identity and Access Management (IAM)
- Role-Based Access Control (RBAC)
- Attribute-Based Access Control (ABAC)
- Segregation of Duties (SoD)
- Access reviews

Assignment creates the foundation of trust.
Without it, secure operations are impossible.

LAYER 02

Runtime

Who Is?

This layer verifies:

- Authentication
- Session legitimacy
- Identity assurance
- Device trust
- Access context

Examples include:

- Multi Factor Authentication (MFA)
- Conditional access
- Identity verification
- Session management

Runtime determines whether the user is who they claim to be.

LAYER 03

Behavior

What Are They Doing?

This layer focuses on activity.
Questions include:

- Is this normal?
- Is this expected?
- Is this consistent with historical behavior?
- Does this sequence make sense?

Unlike assignment and authentication, behavior evolves continuously.
Risk becomes contextual rather than static.

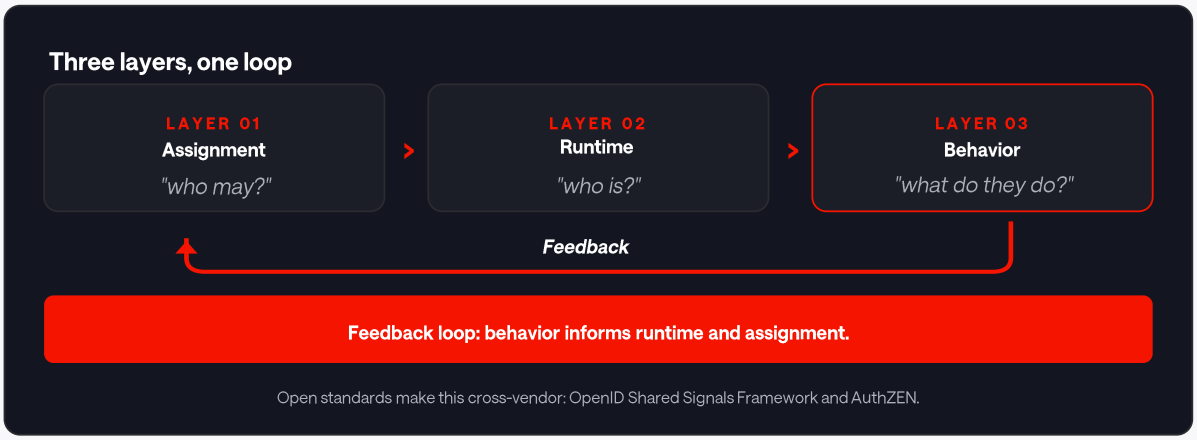
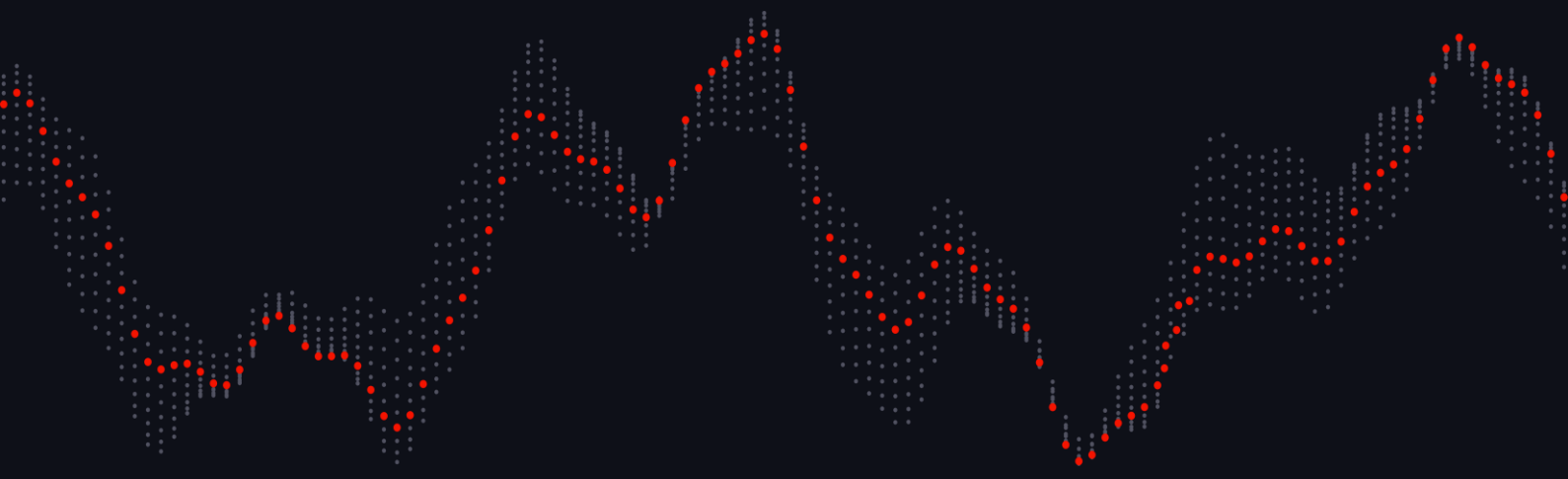


Figure 4. *Modern security increasingly depends on the continuous interaction between governance, authentication, and behavior rather than isolated controls.*

11

SECTION 11

Why Behavior Matters



Behavior introduces something traditional controls cannot easily provide: **Context.**

Consider two users performing the same action.

USER A

performs the action every day.

USER B

has never performed the action before.

Technically: The activity is identical.

Behaviorally: **The risk may be very different.**

This distinction becomes increasingly important in environments where attackers use legitimate credentials.

Behavior as an Early Warning Signal

Behavioral changes can become visible before damage occurs. These indicators may not prove malicious intent, but they can show that an activity deserves closer attention.

Examples include:

- Unusual administrative activity
- Changes in working patterns
- Unexpected system usage
- Sudden privilege changes
- First-time access to sensitive data
- Unusual transaction sequences

KEY INSIGHT

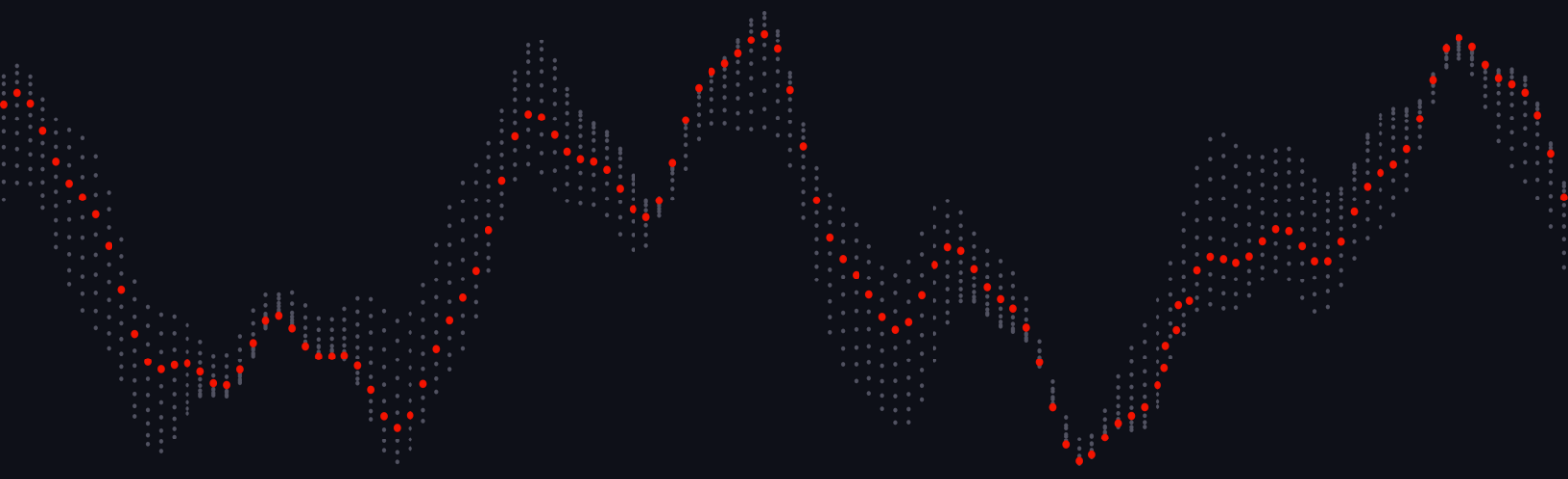
Behavioral signals are rarely evidence. They are often early indicators.

The objective is not certainty. The objective is earlier visibility.

12

SECTION 12

The Regulatory Shift



Regulators increasingly recognize the importance of rapid detection.

Compliance programs have traditionally focused on proving that controls exist.

Resilience frameworks increasingly ask whether organizations can detect, respond to and report an incident quickly when prevention fails.

NIS2

NIS2 emphasizes:

- Risk management
- Operational resilience
- Incident reporting
- Management accountability

The underlying expectation is clear: Organizations must understand what is happening within critical systems.

DORA

DORA introduces similar expectations for financial institutions. The focus extends beyond prevention toward:

- Operational resilience
- Continuous monitoring
- Incident management
- Incident management

The question increasingly becomes: How quickly can an organization identify abnormal activity?

A Changing Audit Conversation

Historically, audits focused heavily on access.

Typical questions included:

- Are roles defined?
- Are permissions reviewed?
- Are conflicts mitigated?

These questions remain important.

Resilience reviews and audits increasingly extend beyond access governance to operational questions such as:

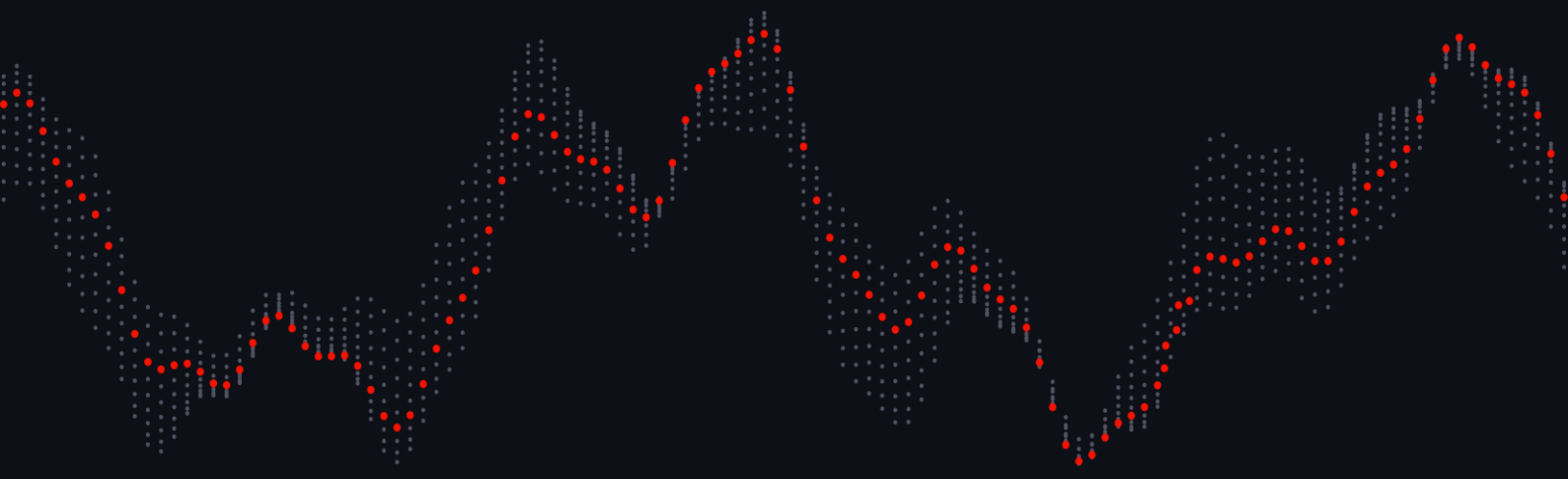
- **How quickly can misuse be detected?**
- **How are abnormal behaviors identified?**
- **How is operational visibility maintained?**
- **How are identity-driven risks monitored?**

Tomorrow's audit may focus less on whether a control exists and more on how quickly an organization recognizes when that control fails.

13

SECTION 13

The Future of Crown-Jewel Protection



Most organizations already have substantial governance frameworks, so the next step is unlikely to be more roles, policies or audit evidence.

The harder challenge is gaining visibility into how access is actually used.

As enterprise environments continue to expand across cloud, SaaS, third parties, operational technology, and industry-specific platforms, behavior increasingly becomes the common language connecting them all.

The question is no longer simply:

Is this action authorized?

THE MORE IMPORTANT QUESTION BECOMES:

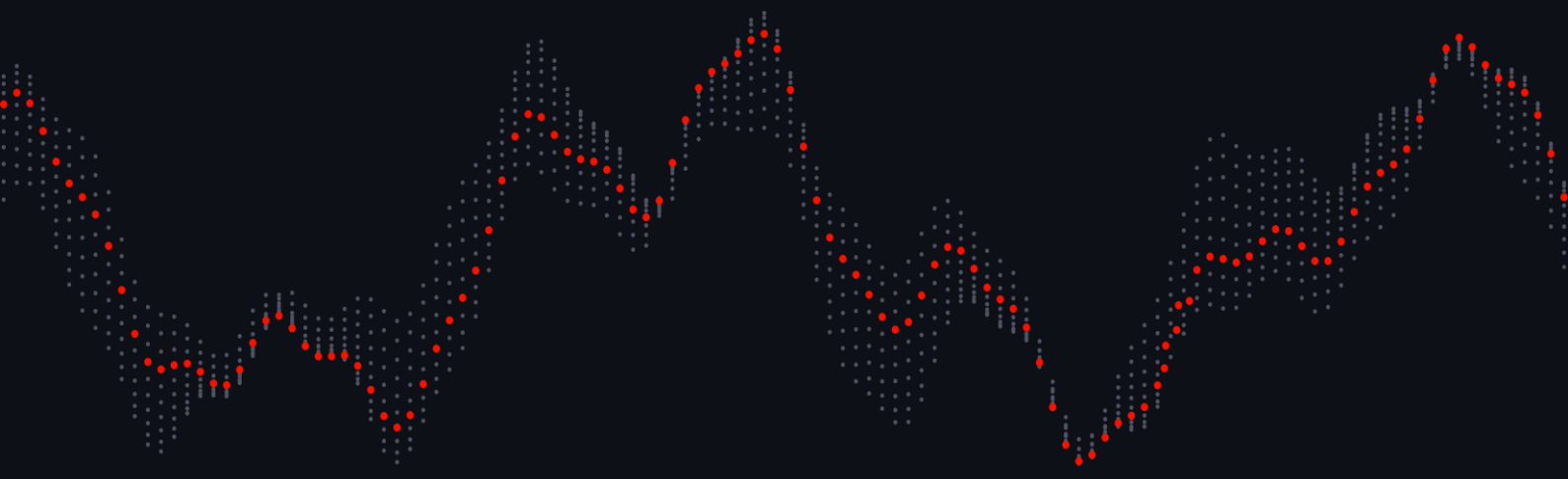
Does this behavior make sense?

Organizations that can answer this question quickly are better equipped to contain misuse, protect critical operations and meet their resilience obligations.

14

SECTION 14

Conclusion



The next chapter of enterprise security does not replace identity governance, compliance, access control or security operations.
Behavioral analytics like User and Entity Behavior Analytics (UEBA) and Identity Threat Detection and Response (ITDR) complement these disciplines by showing how legitimate access is used after authentication.

> Whether the platform is SAP, Avaloq, Epic, Oracle, Abacus, a core banking system or another crown-jewel application, the question remains the same:
>
> **Can we detect misuse quickly enough?**

Increasingly, the answer to that question may determine the difference between a contained incident and a business crisis.

The future of resilience will depend not only on controlling access, but on understanding behavior.

And in a world where attackers increasingly operate through legitimate identities, that understanding may become one of the most important security capabilities organizations develop over the coming decade.

exeon