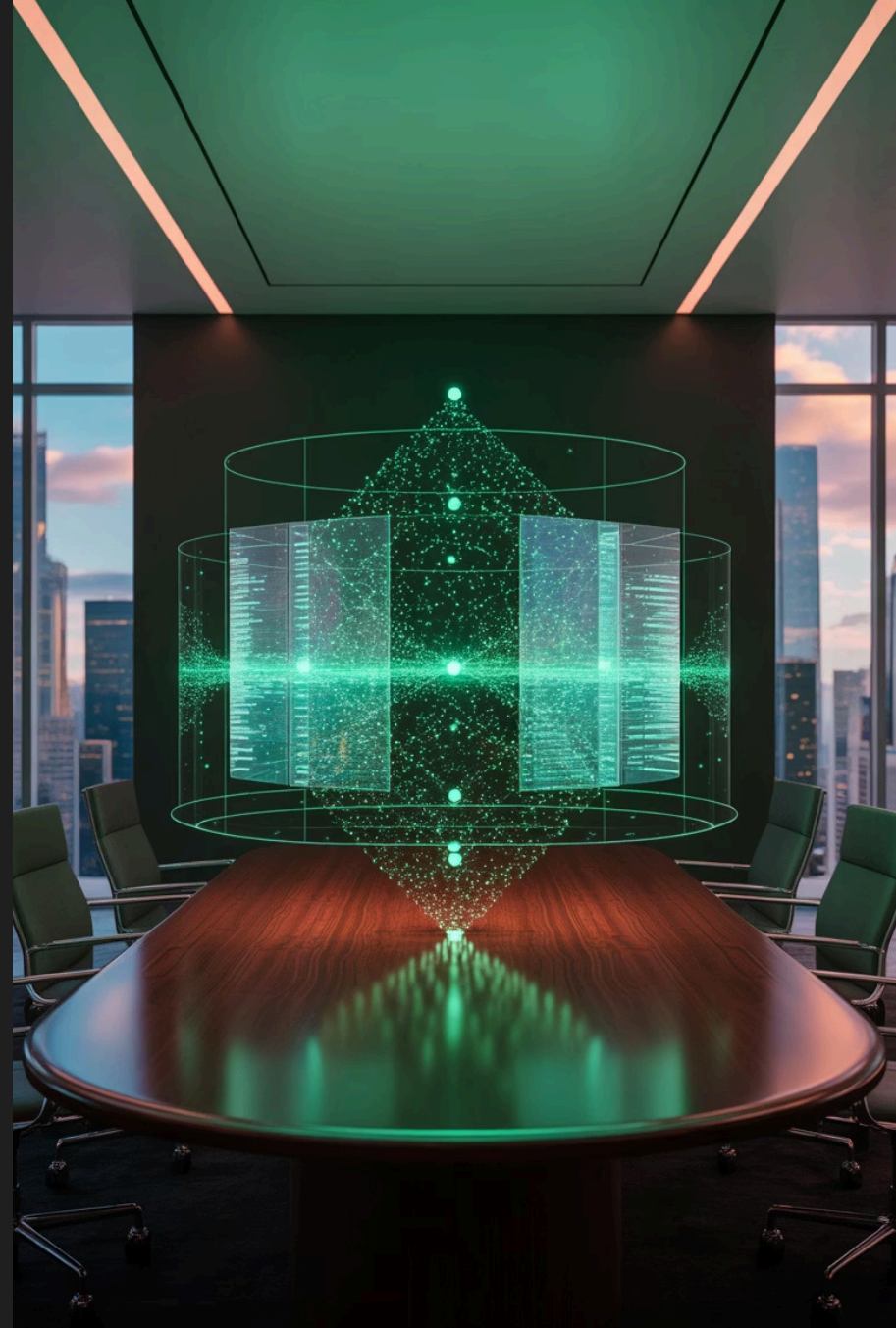
From Blind Spots to Insights: How Observable Identity Systems Transform Security and Performance

Digital transformation has made identity verification systems critical infrastructure for the insurance industry. With identity fraud attempts in financial services rising 30% year-over-year between 2020 and 2023, insurers need robust observability solutions to protect their operations and customers.

This presentation explores how observable cloud-based identity verification systems provide unprecedented visibility into verification workflows through instrumented biometrics, AI-powered analytics, and transparent blockchain implementations.



Shikha Gurjar
Technical Project Manager
Essential Services
Guidewire Software

The Rising Threat Landscape

30%

YoY Increase

Identity fraud attempt growth in financial services (2020-2023)

87%

MTTD Improvement

Reduction in mean time to detection with observable systems

74%

Response Time

Reduction in incident response times

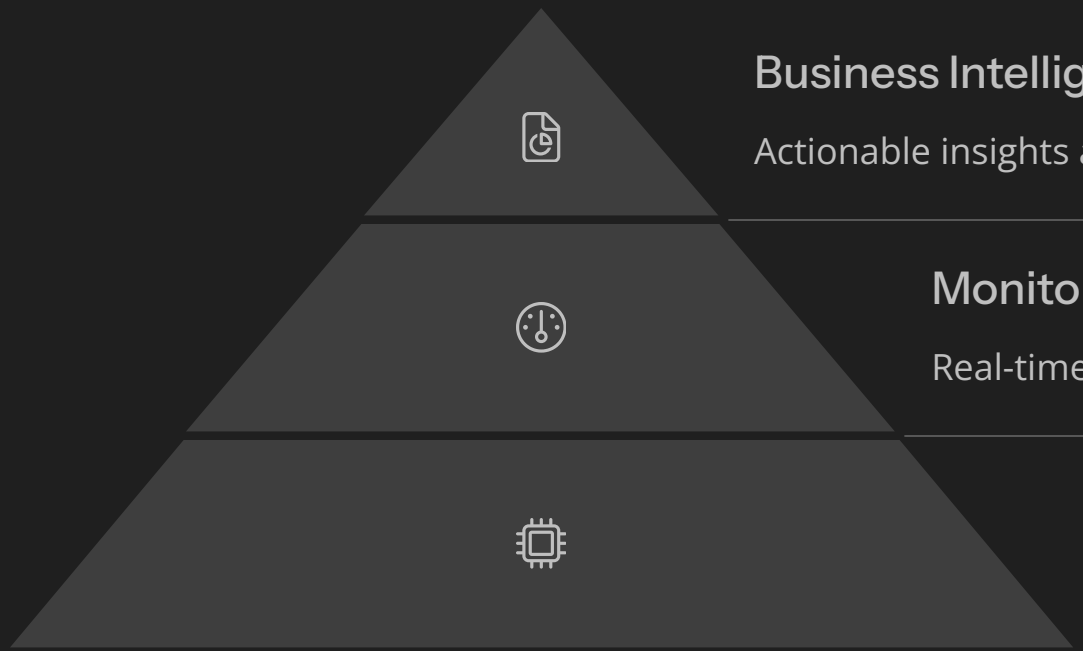
68%

System Resilience

Overall enhancement in system resilience

As digital transactions become the norm in insurance, fraudsters have increasingly targeted identity systems. The dramatic rise in sophisticated attacks requires equally sophisticated detection and response capabilities that traditional security approaches cannot provide.

Components of Observable Identity Systems



Business Intelligence

Actionable insights and metrics

Monitoring & Alerting

Real-time visibility and notifications

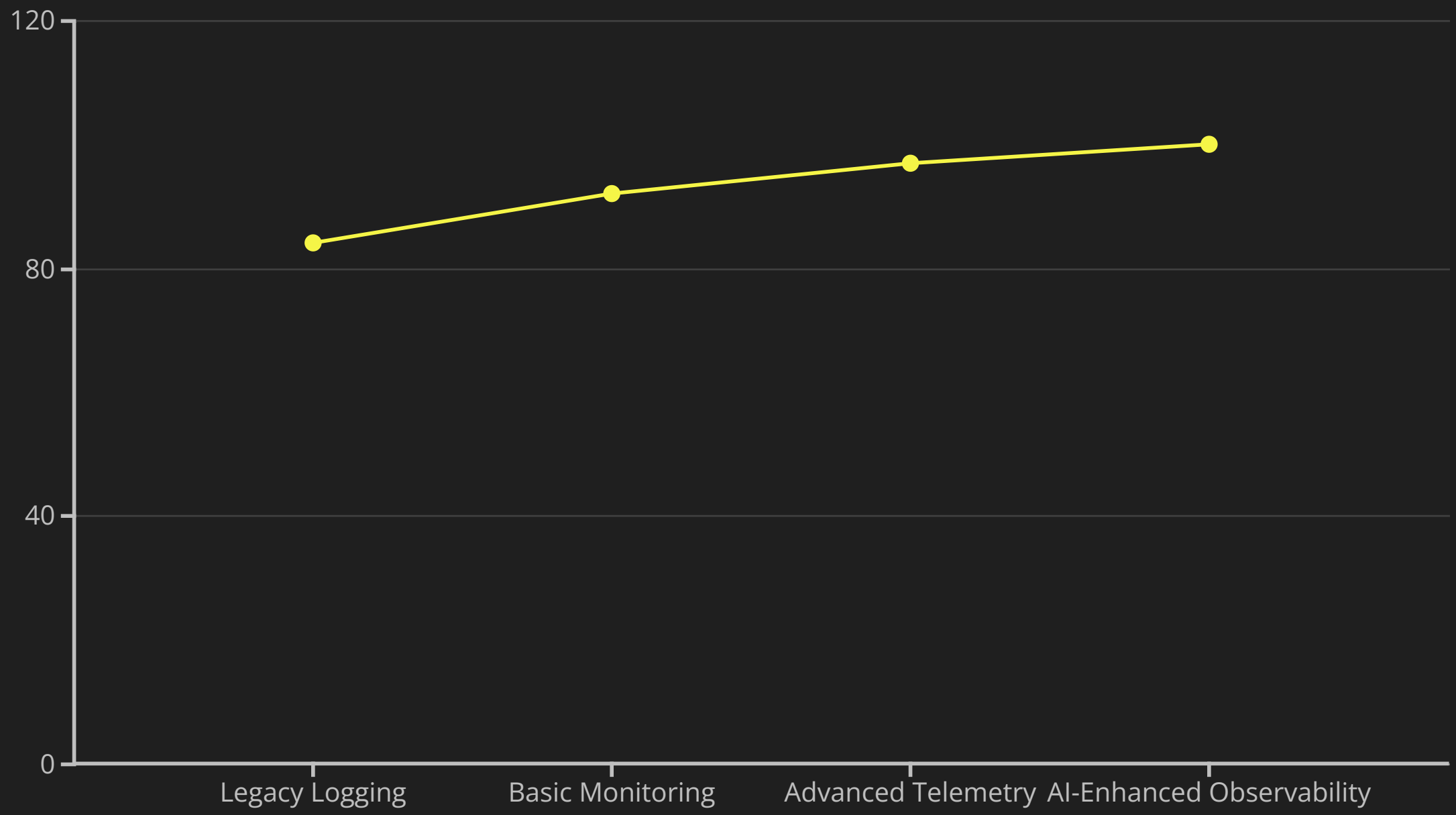
Instrumentation

Biometrics, AI, and blockchain data capture

Observable identity systems are built on a foundation of comprehensive instrumentation that captures critical data points throughout the verification process. This instrumentation feeds sophisticated monitoring and alerting systems that provide real-time visibility into system performance and security events.

At the top level, these systems transform raw data into business intelligence, enabling insurers to make data-driven decisions about security investments, process improvements, and customer experience enhancements.

Breakthrough in Fraud Detection Accuracy



Modern observability approaches have revolutionized fraud detection capabilities. With 99.99% accuracy in near real-time detection of sophisticated spoofing attacks, these systems represent a quantum leap beyond traditional monitoring methods.

AI-based monitoring can identify subtle document fraud patterns by analyzing thousands of data points simultaneously – patterns that would remain completely invisible to traditional logging approaches. This capability is particularly valuable for insurance companies handling high-value transactions where fraud prevention is critical.

Operational Improvements Through Observability

Transaction Tracing

60% reduction in time to trace complex identity verification transactions across microservices, enabling faster troubleshooting and issue resolution.

Capacity Planning

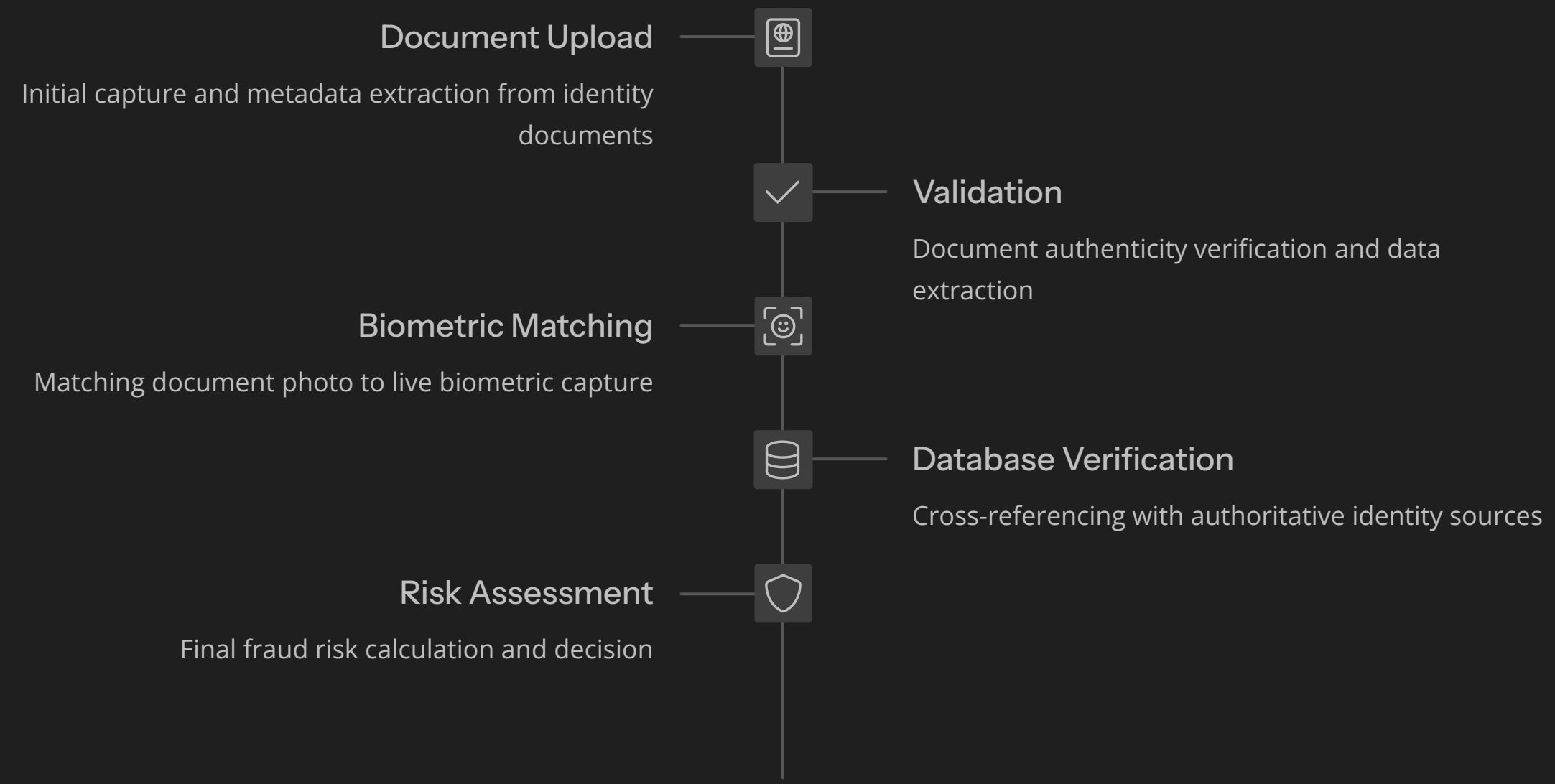
Proactive identification of system bottlenecks and resource requirements, preventing outages during peak verification periods and ensuring smooth customer experiences.

Continuous Improvement

Detailed performance metrics across the verification pipeline, enabling data-driven optimization of each step in the identity verification process.

Beyond security benefits, observable identity systems deliver significant operational advantages. By providing unprecedented visibility into system performance, these tools help operations teams identify and resolve issues before they impact customers.

Distributed Tracing Across Verification Microservices



Modern identity verification systems typically consist of multiple specialized microservices working together. Distributed tracing provides end-to-end visibility into how verification requests flow through these services, identifying bottlenecks and failure points.

Each stage of the verification process generates valuable telemetry data that, when properly correlated, creates a comprehensive view of the customer journey and system performance.

Advanced Correlation Techniques for Identity Events

Collect

Gather raw events from all identity system components

Filter

Remove noise and focus on significant identity signals

Alert

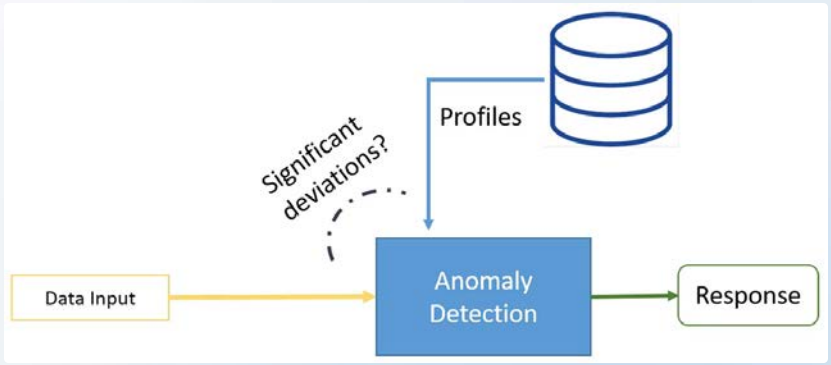
Notify teams of anomalies or security incidents

Correlate

Link related events across the verification pipeline

Effective observability requires sophisticated correlation of events across the identity verification ecosystem. By connecting events from document scanning, biometric verification, and backend database checks, security teams can identify complex attack patterns that would be invisible when viewing components in isolation.

Advanced correlation engines use machine learning to establish baseline behaviors and detect subtle deviations that may indicate fraud attempts or system issues, enabling proactive intervention before problems escalate.



Behavior-Based Anomaly Detection

Establish Behavioral Baselines

Collect typical user interaction patterns with identity verification systems, including typing patterns, device handling, and navigation behaviors.

Apply Machine Learning Models

Train AI systems to recognize normal behavior and identify statistically significant deviations that may indicate fraud or account takeover attempts.

Calculate Risk Scores

Assign dynamic risk scores based on behavioral anomalies, combining multiple signals to reduce false positives while maintaining high detection rates.

Trigger Adaptive Authentication

Implement additional verification steps only when risk thresholds are exceeded, balancing security and user experience.

The future of identity verification lies in behavior-based anomaly detection that looks beyond what users provide and examines how they interact with systems. These approaches can detect sophisticated fraud attempts even when all credentials appear legitimate.

Balancing Monitoring and Privacy

Comprehensive Monitoring Needs

- Detailed transaction data capture
- Biometric verification telemetry
- User behavior analytics
- Cross-system correlation
- Long-term trend analysis

Privacy Considerations

- Data minimization principles
- Anonymization techniques
- Consent management
- Regional compliance requirements
- Data retention policies

Balanced Approach

- Privacy-by-design architecture
- Purposeful data collection
- Tiered access controls
- Transparent data usage
- Regular privacy impact assessments

Implementing observable identity systems requires carefully balancing comprehensive monitoring with privacy protection. While detailed telemetry provides security and operational benefits, it must be collected and managed in ways that respect user privacy and comply with regulations.

Leading organizations are adopting privacy-by-design approaches that incorporate data minimization, purpose limitation, and anonymization techniques while still maintaining robust observability capabilities.

Implementation Roadmap

Assessment

Evaluate current identity systems and observability gaps

Instrumentation

Add telemetry to critical identity verification components

Integration

Connect identity data to observability platforms

Automation

Implement alerts, dashboards and response workflows

Refinement

Continuously improve based on operational feedback

Implementing observable identity systems is a journey that begins with understanding your current capabilities and gaps. Most organizations find success with a phased approach that delivers incremental value while building toward a comprehensive solution.

The implementation process typically takes 6-12 months for enterprise-scale deployments, with early security and operational benefits emerging after just 2-3 months. Cross-functional teams involving security, operations, and development stakeholders achieve the best results.

Key Takeaways and Next Steps

Measurable Benefits

Observable identity systems deliver quantifiable improvements in security detection, operational efficiency, and system resilience.

Holistic Approach

Effective implementations require instrumentation across the entire identity verification lifecycle, from document capture to risk assessment.

Privacy Balance

Success depends on balancing comprehensive monitoring with robust privacy protection through thoughtful system design.

Strategic Journey

Start with high-impact areas, build momentum with quick wins, and develop a long-term roadmap for continuous improvement.

Observable identity systems represent a critical evolution in how insurers protect their digital infrastructure while gaining valuable operational insights. By implementing these approaches, organizations can dramatically reduce fraud risk while improving customer experience through more reliable, efficient verification processes.

Begin your journey by assessing your current identity verification observability, identifying high-priority gaps, and developing a phased implementation plan that delivers incremental benefits while building toward comprehensive coverage.

Thank you