KROLL™

Securing OT Access with Identity and Visibility

Kroll, Saviynt, and Nozomi Networks unite identity governance and OT security to enhance visibility, reduce risk, and build operational resilience.

Identity Lifecycle Management for OT Environments

Challenge Statement

Operational Technology (OT) systems face unique identity and access challenges. They rely on systems such as SCADA (Supervisory Control and Data Acquisition), ICS (Industrial Control Systems), and IIoT (Industrial Internet of Things), all of which must run continuously, making standard IT security tools ineffective. Without clear visibility into who is doing what, there's a higher risk of unauthorized access and system disruptions. Because these environments cannot tolerate system downtime, any security solution must operate in a non-intrusive, agentless manner that does not disrupt critical operations.

Solution Offering

Kroll's offering combines Saviynt's identity platform with Nozomi Networks' OT security tools. This powerful combination gives organizations real-time visibility into who is accessing OT systems and how. By merging Saviynt's identity intelligence with Nozomi's threat detection, teams can quickly spot risks and take action—strengthening access governance and reducing operational threats across critical infrastructure.

Strategic Capabilities Unlocked by the Solution

- **User and Device Inventory:** Centralized inventory of OT device and user account data
- **Activity-Based Risk Detection:** Monitor user activity and generate alerts for suspicious behavior or policy violations
- **Alert Synchronization:** OT security events alerting and response capability
- **Contextual Risk Enrichment:** Enrich alerts with identity attributes (e.g., role, department, location) to improve risk assessment accuracy
- **Actionable Risk Reporting:** Generate comprehensive reports that combine identity context OT activity data for informed decision-making
- **Risk Remediation:** Security administrators can accept risk or revoke access leveraging Saviynt, with automated ticketing via ITSM platform

Business Value

Holistic View: A centralized view of OT users, devices, and security events

Contextualized Alerts: Alerts are enriched with user identity information, reducing noise and improving the accuracy of risk assessment

Informed Decision-Making: Actionable insights empower remediation and risk acceptance

Improved Governance: Strengthens compliance and audit readiness in OT environments

Why Kroll

- **Deep OT Expertise:** Kroll secures industrial systems without disrupting operations, thanks to extensive experience in cyber risk and incident response
- **Holistic, Risk-Driven Approach:** We go beyond tech—delivering solutions grounded in operational resilience and real-world threat intelligence
- **Proven IAM Leadership:** Our track record in Identity and Access Management enables seamless modernization of access controls and governance
- **Trusted Global Partner:** With thousands of incident responses under our belt, Kroll brings unmatched insight to OT-IAM convergence
- **Frameworks:** Supports OT-IT segmentation through Purdue Model adoption
- **Zero Trust:** Applies Zero Trust principles within OT environments to strengthen identity-driven defense
- **Purdue:** Aligns with leading OT security frameworks including IEC 62443 and NIST SP 800-82
- **Downtime Reassurance:** Proven ability to secure ICS environments without downtime, which is a top priority for OT operators

KROLL™ Saviynt

Secure Operational Technology Management Solution

Challenge Statement

- OT environments pose unique access management challenges due to specialized devices, legacy systems, and strict uptime requirements
- Traditional IT security tools lack the necessary context and capabilities to effectively monitor and control access in OT environments

Solution Offering

- Combined data between Saviynt's IGA platform and Nozomi Networks enhanced operational security
- Combine identity governance with OT visibility and threat detection
- Enables access management, activity monitoring, and risk mitigation in OT environments
- Leverages Saviynt's identity context to strengthen OT security posture
- The combined approach is fully agentless and non-intrusive, ensuring no impact on ICS, SCADA, or other critical OT systems

Foundational Visibility and Alerting

Objective:

- **Data Ingestion:** OT device and user account data is imported into Saviynt via flat files to establish identity governance
- **Activity Monitoring:** OT tools monitor user activity and generate alerts for suspicious behavior or policy violations
- **Alert Synchronization:** Saviynt retrieves OT alerts using API integration
- **Enrichment and Analysis:** Alerts are enriched with user attributes (e.g., role, department) from Saviynt to assess risk contextually
- **Risk Reporting:** Generate actionable risk reports combining alert data and identity context
- **Risk Remediation:** Security admins can accept risk or modify access

Business Value

Holistic View: A centralized view of OT users, devices, and security events

Contextualized Alerts: Alerts are enriched with user identity information, reducing noise and improving the accuracy of risk assessment

Manual Control: Provides security administrators with the necessary information to make informed decisions and manually initiate remediation

Operational Excellence: Improves ROI through faster incident response, reduced downtime risk, and streamlined compliance activities

Automation and Enhanced Governance

Objective:

- **Automated Reconciliation:** Ensure Saviynt's identity repository stays current by automatically syncing device and user account data from OT systems
- **Automated Provisioning/Deprovisioning:** Trigger access revocation in OT systems directly from Saviynt, eliminating manual ITSM ticket creation and speeding up remediation

Business Value

Increased Efficiency: Reduces manual effort for security administrators

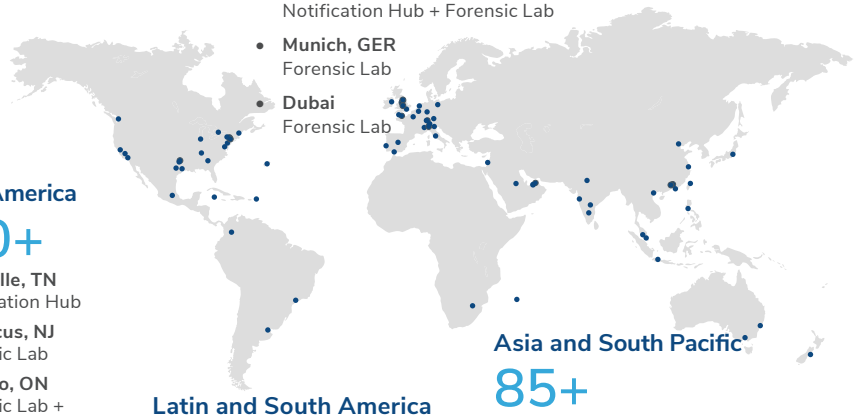
Faster Remediation: Drastically shortens the time to respond to a security incident

Enhanced Security Posture: Automates the enforcement of access policies, reducing the risk of unauthorized access

Expense Optimization: Reduces operational costs by decreasing manual access reviews and reconciliation efforts

Kroll's Market Presence

Global Footprint



Europe, Middle East and Africa
200+

- **London, UK**
  Notification Hub + Forensic Lab
- **Munich, GER**
  Forensic Lab
- **Dubai**
  Forensic Lab

North America
350+

- **Nashville, TN**
  Notification Hub
- **Secaucus, NJ**
  Forensic Lab
- **Toronto, ON**
  Forensic Lab + Notification Hub

Latin and South America
15+

- **Sao Paulo, Brazil**
  Forensic Lab

Asia and South Pacific
85+

- **Melbourne**
  Notification Hub
- **Hong Kong**
  Forensic Lab
- **Singapore**
  Forensic Lab

Key Stats

5,700+
Risk Advisory clients

3,000+
Kroll professionals dedicated to Risk Advisory

1,000+
Cyber incidents handled by Kroll each year and over **100,000+** hours of security testing and assessment

85+
Insurance carriers have Kroll on their panel of incident response vendors

15+
Certified Zscaler practitioners

Our Clients

94%
of Am Law 100 law firm

48%
of Fortune 500 companies

47%
of the S&P 500 companies

ABOUT KROLL

World's largest IR provider with **1000+** IR cases a year

Preferred vendor for **85+** insurance carriers

Experience from **Govt. and Law Enforcement, Industry and Consulting** backgrounds

EUROPOL

700+ experts across 19 countries

100+ certifications

CISM CREST ISO 27001

Expertise in **AI, Crypto, Cloud, Data Analytics, Web 3.0 security and data** risk

700k+ actively monitored endpoints

Rated as **industry leaders**

FORRESTER 2021 Computing Security Awards WINNER

computing Security Excellence Awards 2023 WINNER

SC 2022 awards WINNER

Kroll Key Contacts

Nicole Koopman
Global Head of Commercial Office and Managing Director, Enterprise
+1 2128333258
nicole.koopman@kroll.com

Gaurav Sheth
Global IAM Leader
+1 9733559401
gaurav.sheth@kroll.com

Sameer Koranne
Head of OT Security
+1 7132375317
sameer.koranne@kroll.com

Additional hotlines at:
kroll.com/hotlines

Or via email:
CyberResponse@kroll.com

About Kroll

As the leading independent provider of financial and risk advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.