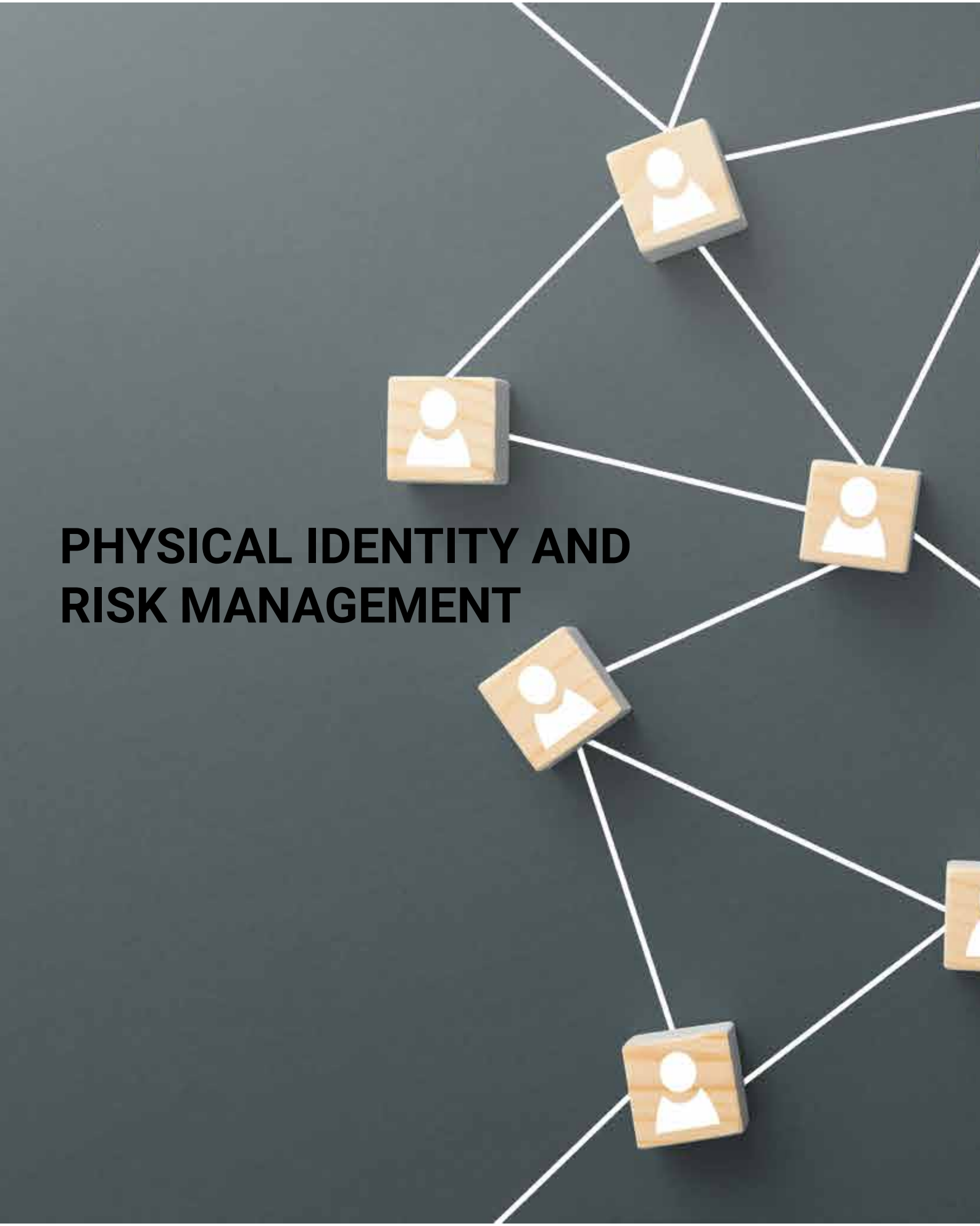
Innominds



PHYSICAL IDENTITY AND RISK MANAGEMENT

THE CHALLENGE

Organizations face increasingly sophisticated securitythreats every day. But despite technological advances, today's threats are strikingly similar to the days of metal keys and locks. The answer still is that assets and keys should be in the right hands to prevent the wrong people from infiltrating secured areas and locks. To combat identity and physical access threats, organizations traditionally spend a lot of resources on reactive monitoring or adding new technologies at vulnerable access points.

However, without a way to predict, analyse or measure the security problem in the first place, this adhoc approach results in inefficient spending, time wasted on false alarms and in detecting access transgressions after they are committed. A strategy to create robust physical security would need to focus on how to detect and prevent security events, rather than on post-facto knee-jerk reactions.

THE SOLUTION

iFusion Risk Analytics enables organizations to leverage their physical security data beyond traditional reporting to predict possible security events. iFusion Risk Analyticscollects your security system logs and using analytics and machine learning, transforms this data into critical knowledge and actionable insights. Your organization can be made aware of potential risks in advance and by applying iFusion Risk Analytics Rules, automatically take preventive actions on a threat — potentially preventing a security catastrophe.

Features

Take advantage of the intelligence provided by iFusion Risk Analytics with a suite of powerful tools:

The iFusion Risk Analytics Dashboard gives a birds-eye view of the potential risks across an organization. It makesit easy for you to rank risks in order of severity, find security vulnerabilities or suspicious behavior associated with specific people/sites/readers, and drill down to the data used to derive these risk scores. In addition, you can easily share, schedule, and customize reports to meet your needs.

iFusion Risk Analytics Rules allow you to automatically act on your findings. Use the intuitive Rule Editor to specify conditions and actions. Automatically suspend access, assign training, send notifications, add people to a watchlist, assign tasks, or trigger area access audits.

The iFusion Risk Analytics Data Analyst Toolbox is an extensive list of data preparation algorithms available for data analysts. Use these tools to develop your own risk metrics, and export results into the iFusion Risk Analytics engine or your own business intelligence tool.

Risk Metrics

iFusion Risk Analytics uses standardized measures called Risk Metrics. Each metric goes beyond basic reporting by analyzing past events to establish baselines for each person/site/reader.

Risk Metrics are divided into two categories:

Attributional Metrics

"What you have." iFusion Risk Analytics compares the assets and privileges held by cardholders to their peers and identifies unnecessary vulnerabilities. Examples of Attributional metrics are:

Unused Badges/Access: Unusually large amounts of active cards/access that sit unused.

Wild Badges: Unusually large numbers of lost/ stolen/unreturned cards.

Excess Badges/Access: Unusually large amounts of active cards/access.

KEY HIGHLIGHTS

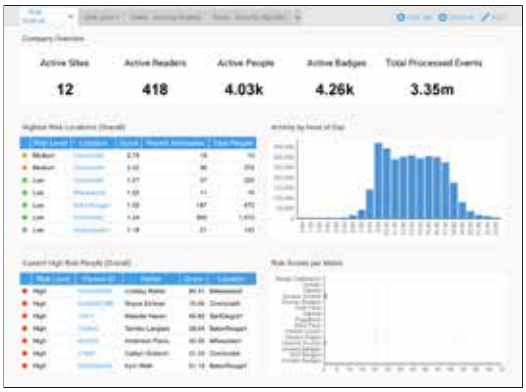
- **ETL (Extract-Transform-Load):** Easily collect data from disparate PACS.
- **Risk Evaluation:** Use pre-built risk metrics to uncover insider threats and security vulnerabilities or build your own using our Data Analyst Toolbox.
- **Dashboards and Reports:** Review results on the Analytics Dashboard or create your own with our full-featured reporting suite.
- **Actions:** Use the Analytics Best Practice Rule Set to automate responses to a host of common security issues or create custom rules with our intuitive rule editor. Revoke access, assign training, send notifications and more.

Behavioral Metrics

"What you do." iFusion Risk Analytics analyzes access control logs to establish baseline patterns of behavior for cardholders, readers, sites and overall. It can then identify anomalies that would indicate elevated risks. Examples of behavioral metrics are:

- **Unusual Ingress/Egress:** Unusual entry times or exit times.
- **Piggybacking:** Also called "tailgating" — entering a space without badging in.
- **Badge Duplication/Sharing:** Seeing a person in two places at once — an indicator that one or more of their credentials is not in their possession.
- **Unseen Doors:** Exploring places you don't normally go.
- **Unusual Denials:** Access denials that are suspicious due to context — a potential indicator of badge fishing.
- **Zombie Badges:** Using an expired/suspended badge.

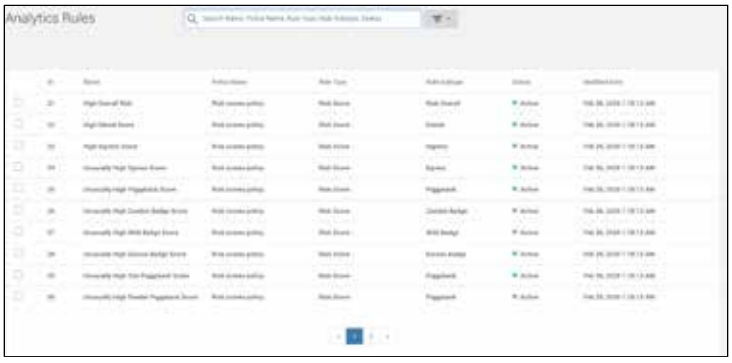
iFusion Risk Analytics goes beyond mere reporting to deliver actionable insights. It allows organizations to clearly assess the current risk levels across their global infrastructure with straight-forward measures of risk for cardholders and locations. In addition, iFusion Risk Analytics can take automatic action to help mitigate those risks.



The advantage of a clear understanding of your organization's operations and risk levels will enable smarter decisions, greater visibility of activities in high risk areas and continuous informed process improvement to streamline operations making your secure workplace more efficient than ever before.

BENEFITS

- Identify high-probability risks while there is still time to act.
- Proactively and automatically take action upon risk discovery.
- Minimize security and compliance risks.
- Analyze behavior across your global infrastructure, regardless of the number of systems involved.



About Innominds

Innominds is an AI-first platform-led digital transformation and full-cycle software product engineering services company headquartered in San Jose, CA. Innominds powers the digital next initiatives of global enterprises and software product companies with an integrated expertise in devices and embedded engineering, software apps and product engineering, cloud, analytics, DevOps, data, security and quality engineering.