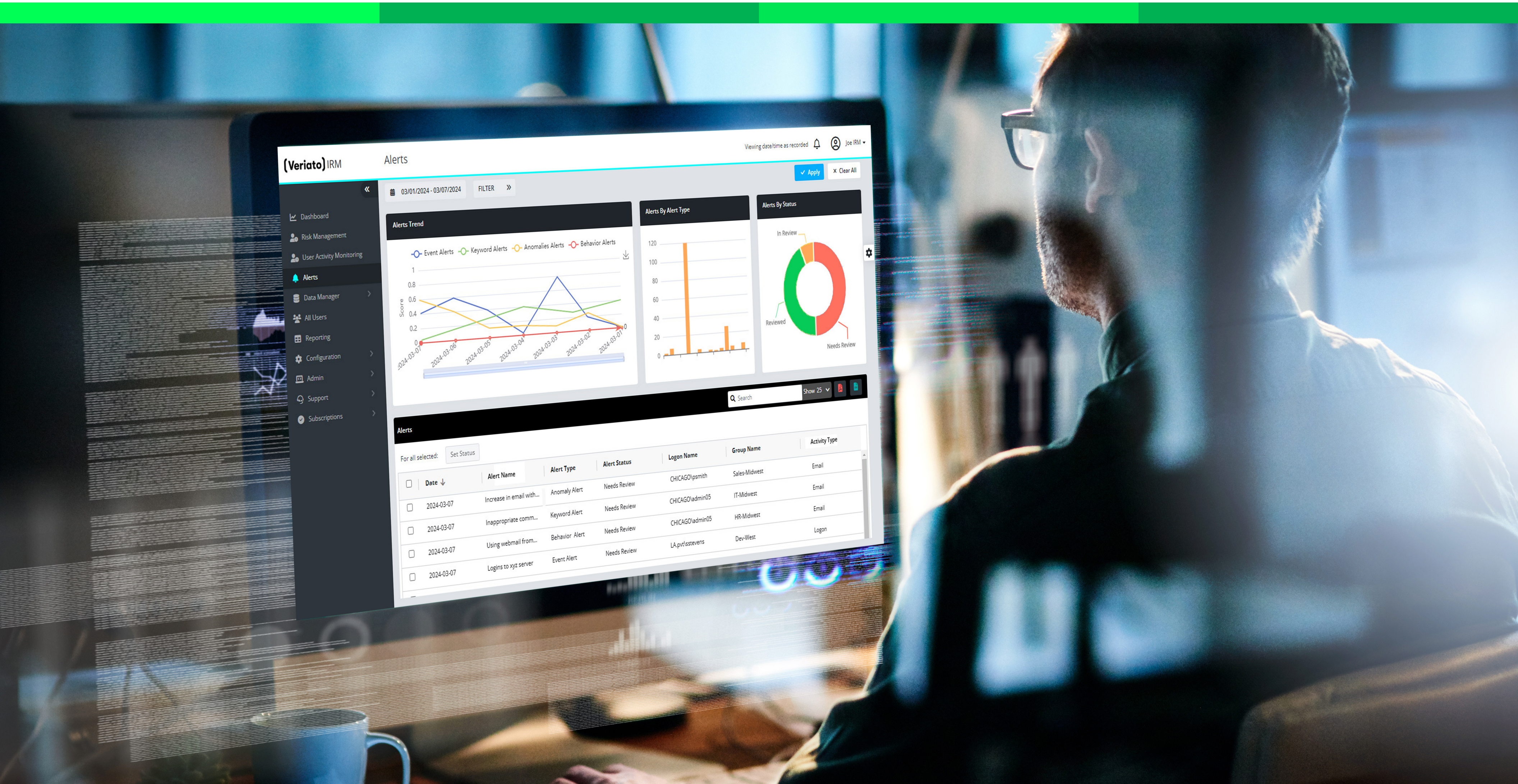
DA FORENSICS
Digital Analysis you can Trust

Veriato Insider Risk Management (IRM)

Next generation insider risk management and threat detection, powered by generative AI.



Alerts

For all selected: Set Status

☐	Date ↓	Alert Name	Alert Type	Alert Status	Logon Name	Group Name	Activity Type
☐	2024-03-07	Increase in email with...	Anomaly Alert	Needs Review	CHICAGO\psmith	Sales-Midwest	Email
☐	2024-03-07	Inappropriate comm...	Keyword Alert	Needs Review	CHICAGO\admin05	IT-Midwest	Email
☐	2024-03-07	Using webmail from...	Behavior Alert	Needs Review	CHICAGO\admin05	HR-Midwest	Email
☐	2024-03-07	Logins to xyz server	Event Alert	Needs Review	LA.pvt\sstevens	Dev-West	Logon

DA FORENSICS
Digital Analysis you can Trust

DA Forensics, Inc.

Digital Forensics you can trust

DA Forensics is a premier private investigations firm based in the Dallas/Fort Worth area, founded by George Rodriguez, a retired federal agent with extensive experience in digital forensics and employee investigations. As a former member of the Office of Professional Responsibility, akin to Internal Affairs, George brings unparalleled expertise in conducting sensitive and high-stakes investigations involving employee misconduct, policy violations, and organizational risks.

At DA Forensics, our team employs the latest techniques, tools, and training to deliver thorough and reliable digital forensic investigations. We specialize in collecting and analyzing evidence to uncover the actual facts of any matter, providing clients with precise and actionable findings. Guided by a commitment to integrity and ethics, we strive to deliver accurate, cost-effective solutions that empower justice through knowledge.

George Rodriguez
Phone: 817-391-1502
Email: GRodriguez@da-forensics.com
Address:
300 Burnett Street Suite 144
Fort Worth, TX 76102
TX License: A10518901

New Kinds of Threats Require a Next-Generation IRM Solution

No comprehensive cyber security posture is complete without an insider risk solution. Today's cyber security landscape has changed dramatically and threats are more numerous and more complex.

82% of data breaches are caused by unsecure or unintentional behaviors of employees (Gartner).

$4.45M is the average cost of a data breach in 2023, an increase of 15% in 3 years (IBM).

85 days is the average time to contain an insider incident (Poneman Institute).

Veriato offers predictive behavior intelligence built with AI to help organizations manage insider risk and monitor employee activity in their remote, hybrid and in-office environments.

Veriato applies the power of Generative AI to detect, identify and predict risky user behaviors based on user activity data, language & sentiment analysis and anomaly detection though pattern matching. Veriato IRM can proactively identify high-risk activity, analyze employee behavior and monitor your intellectual property faster and more accurately than any other solution on the market.

With Veriato IRM, cyber security teams can:

Prevent the most common cause of data breaches and ransomware attacks.

Leverage the power of generative AI to help predict insider risks before they turn into threats.

Go beyond basic activity alerts and access management to truly monitor employee behavior, language and sentiment.

Dramatically cut down response time by continuously capturing user activity and behavior data.

Used and Loved by Thousands of Customers In Over 35 Countries

Gartner
Market Guide
for IRM Solutions

FORRESTER
Insider Risk Solutions
Landscape Report

G2
★★★★⯪

PC PCMAG.COM EDITORS' CHOICE
4.5 Excellent

Capterra
★★★★⯪

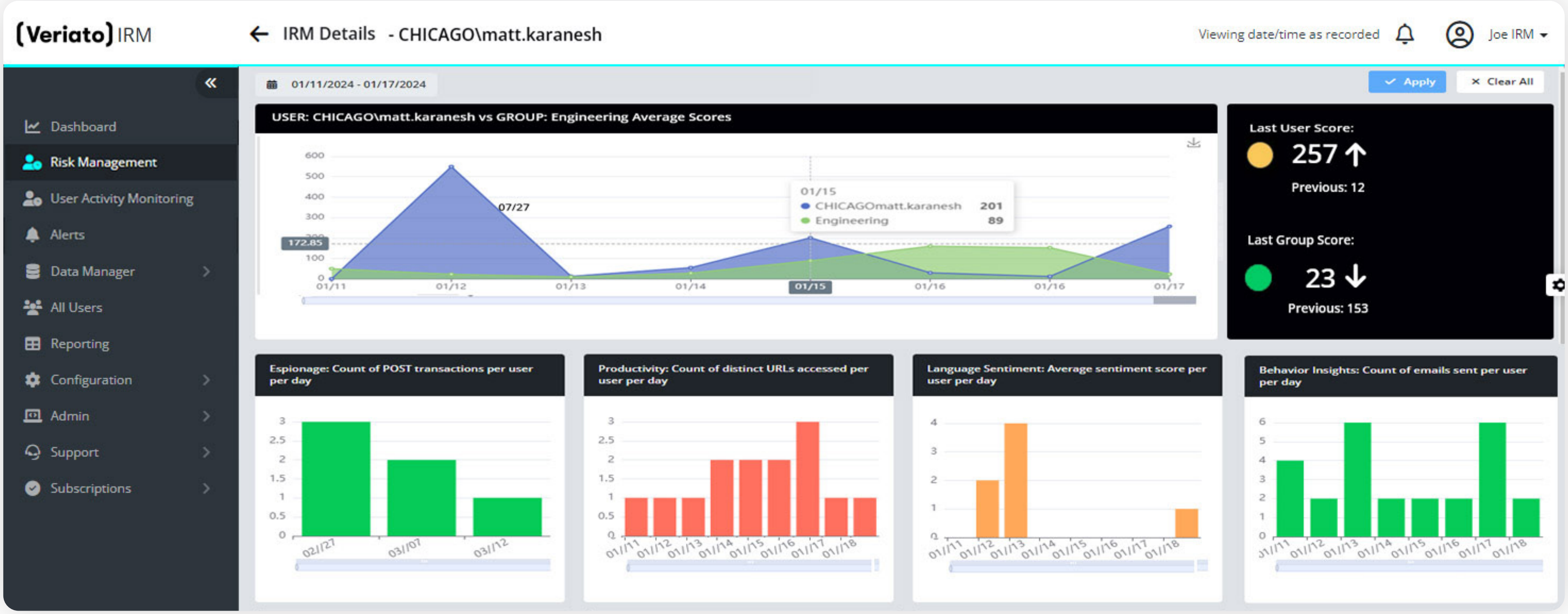
b.
9.16/10

Bring the Power of Generative AI to Your Cyber Security Stack

By integrating the next generation predictive behavior analytics with the power of generative AI, Veriato redefines inside risk management landscape. Our large language models analyze user activity and communication streams to continuously look for signs of potential risk and help predict risks before they turn into threats.

Veriato prioritizes the highest risk signals, reducing alert fatigue and dramatically improving the time it takes to identify and contain a threat. And, our system becomes smarter over time, as our AI learns and adjusts from new data and through reinforcement learning from human feedback (RLHF).

Veriato establishes a behavioral baseline for every individual so that any deviation from typical behavior is immediately identified and analyzed for potential risk. All changes are then ingested and analyzed in near real time, making the model more effective, timely and accurate. Using "human-in-the-loop" design, companies can provide feedback on false positives to provide training data to our AI, improving risk scores and prioritization of alerts.



IRM Details - CHICAGO\matt.karanesh

Viewing date/time as recorded

01/11/2024 - 01/17/2024

USER: CHICAGO\matt.karanesh vs GROUP: Engineering Average Scores

Last User Score: 257 ↑ Previous: 12

Last Group Score: 23 ↓ Previous: 153

Espionage: Count of POST transactions per user per day

Productivity: Count of distinct URLs accessed per user per day

Language Sentiment: Average sentiment score per user per day

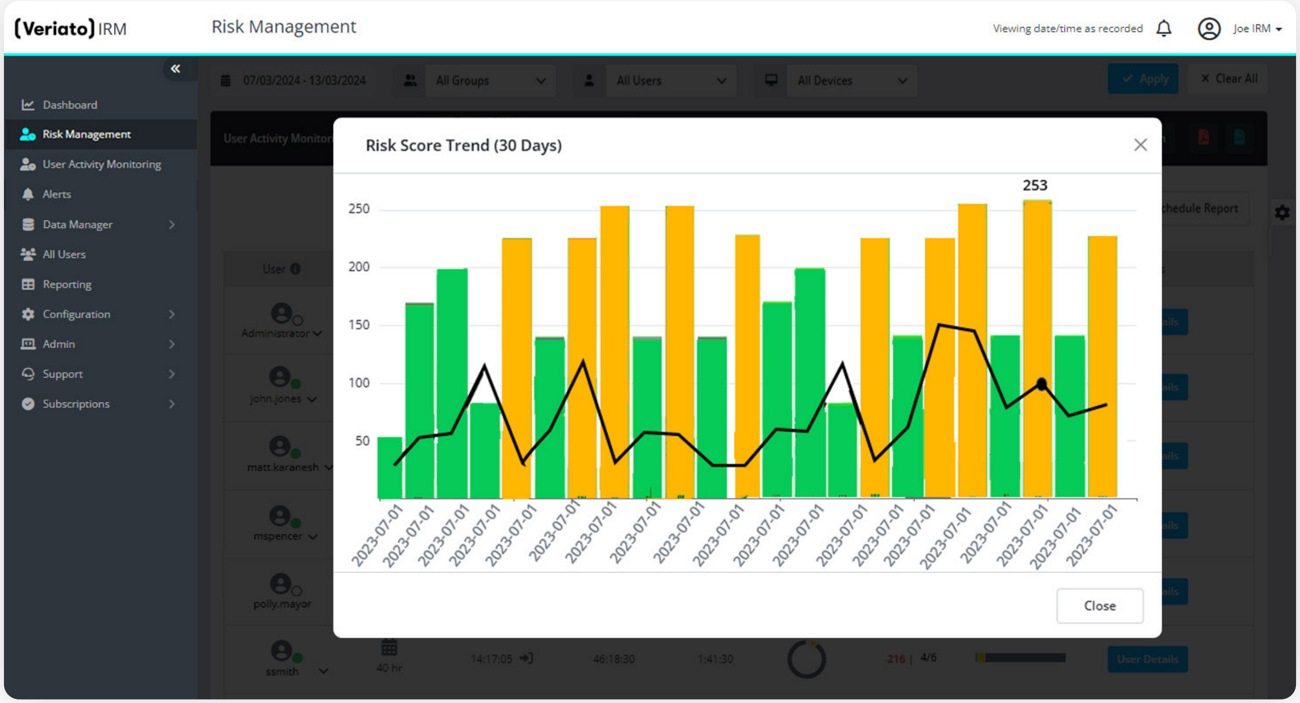
Behavior Insights: Count of emails sent per user per day

AI Risk Scoring

Take action faster and more effectively with risk scoring. Veriato AI assigns risk scores based on thousands of criteria from past behavior and combines this insight with analysis of real time activity across endpoints and channels all at a global scale. Veriato risk analysis is designed to dramatically reduce the number of alerts that otherwise have to be manually monitored, allowing our customers to focus on high risk scores to narrow down the root cause.

Veriato combines the power of AI with predictive behavior analytics capabilities. Prioritization is built-in, so security teams can focus on the most pressing issues.

Veriato's AI makes sense of the influx of alerts, assigning risk scores based on deep analysis to save time and resources and catch issues faster.



Benefits of AI Risk Scoring:

Prioritization: AI analyzes alerts and assigns risk scores to help security teams prioritize quickly and effectively.

Scale and speed: Works at scale to deliver fast and accurate risk score across even the largest global organizations so security teams can act quickly and with confidence.

Deep analysis: Applies rich AI reasoning to alerts across a range of parameters for highly accurate prioritization.

Language Sentiment Analysis

Understand employee activity with depth and precision. Veriato AI uses large language models to read and analyze communications at a massive scale with incredible accuracy.

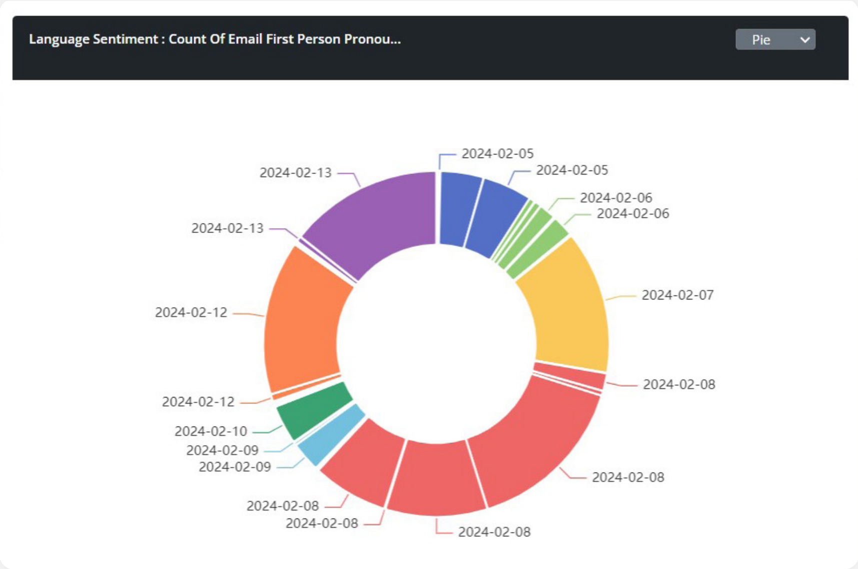
Understand nuanced sentiment, spot potential employee issues and manage compliance with confidence, which is particularly valuable in regulated industries like healthcare and financial services.

Veriato AI analyzes content across emails, texts, messages, documents and more to provide a clear, rich picture of sentiment & activity.

Spot negative sentiment and behavior. Identify potential insider risk issues from disgruntled employees.

Identify inappropriate communication. Uncover conversations between employees & competitors, illegal or fraudulent activity or nuances such as harassment.

Spot compliance breaches. Identify misuses of data and PII and uncover out-of-compliance activity.



Automatic PII/PHI Identification

Veriato leverages GenAI capabilities to perform a deep analysis of data. Using pretrained large language model, Veriato recognizes if any sensitive data is shared, triggering scored alerts. In addition, to preserve privacy concerns, Veriato redacts such sensitive information prior to storing.

AI analysis flags sensitive data.

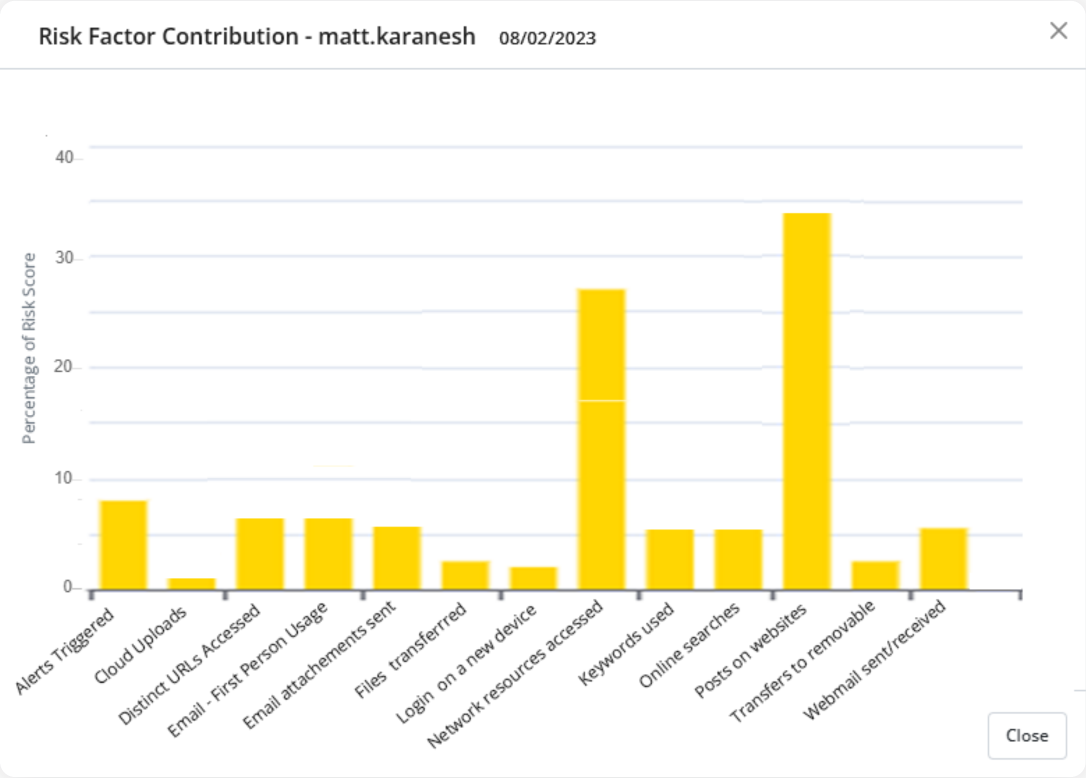
Risk scores and alerts help teams prioritize issues quickly.

Sensitive data can be quickly redacted to remove future risk.

Monitor, Capture & Analyze User Activity Across the Entire Organization

Veriato IRM combines the power of an AI-based insider risk management solution with robust user activity monitoring (UAM) capabilities.

Veriato continuously collects endpoint data across more than 60 activities, including email, chat, application use, web browsing history and much more. Activity signals are then combined with behavioral and sentiment analysis to generate risk scores and help predict potential threats.


Risk Factor Contribution - matt.karanesh 08/02/2023

Email & Chat Monitoring

Capture communications activity in traditional email platforms as well as many popular chat and messaging applications.

Web & Application Use

Categorize websites and applications. Track websites visited, searches conducted and applications used for each user. Block specific applications and websites.

File & Document Tracking

Track activities on local, removable, and cloud storage, as well as print operations. See when files are created, edited, deleted, or renamed.

Keystroke Logging

Record every keystroke, including "hidden" characters and combinations and trigger real-time alerts based on specific keywords.

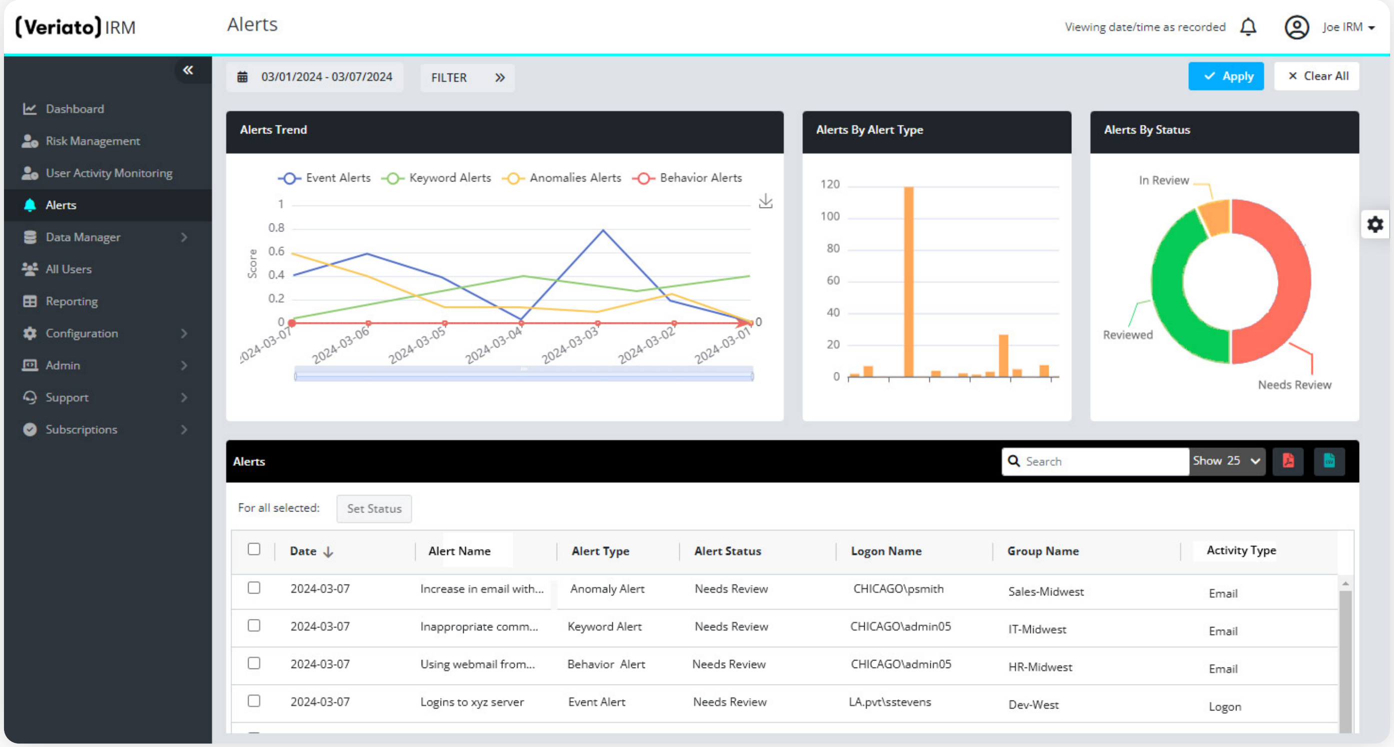
Screenshots

Capture and play back screenshots as a continuous stream or set up activity or keyword triggers.

Generate Accurate Real-Time Alerts & Investigate Potential Threats with Ease

Real-Time Alerts

Veriato offers powerful real-time alert capabilities that are designed to be highly customizable while also avoiding alert fatigue. Customize frequency, triggers/conditions and even sensitivity for each alert. Select from typical event or keyword alerts or set up AI-powered anomaly and behavioral triggers.



☐	Date ↓	Alert Name	Alert Type	Alert Status	Logon Name	Group Name	Activity Type
☐	2024-03-07	Increase in email with...	Anomaly Alert	Needs Review	CHICAGO\psmith	Sales-Midwest	Email
☐	2024-03-07	Inappropriate comm...	Keyword Alert	Needs Review	CHICAGO\admin05	IT-Midwest	Email
☐	2024-03-07	Using webmail from...	Behavior Alert	Needs Review	CHICAGO\admin05	HR-Midwest	Email
☐	2024-03-07	Logins to xyz server	Event Alert	Needs Review	LA.pvt\sstevens	Dev-West	Logon

Anomaly Alerts

Receive a notification when anomalous activity is detected. Compare to user's own past activity, the group, changes in their risk score or behavior associated with possible compromised credentials.

Event Alerts

Trigger an alert based on specific activity, like an attachment being sent via a person email or a website being visited by a user.

Keyword Alerts

Easily set up alert words or keywords to trigger real-time notifications, automated reports or even screenshots. Organize your alert words into categories.

Behavioral Alerts

Leverage generative AI language and sentiment analysis to trigger alerts based on tone, language sentiment and other behavior.

Reports

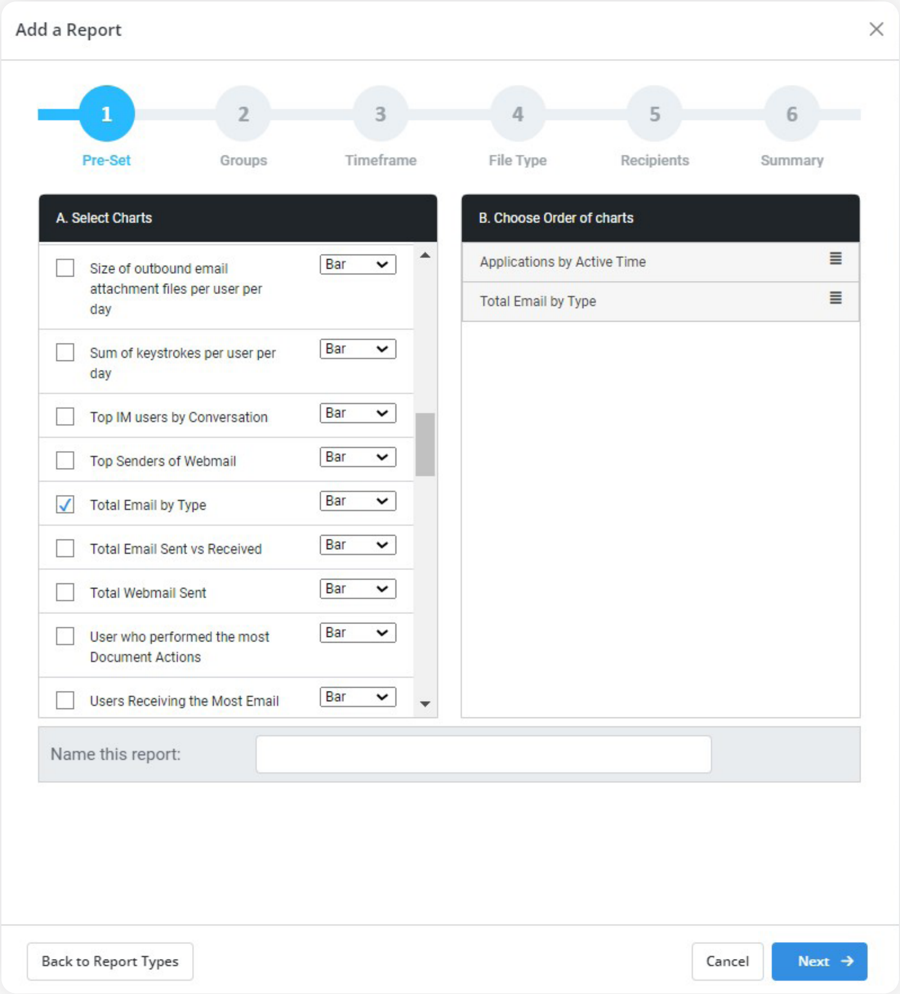
Veriato IRM reporting offers organizations unprecedented visibility into their employee's behavior and activities. Generate comprehensive reports on everything from disengagement signals to anomalies and toxic language. Identifying potential risks or investigating threats has never been easier.

Select from 100s of charts and prebuilt templates.

Automatically deliver your report by email at the frequency and to the recipients you specify.

Trigger automatic reports based on keywords, activities or AI-identified behavioral conditions.

Export data for further analysis or to upload into another platform or dashboard.



A. Select Charts

- □ Size of outbound email attachment files per user per day — Bar
- □ Sum of keystrokes per user per day — Bar
- □ Top IM users by Conversation — Bar
- □ Top Senders of Webmail — Bar
- ☑ Total Email by Type — Bar
- □ Total Email Sent vs Received — Bar
- □ Total Webmail Sent — Bar
- □ User who performed the most Document Actions — Bar
- □ Users Receiving the Most Email — Bar

B. Choose Order of charts

- Applications by Active Time
- Total Email by Type

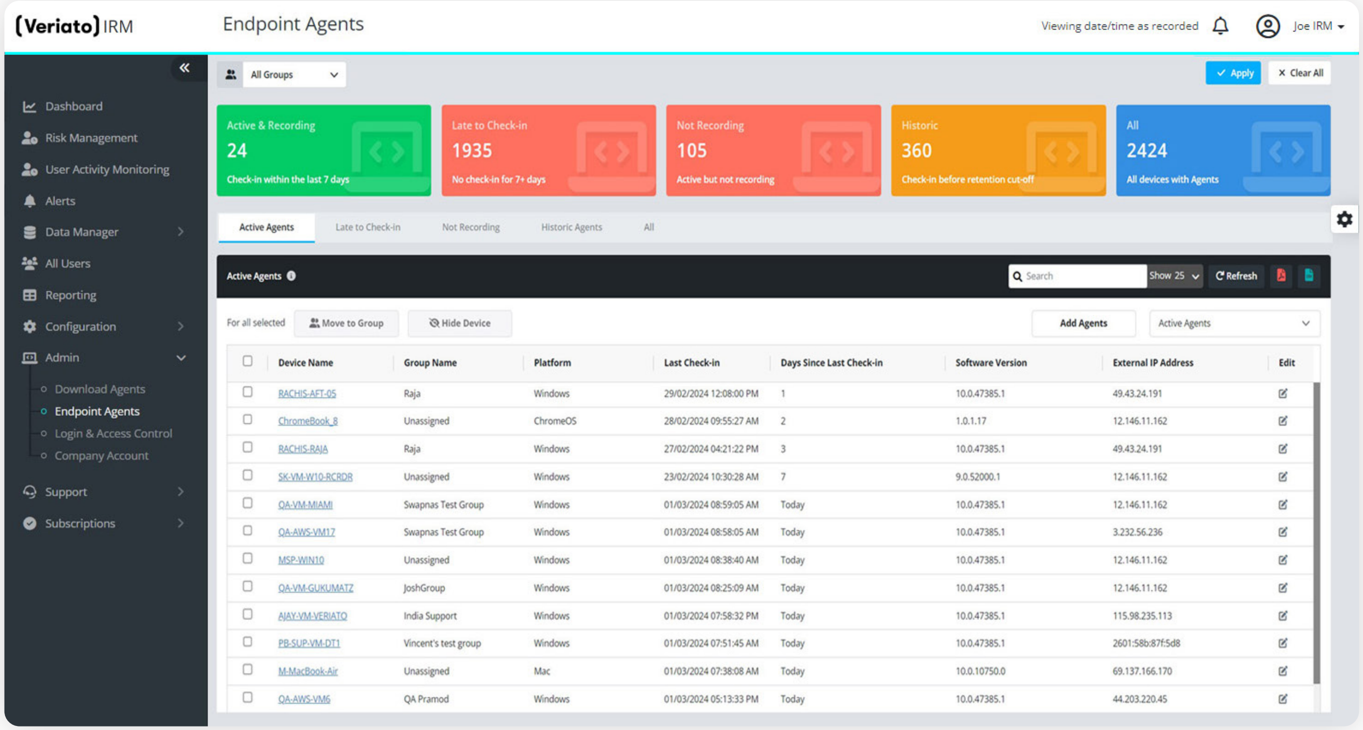
Name this report:

Designed to Fit Any Organization

Deployment

Veriato is designed from the ground up to work with any organization from enterprise to small business and to be flexible with your existing environment.

Easy to implement, integrate and use. Veriato is built to work in the cloud, on-premise or in a hybrid configuration. No need to purchase new hardware, Veriato works with what you have, to be up and running quickly and at a lower cost.



□	Device Name	Group Name	Platform	Last Check-in	Days Since Last Check-in	Software Version	External IP Address	Edit
□	RACHIS-AFT-05	Raja	Windows	29/02/2024 12:08:00 PM	1	10.0.47385.1	49.43.24.191	✎
□	ChromeBook_8	Unassigned	ChromeOS	28/02/2024 09:55:27 AM	2	1.0.1.17	12.146.11.162	✎
□	RACHIS-RAJA	Raja	Windows	27/02/2024 04:21:22 PM	3	10.0.47385.1	49.43.24.191	✎
□	SK-VM-W10-RCRDR	Unassigned	Windows	23/02/2024 10:30:28 AM	7	9.0.52000.1	12.146.11.162	✎
□	QA-VM-MIAMI	Swapnas Test Group	Windows	01/03/2024 08:59:05 AM	Today	10.0.47385.1	12.146.11.162	✎
□	QA-AWS-VM17	Swapnas Test Group	Windows	01/03/2024 08:58:05 AM	Today	10.0.47385.1	3.232.56.236	✎
□	MSP-WIN10	Unassigned	Windows	01/03/2024 08:38:40 AM	Today	10.0.47385.1	12.146.11.162	✎
□	QA-VM-GUKUMATZ	JoshGroup	Windows	01/03/2024 08:25:09 AM	Today	10.0.47385.1	12.146.11.162	✎
□	AJAY-VM-VERIATO	India Support	Windows	01/03/2024 07:58:32 PM	Today	10.0.47385.1	115.98.235.113	✎
□	PB-SUP-VM-DT1	Vincent's test group	Windows	01/03/2024 07:51:45 AM	Today	10.0.47385.1	2601:58b:87f:5d8	✎
□	M-MacBook-Air	Unassigned	Mac	01/03/2024 07:38:08 AM	Today	10.0.10750.0	69.137.166.170	✎
□	QA-AWS-VM6	QA Pramod	Windows	01/03/2024 05:13:33 PM	Today	10.0.47385.1	44.203.220.45	✎

Built for flexibility

Designed to work for organizations of any size from large enterprises to small teams.

Scale without performance impact

Can monitor tens of thousands of endpoints with little to no performance impact.

Flexible architecture

Choose from cloud, hybrid or on-premise deployment options.

Configurable on-premise options (BYODB & BYOS)

On-premise or private cloud customers can bring their own Database or own server – Linux or Windows.

Data centric architecture

Allows for advancement of AI-based features in upcoming releases including language analysis using generative AI.

Recording & Scoring

With Veriato, organizations have complete freedom to set up our solutions to fit their business requirements, company policies and regulatory requirements.

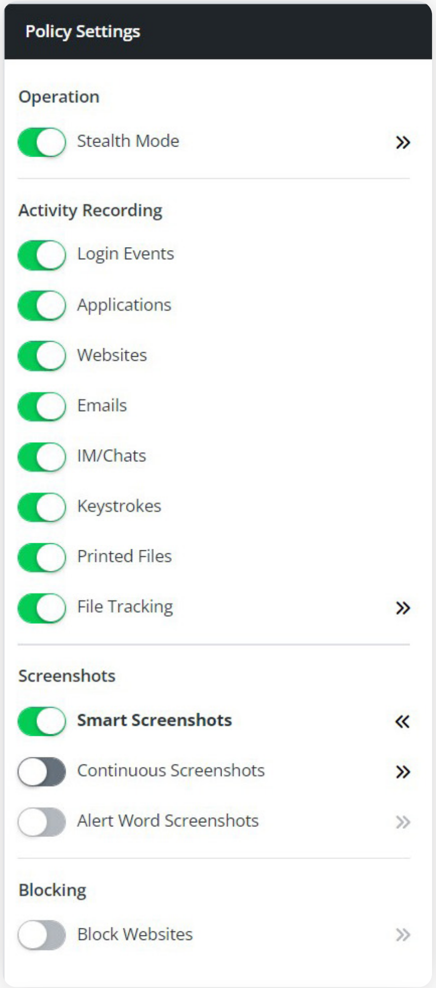
Decide which data is captured for each team, department or across the entire organization.

Configure rules for capturing PII/PHI and other sensitive data.

Determine how and where the data is stored to meet GDPR and similar regulatory requirements.

Customize risk thresholds to fit established metrics and existing company policies.

Identify risky websites, applications and specify business-critical files.



Policy Settings

Operation

- ● Stealth Mode »

Activity Recording

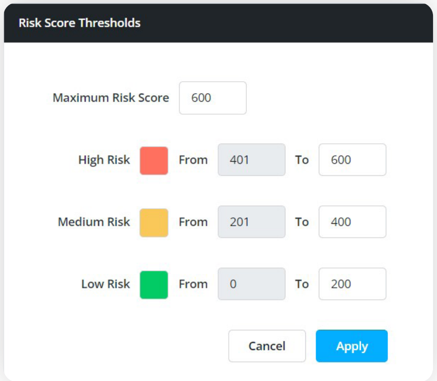
- ● Login Events
- ● Applications
- ● Websites
- ● Emails
- ● IM/Chats
- ● Keystrokes
- ● Printed Files
- ● File Tracking »

Screenshots

- ● **Smart Screenshots** «
- ○ Continuous Screenshots »
- ○ Alert Word Screenshots »

Blocking

- ○ Block Websites »



Risk Score Thresholds

Maximum Risk Score 600

High Risk	🟥	From	401	To	600
Medium Risk	🟨	From	201	To	400
Low Risk	🟩	From	0	To	200

Cancel Apply

DA FORENSICS
Digital Analysis you can Trust

With DA Forensics' monitoring and expert investigative services powered by Veriato's cutting-edge software, organizations gain unparalleled visibility into insider threats, productivity trends, and data security risks across remote, hybrid, and in-office environments. Veriato's AI-driven platform provides proactive solutions for Insider Risk Management (IRM), User Activity Monitoring (UAM), and Data Loss Prevention (DLP), delivering real-time monitoring, alerts, detailed reporting, and actionable insights. Through DA Forensics' expertise, companies can leverage this advanced technology to predict and prevent risks, ensure operational efficiency, and maintain a secure, productive workplace environment.

Sales: 817-391-1502