Product Brief

Imperva Data Risk Analytics

Detect data threats before they become security incidents or breaches

thalestct.com

THALES
Building a future we can all trust

Protecting sensitive data is hard for enterprise security groups with limited resources and tools. Often it is the group's tools themselves that make data breach detection so difficult. Tools that cannot properly contextualize alerts overwhelm security staff with an avalanche of mostly "false positives", making it very hard to know what to do or even where to begin.

Organizations need advanced data risk analytics to eliminate all the noise and help security staff gain actionable threat insights to accelerate risk mitigation and breach detection.

Reduce false positives through data context

Imperva Data Risk Analytics, a key capability of Imperva Data Security Fabric (DSF), helps identify data breach threats without all the noise. Typical User and Entity Behavior Analytics (UEBA) tools just focus on network or system access anomalies such as login and logout. Data Risk Analytics takes into account what data users access, the user's roles, whether the data is sensitive or not, and what the user does with it. By correlating all of this event information, Data Risk Analytics contextually determines if an activity is simply an anomaly without risk, or an actual serious threat to sensitive data before generating an alert. This filters out false positives and enables teams to act only on higher-risk incidents that should be further investigated.

Highlights

Reduce false positives and prioritize what matters most

Gain actionable insights that make staff more efficient and effective

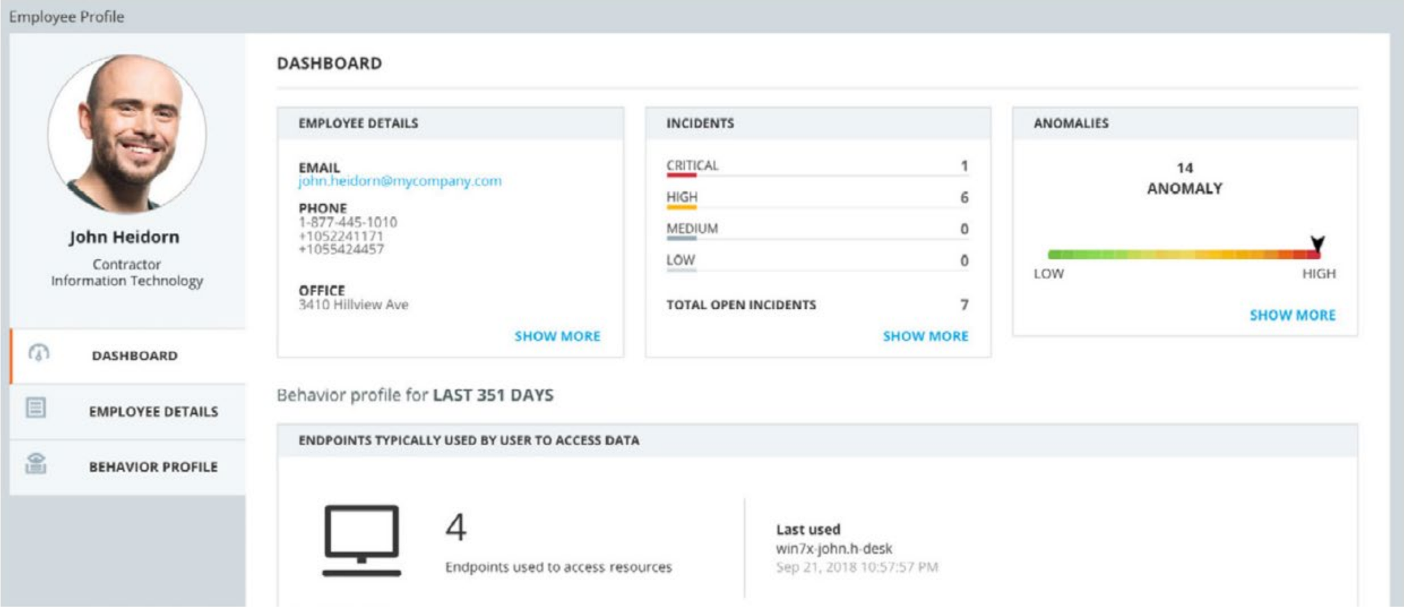
Detect complex or evasive behavior that indicate threats such as privilege abuse or compromised accounts

Achieve Fast Time to Value from features that work right out of the box

Actionable insights make staff more effective

Investigating data threats through the information that a typical UEBA solution (such as a SIEM) provides often requires pre-knowledge of the accessed data set, or deep knowledge of data access languages like Structured Query Language (SQL), to know if any sensitive data has been misused or if users are accessing data inappropriately.

Imperva Data Risk Analytics takes data sensitivity into account and translates all of this complex data access information into plain language that any security staff member can understand even if they don't have data set or language knowledge. An intuitive dashboard provides a prioritized incident summary. From there, you can click-through to detailed incident reports providing a full description of the threat in clear language, so you know what you need to do.



John Heidorn
Contractor
Information Technology

DASHBOARD

EMPLOYEE DETAILS

EMAIL
john.heidorn@mycompany.com

PHONE
1-877-445-1010
+1052241171
+1055424457

OFFICE
3410 Hillview Ave

INCIDENTS	
CRITICAL	1
HIGH	6
MEDIUM	0
LOW	0
TOTAL OPEN INCIDENTS	7

ANOMALIES

14
ANOMALY

Behavior profile for **LAST 351 DAYS**

ENDPOINTS TYPICALLY USED BY USER TO ACCESS DATA

4
Endpoints used to access resources

Last used
win7x-john.h-desk
Sep 21, 2018 10:57:57 PM

Figure 1: The dashboard provides visibility security teams need to investigate data breach threats.

Unravel complex threat behavior and prioritize what matters most

Imperva Data Risk Analytics uses unique, purpose-built data threat detection techniques proven to identify data-centric threats many security tools miss. For example, one of the many techniques looks for activity such as a user abusing a service account to access data, a potential sign the account is compromised or someone is trying to conceal their identity for malicious intent.

Data Risk Analytics prioritizes critical incidents by applying grouping and scoring algorithms that factor in variables such as sensitive data type, privileged account, amount of data involved and more. If multiple incidents are related (e.g. they are all associated with the same user account or multiple users are abusing the same service account), they will be grouped into one issue. Security staff are prominently shown the high-risk incidents, and false positive noise is suppressed.

Active Attack Detection

During an attack, minutes count, and that's why Imperva Data Risk Analytics includes a capability called Active Attack Detection. Using Imperva Labs analysis of exploits observed in large numbers of breaches, Imperva Data Risk Analytics recognizes known attack exploit behaviors and immediately triggers a critical alert to notify the security team. The types of exploits recognized include:

- Malware deployment, including ransomware
- Audit tampering
- Credentials extraction
- Privilege escalation
- Database weaponization
- Data exfiltration

Enterprise coverage, speed, and scale

To mitigate the risk of data breaches enterprise-wide, you need to be able to detect threats across all your sensitive data repositories on-premises, in the cloud, or across multiple clouds. Human beings just can't do it at the speed and scale required. Imperva Data Risk Analytics seamlessly leverages the reach of Imperva Data Security Fabric (DSF) to access data everywhere. Through automation and machine learning, Imperva Data Risk Analytics uncovers suspicious data access and risky behavior across millions and even billions of data access events that happen across potentially thousands of databases every day in a large, data-driven organization. Over time, the analytics engine continuously learns the details of who the users are, what they typically access, and how they typically use the data, using this contextual behavior baseline to constantly fine tune its accuracy.

Fast Time to Value

Data Risk Analytics is a key component of Imperva Data Security Fabric. It helps security teams detect and pinpoint critical threats to data, prioritizes what matters most, and provides actionable insights allowing you to accelerate threat investigation and response - even if you don't know much about the data - and don't know database languages.

Imperva Data Risk Analytics does not require you to create policies before it can recognize non-compliant or risky behavior. Purpose-built threat recognition intelligence comes right out of the box, so you can start seeing the benefits and changes in days, not months. Then it continuously tunes and adapts to changing circumstances. Imperva Data Risk Analytics helps you spot and mitigate data breach risks before they become damaging incidents.

Imperva Data Risk Analytics is part of a holistic Imperva Data Security Fabric solution for all enterprise data assets across on-premises, cloud, hybrid and multi-cloud enterprise environments.

Imperva Data Risk Analytics is available to the U.S. Federal Government through Thales Trusted Cyber Technologies.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com