Next-Generation Database Activity Monitoring

Agentless, Cloud-Native, Unified

Database security challenges have fundamentally changed

Databases contain an organization's most valuable assets—customer records, financial data, intellectual property, operational insights, and more. Legacy database security solutions have made it hard to protect these critical assets, leaving organizations vulnerable despite years of deployment efforts and millions in investment.

Over the past two decades, the database security challenges have evolved dramatically. Instead of only securing on-premises databases from a handful of vendors, organizations must now protect hundreds of databases across cloud and hybrid environments, accessed by thousands of users, applications, and AI systems.

Legacy solutions that already struggled to secure databases now fail completely when faced with new kinds of databases and emerging use cases, including the proliferation of APIs, increasing attack sophistication, and the emergence of AI agents.

Securing databases requires a new approach that can scale to meet the demands of modern database security and integrate seamlessly into an end-to-end approach to data security.

Exponential growth in attack surface

Cloud migration: As databases move from secure on-premises environments to cloud platforms with internet-facing endpoints, the attack surface grows significantly. This shift extends beyond the traditional perimeter and requires security teams to protect a broader range of services.

API proliferation: Every database now connects to multiple APIs, microservices, and third-party integrations, creating more paths for attack.

User expansion: Database access expanded from DBAs and analyst to data scientists, contractors, thousands of users, applications, and AI systems.

Attacker sophistication: Attackers evolved from opportunists to organized criminal enterprises with sophisticated tools and economic incentives to target data stored in databases.

Heightened regulatory and financial consequences: Data breaches and data vulnerabilities now carry severe financial penalties due to regulations like GDPR, CCPA, SOC, and others.

Dynamic and unpredictable access patterns: Modern applications, analytics tools, and AI agents don’t follow predetermined access patterns. They can construct complex queries across multiple tables and databases in real time, making traditional role-based access controls obsolete.

Why legacy DAM solutions fall short

For over two decades, legacy Database Activity Monitoring (DAM) vendors like Imperva and Guardium have promised comprehensive security for sensitive data. Despite billions in investment and years of deployment efforts by thousands of organizations, legacy DAM solutions have failed to secure sensitive data across on-premises and cloud environments.

Legacy DAMs are built on outdated agent-based architectures that take years to deploy and require dedicated full-time resources to operate. Even when successfully deployed, legacy DAM solutions can, at best, help organizations pass regulatory audits—they deliver minimal security outcomes.

Long deployment cycles and high operational overhead

Legacy DAM solutions require installing agents on each database server. Since databases must be offline during agent installation and upgrades, any deployment work can only be done during maintenance windows (usually once a month). This results in long deployment cycles. Because of the complexity and time required to install each agent one by one, most companies only monitor the databases they absolutely must monitor to comply with regulations—creating security gaps.

Limited scalability and performance impact

Legacy DAM agents consume CPU, memory, and disk IO resources. The resource consumption impacts database performance, particularly under high-load conditions. This creates a tension between security monitoring and operational efficiency, often resulting in reduced monitoring capabilities or selective deployment that, once again, creates security gaps.

Reactive rather than proactive protection

Legacy DAM solutions focus on detection and alerting rather than prevention. They excel at generating logs and alerts but offer limited capabilities for real-time policy enforcement and automated remediation. In an era where AI agents can extract and process data in an instant, reactive approaches are insufficient.

Varonis Next-Gen DAM

Varonis Next-Gen DAM overcomes the architectural limitations of legacy DAM to scale database security with minimal overhead. Varonis Next-Gen DAM is agentless, deploys quickly, and requires near-zero operational overhead. And as part of the Varonis Data Security Platform, Varonis Next-Gen DAM integrates into an end-to-end approach to data security, enabling organizations to continuously reduce their sensitive data exposure and respond to threats automatically.

- **SaaS deployment:** Varonis Next-Gen DAM is delivered as a cloud service, eliminating the need for on-premises or VM infrastructure, software installation, and ongoing maintenance. Organizations can secure databases within days or weeks rather than years.

- **Agentless monitoring:** Rather than deploying agents on every database server, Varonis uses Gatekeeper, a stateless database proxy architecture that deploys and scales fast and does not impact database performance. This approach has no impact on database performance, removes operational overhead, and shortens deployment cycles.

- **Zero-downtime updates:** Varonis DAM updates are delivered transparently without impacting database performance or requiring maintenance windows. Security policies and detection algorithms are continuously updated without user intervention.

- **Comprehensive data coverage:** While legacy DAM solutions can only work with on-premises databases, Varonis Next-Gen DAM intercepts communications at the network level and as a result, works with all database types – on-premises, cloud, managed, and unmanaged, as well as with any client application, query tool, or access method.

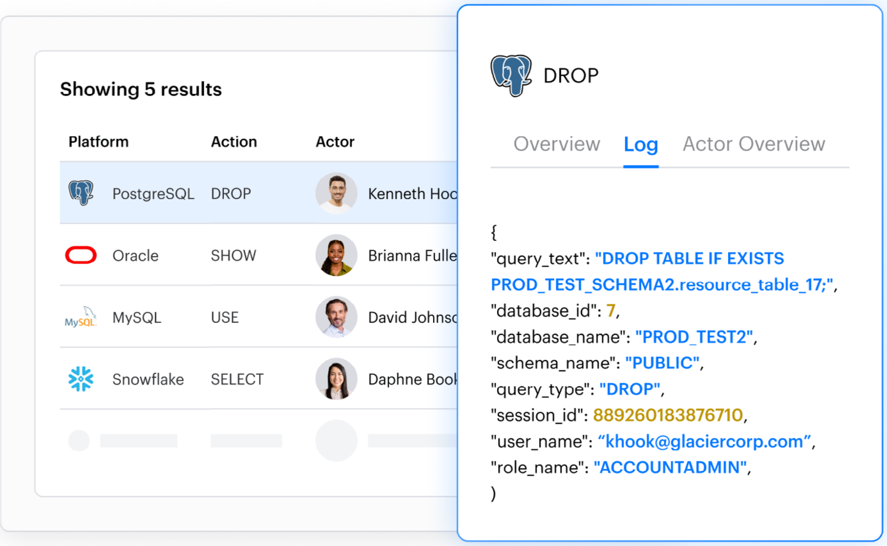
Comprehensive data protection beyond activity monitoring

Modern database security requires more than just activity monitoring. Organizations need comprehensive protection that addresses the full spectrum of data security challenges. Role-based access controls alone are not enough. Organizations must ensure that each user and application can only access the data they need and understand their usage patterns to ensure that their access doesn't get misused.

Varonis provides comprehensive data protection that includes:

Activity monitoring

Capture every database query with complete forensic detail of who accessed which data, when, and how. Automatically detect and block suspicious queries and sensitive data exfiltration in real-time.



Showing 5 results

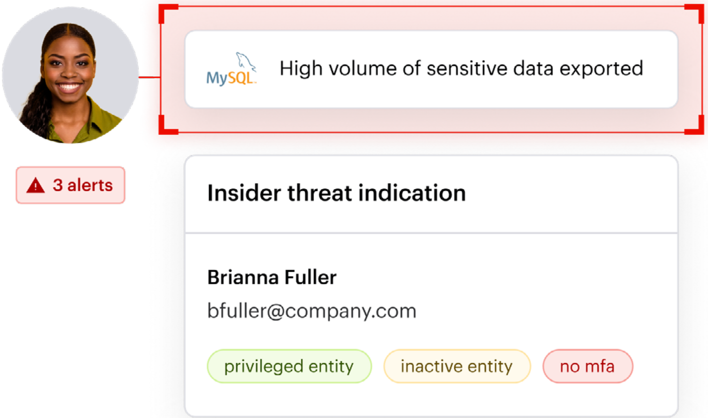
Platform	Action	Actor
PostgreSQL	DROP	Kenneth Hoc
Oracle	SHOW	Brianna Fulle
MySQL	USE	David Johnsc
Snowflake	SELECT	Daphne Bool

DROP

```
{
"query_text": "DROP TABLE IF EXISTS
PROD_TEST_SCHEMA2.resource_table_17;",
"database_id": 7,
"database_name": "PROD_TEST2",
"schema_name": "PUBLIC",
"query_type": "DROP",
"session_id": 889260183876710,
"user_name": “khook@glaciercorp.com”,
"role_name": "ACCOUNTADMIN",
)
```

Data-centric UEBA

Detect abnormal access patterns with behavioral analytics trained on activity across your whole tech stack from databases to cloud services, and SaaS applications.



High volume of sensitive data exported

3 alerts

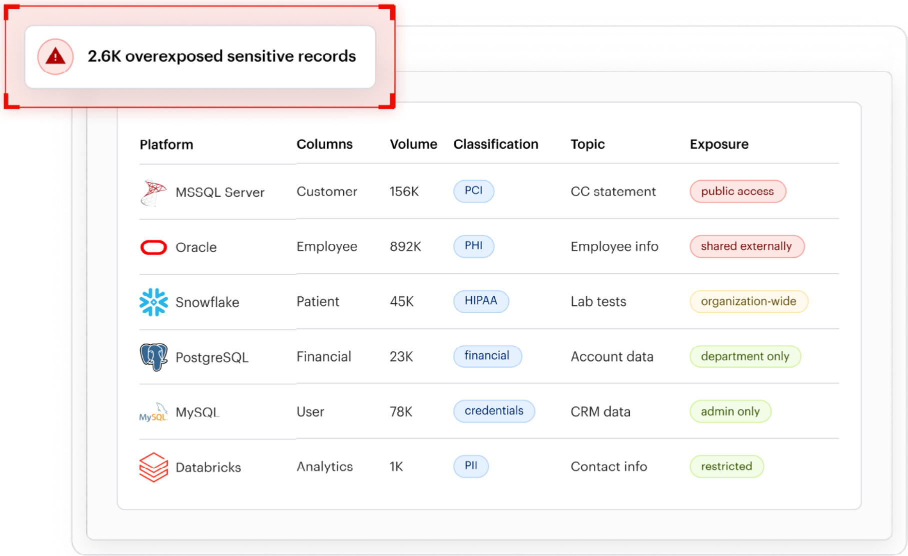
Insider threat indication

Brianna Fuller
bfuller@company.com

privileged entity · inactive entity · no mfa

Data discovery and classification

Discover and classify sensitive data automatically across your databases, cloud services, and SaaS applications while continuously mapping data sensitivity to compliance frameworks.

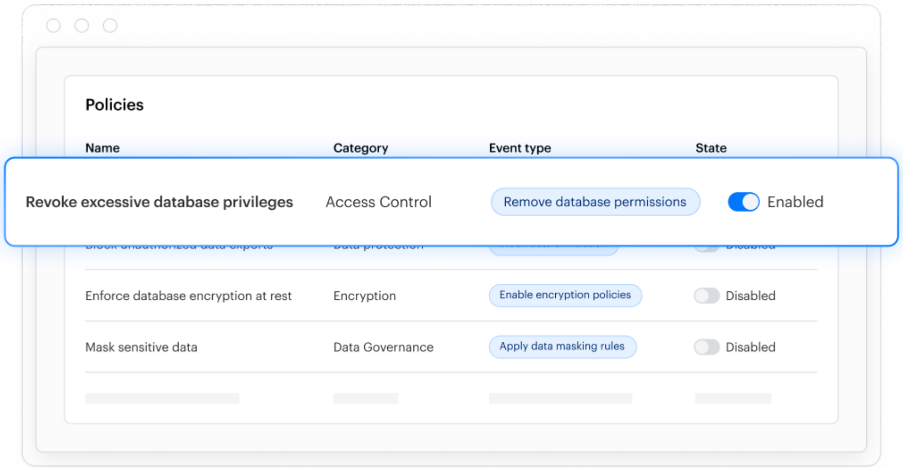


2.6K overexposed sensitive records

Platform	Columns	Volume	Classification	Topic	Exposure
MSSQL Server	Customer	156K	PCI	CC statement	public access
Oracle	Employee	892K	PHI	Employee info	shared externally
Snowflake	Patient	45K	HIPAA	Lab tests	organization-wide
PostgreSQL	Financial	23K	financial	Account data	department only
MySQL	User	78K	credentials	CRM data	admin only
Databricks	Analytics	1K	PII	Contact info	restricted

Automated remediation

Revoke excessive permissions, mask sensitive data, and enforce other security policies automatically. Maintain consistent policies for all your data with minimum overhead.

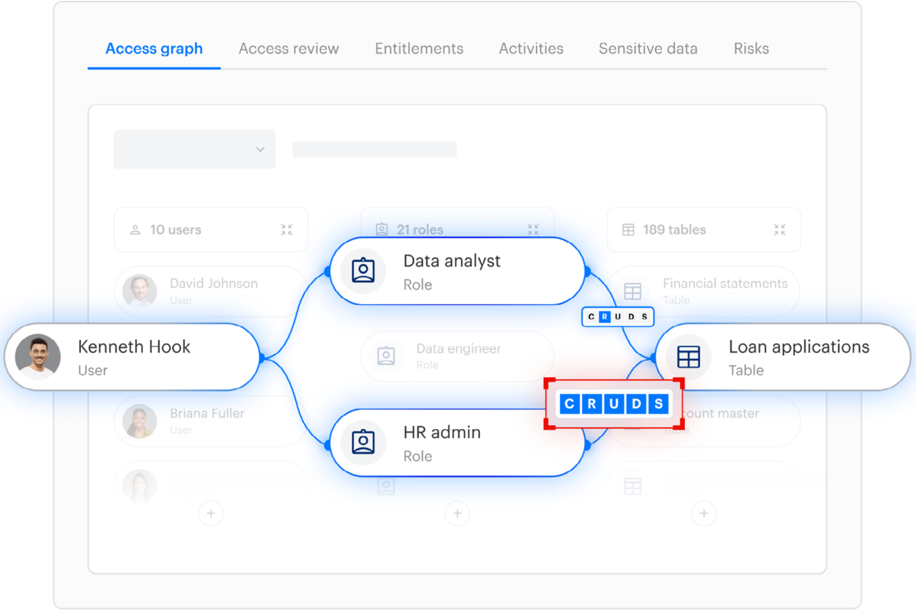


Policies

Name	Category	Event type	State
Revoke excessive database privileges	Access Control	Remove database permissions	Enabled
Block unauthorized data exports	Data protection	[illegible]	Disabled
Enforce database encryption at rest	Encryption	Enable encryption policies	Disabled
Mask sensitive data	Data Governance	Apply data masking rules	Disabled

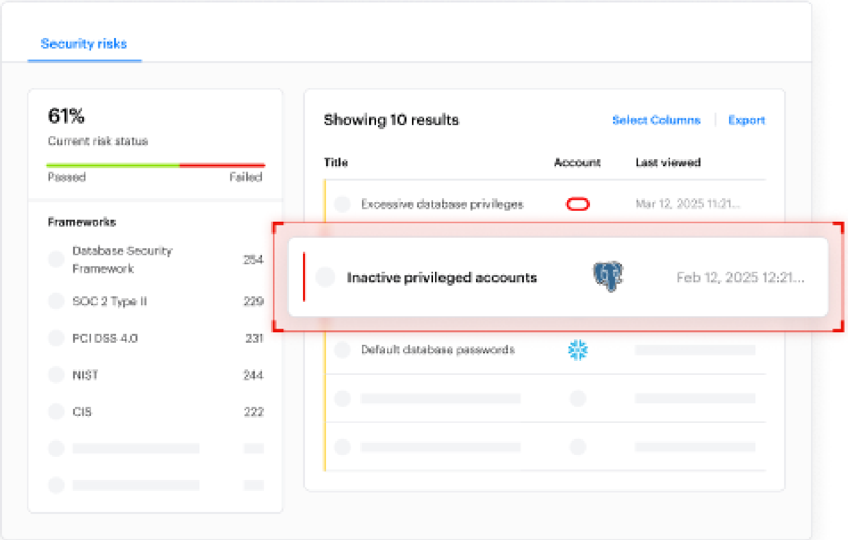
Identity protection

Connect database permissions and activities to corporate identities. Easily review, modify, and revoke access to achieve least privilege and weed out stale entitlements.



Posture management

Automatically detect and remediate risky configurations while continuously validating your security posture against hundreds of industry frameworks like NIST, HIPAA, and GDPR.



61%

Current risk status

Passed Failed

Frameworks

Database Security Framework	254
SOC 2 Type II	229
PCI DSS 4.0	231
NIST	244
CIS	222

Showing 10 results

Title	Account	Last viewed
Excessive database privileges		Mar 12, 2025 11:21...
Inactive privileged accounts		Feb 12, 2025 12:21...
Default database passwords		

Point solutions can't stop modern attacks

Attackers and rogue insiders usually target multiple data sources simultaneously, making it essential to detect and respond to threats across the entire data estate rather than within isolated systems.

Example 1: Multi-System Data Exfiltration

Let's say you get the following alerts within the respective systems:

- ⚠ ***Alert! (MSSQL):*** *Select * from hr_compensation by DBMSSQL345*
- ⚠ ***Alert! (Google Drive):*** *Quotes and contracts spreadsheet downloaded by jgcp4567*
- ⚠ ***Alert! (MySQL):*** *Select * from customer_login_credentials by DBMYSQL8976*
- ⚠ ***Alert! (Salesforce):*** *Export report: All Customers by MyCoSFlogin*
- ⚠ ***Alert! (GitHub):*** *Download source code repos by GoodBytes3254*
- ⚠ ***Alert! (MongoDB):*** *select * from GNA_financials by DataWiz123*

When considered one by one, none of the above alerts cause major concerns. Of course, HR Comp data is sensitive, but an FP&A analyst might need it for budget forecasting. Of course, the 'Quotes and Contracts' spreadsheet is sensitive, but a business analyst might need it to calculate the latest average discounts. Other alerts can be explained away as well and given that each of those systems generates dozens or hundreds of alerts each day, the above will most likely get ignored.

However, what if all these alerts were caused by the same user and all those actions were taken within 90 minutes? Now the picture is much different. It's clear that a bad actor is trying to exfiltrate sensitive data that includes customer data, company data, and IP. This should trigger an immediate suspension of all access and an investigation.

Only a unified approach to data security would be able to tie all these activities to a single individual.

Example 2: AI-Driven Data Exposure

An AI agent designed to provide business insights legitimately accesses HubSpot to report on performance metrics. However, if a user asks this same AI agent for granular customer details, it could inadvertently expose personally identifiable information (PII) by combining data from multiple sources—customer databases, support tickets, and sales records.

Only a unified approach to data security can enforce consistent security policies across all data sources that an AI accesses, preventing unauthorized PII disclosure regardless of how a prompt is formulated.

Benefits of a Unified Data Security Platform

A Unified Data Security Platform offers critical advantages over using multiple security solutions:

- **Consistent policy enforcement:** Apply the same data protection policies across different storage systems and access methods.
- **Comprehensive threat detection:** Identify attack patterns that span multiple data repositories rather than isolated incidents.
- **Streamlined operations:** Reduce the operational complexity of managing multiple point solutions with different interfaces and capabilities.
- **Enhanced compliance:** Demonstrate comprehensive data protection controls across all data repositories to satisfy regulatory requirements.

The future of database security

The path forward is clear: agentless, cloud-native database security platforms that deploy rapidly, scale efficiently, and provide comprehensive protection across the entire data estate. The question isn't whether to modernize your database security approach—it's how quickly you can move beyond legacy limitations to achieve real protection.

Organizations that act now will gain a competitive advantage through faster deployments, lower operational costs, and better security. Those who delay will continue struggling with the operational burden and security gaps that legacy DAM solutions create.

Get started with a free Data Risk Assessment.

Reduce your risk without taking any. Contact our team to learn what will be covered in your **free** Data Risk Assessment.

Get started at varonis.com/solutions/data-risk-assessment.

ABOUT VARONIS

Varonis (Nasdaq: VRNS) is the leader in data security, fighting a different battle than conventional cybersecurity companies. Our cloud-native Data Security Platform continuously discovers and classifies critical data, removes exposures, and detects advanced threats with AI-powered automation.

Thousands of organizations worldwide trust Varonis to defend their data wherever it lives — across SaaS, IaaS, and hybrid cloud environments. Customers use Varonis to automate a wide range of security outcomes, including data security posture management (DSPM), data classification, data access governance (DAG), data detection and response (DDR), data loss prevention (DLP), and insider risk management.

Varonis protects data first, not last. Learn more at www.varonis.com.