Is your organization prepared?

A GUIDE TO PCI DSS 4.0 DATA READINESS

DataBee®
A COMCAST COMPANY

databee.ai

Overview of Changes

Recent PCI Security Standards Council (PCI SSC) updates

In 2022, the Payment Card Industry Security Standards Council (PCI SSC) updated its PCI Data Security Standard (PCI DSS) in response to evolving technologies and customer demands. PCI DSS 4.0 included 64 new requirements, with 54 of those effective for assessments beginning March 31, 2025.

The new publication incorporated governance standards effective immediately for all v4.0 assessments across Requirements 2 through 11 that state: roles and responsibilities for performing activities [for the Requirement] are documented, assigned, and understood.

Further, PCI DSS requires organizations to perform targeted risk analyses (TRAs) and manage governance. Continuous controls monitoring (CCM) enables covered entities to document compliance activities and the people responsible for completing them.

To accelerate PCI readiness, organizations need reports based on consistent, accurate datasets enriched with information about management structures so they can identify process owners and business managers. With CCM, organizations can save time and money with real-time insights that help them define how frequently they need to perform activities.

Targeted risk analysis (TRA): Complexity creates compliance challenges

NEW REQUIREMENTS

For security, operations, and compliance teams, the new TRA requirement and the associated activities that define control performance frequency can become overwhelming.

PCI DSS 4.0 sets out two new risk assessment requirements intended to make compliance performance more flexible. These two new requirements are defined as:

- **12.3.1 A targeted risk analysis is documented to support each PCI DSS requirement that provides flexibility for how frequently it is performed.**
- **12.3.2 A targeted risk analysis is performed for each PCI DSS requirement that is met with the customized approach.**

Control Life Cycle Phases

Source: Gartner
779990_C

Source: Gartner®, Inc., Innovation Insight: Cybersecurity Continuous Control Monitoring, Jie Zhang, Pedro Pablo Perea de Duenas, Michael Kranawetter, 17 May 2023.[1]

[1]GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Gartner

Targeted risk analysis (TRA): Complexity creates compliance challenges (cont.)

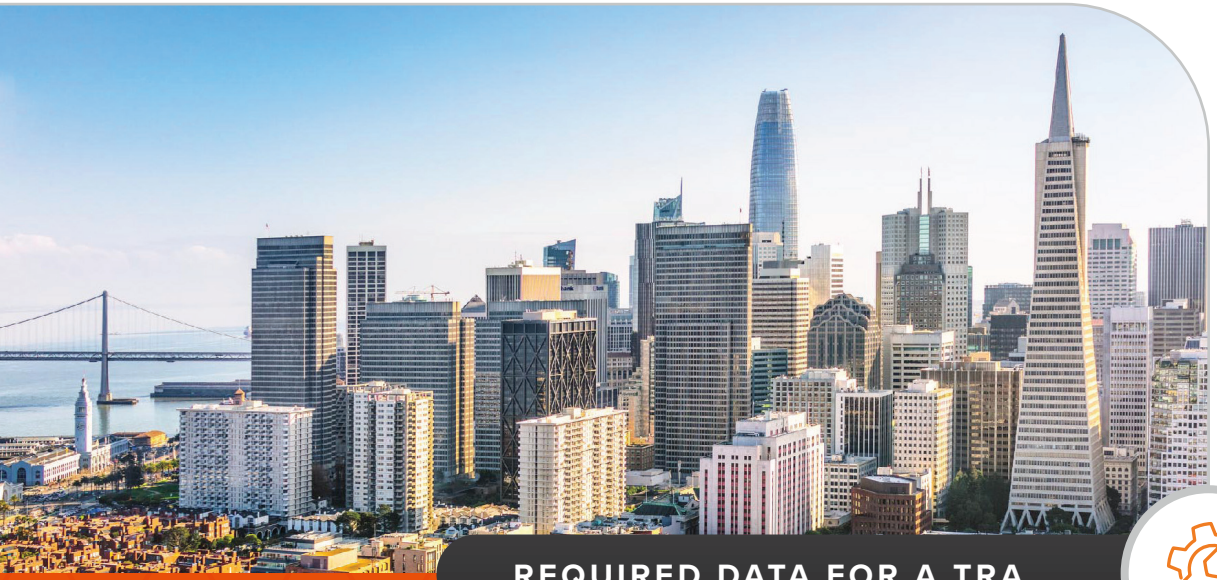
PCI-SUGGESTED FREQUENCIES

While 12.3.2 went into effect immediately for all v4.0 assessments, 12.3.1 became effective on March 31, 2025.

According to PCI DSS, these TRAs enable organizations to define how often they perform a control that achieves compliance with a specific requirement. While Requirement 12.3.1 applies to specific assets that organizations need to protect, Requirement 12.3.2 documents the reasoning behind choosing controls that provide equivalent security when not using the PCI DSS-suggested control.

According to the November 2023 Information Supplement, the TRAs should address the reasoning behind whether they use the following PCI-suggested frequencies for the required controls:

- **5.2.3.1:** Scanning system components not considered at risk for malware at least once every 6 months
- **5.3.2.1:** Performing malware scans or continuous behavioral analysis to identify present but currently inactive malware at least once a day
- **7.2.5.1:** Reviewing application, system accounts, and their related access at least once every 6 months
- **8.6.3:** Changing application and system account passwords/passphrases at least once every 3 months
- **9.5.1.2.1:** Inspecting Point of Interaction (POI) devices to detect tampering or unauthorized substitution at least once every month
- **10.4.2.1:** Reviewing logs for system components that fall outside of the security event, Card Holder Data (CHD), Sensitive Authentication Data (SAD), critical system component, and security function scope at least once every 7 days
- **11.3.1.1:** Addressing non-critical or non-high-risk vulnerabilities based on risk, meaning within 3 months for medium-risk, 6 months for low-risk, and regularly monitoring for informational
- **11.6.1:** Reviewing HTTP headers and payment page contents for unauthorized modifications at least once every 7 days
- **12.10.4.1:** Training incident response personnel at least once per year and when they start employment



REQUIRED DATA FOR A TRA

PCI SSC provides a template that organizations can use to ensure they include the following required information:

- Asset(s) protected
- Threat(s) against the asset
- Factor(s) contributing to the likelihood or impact of threat occurring
- Analysis of and justification for how often the organization performs the requirement
- Whether an annual review requires an update to the analysis
- Existence of defined and documented policies and procedures for performing the TRA consistently

TRA Requirements

Manual analyses: Time-consuming and inconsistent

At the enterprise level, complex systems create compliance challenges. An organization can use hundreds of security tools that generate high volumes of log data to perform the required controls. However, they struggle to gain insights because these technologies use diverse data schemas and often duplicate data points, leading to inaccurate risk analytics and reports.

Traditional security solutions, like security information and event management (SIEM), may enable the appropriate monitoring under PCI DSS 4.0, but they fail to enrich the alerts with business and organizational hierarchy information. This inability to connect security and business data with the people managing day-to-day activities means most companies use point-in-time spreadsheets for documenting how they comply with the roles and responsibilities requirements, which are time-consuming, error-prone, and expensive.

A Solution

Connecting people, data, and technologies with DataBee®

DataBee®, a Comcast Company, offers DataBee for CCM, which delivers consistent and accurate PCI DSS compliance dashboards that empower operational managers, risk managers, and internal auditors.

Enrich security data with management structure for assigning and managing responsibilities

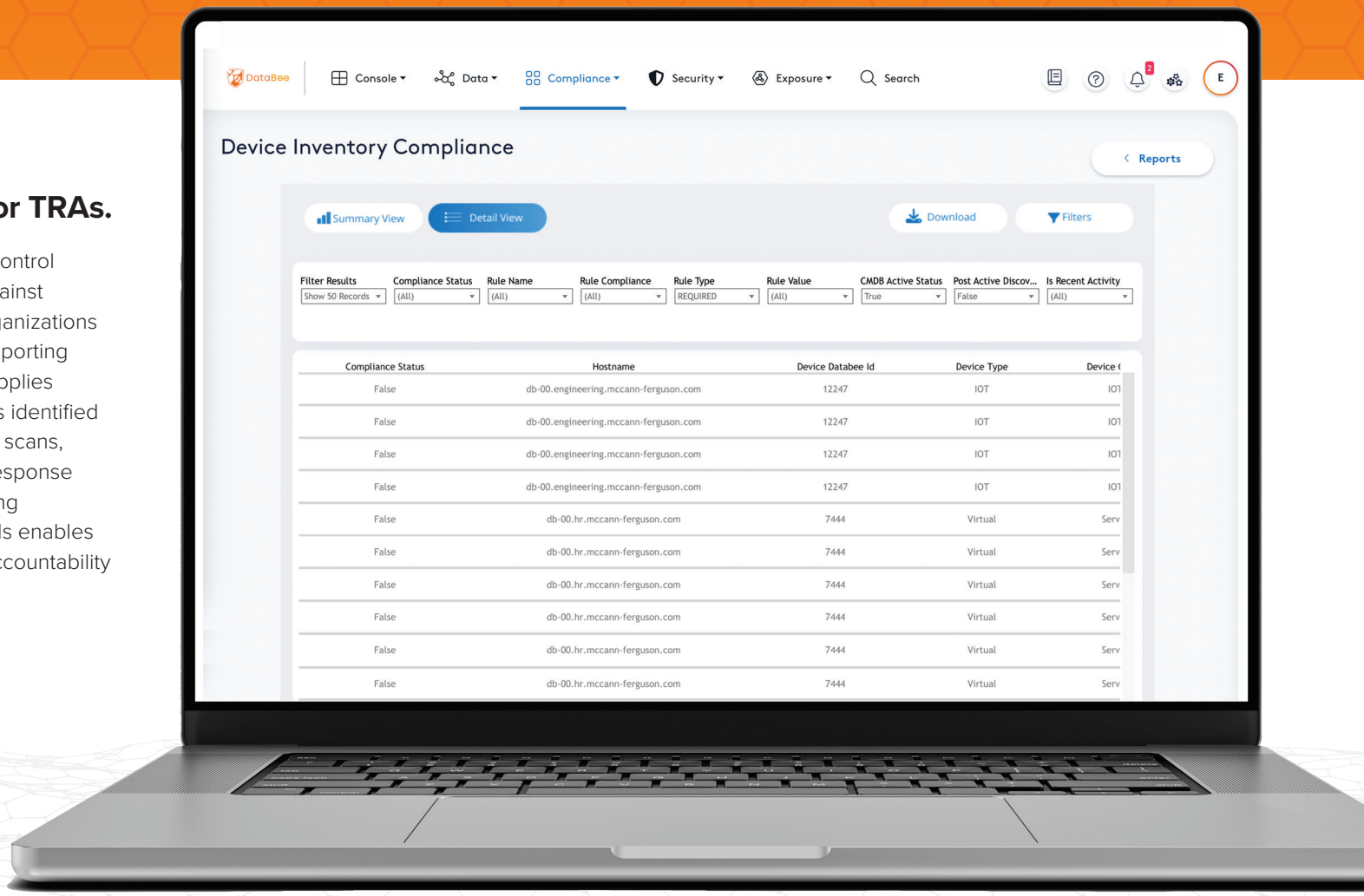
Correlate security data, like vulnerability scans, with the people responsible for remediation activities. Predefined dashboard views and reports empower business managers by providing the data necessary to comply with the enterprise security policy with the ability to drill down into details about the people and assets they manage. By correlating control performance data with process owners and business managers, organizations can:

- **Document their compliance with PCI DSS.**
- **Build accountability over compliance to meet new governance requirements.**

A Solution (cont.)

Build trustworthy risk analytics for TRAs.

Leverage data analytics to establish customized control baselines, then continuously test and measure against target goals. With data transparency and trust, organizations can consistently track performance over time, supporting their TRA control frequency decisions. DataBee applies organization hierarchy data to various other inputs identified with PCI tags, including vulnerability management scans, device inventories, and endpoint detection and response (EDR) tool data. Automatically scoring and rescoring leaders and departments against control standards enables organizations to create a culture of compliance accountability that reinforces their governance documentation.

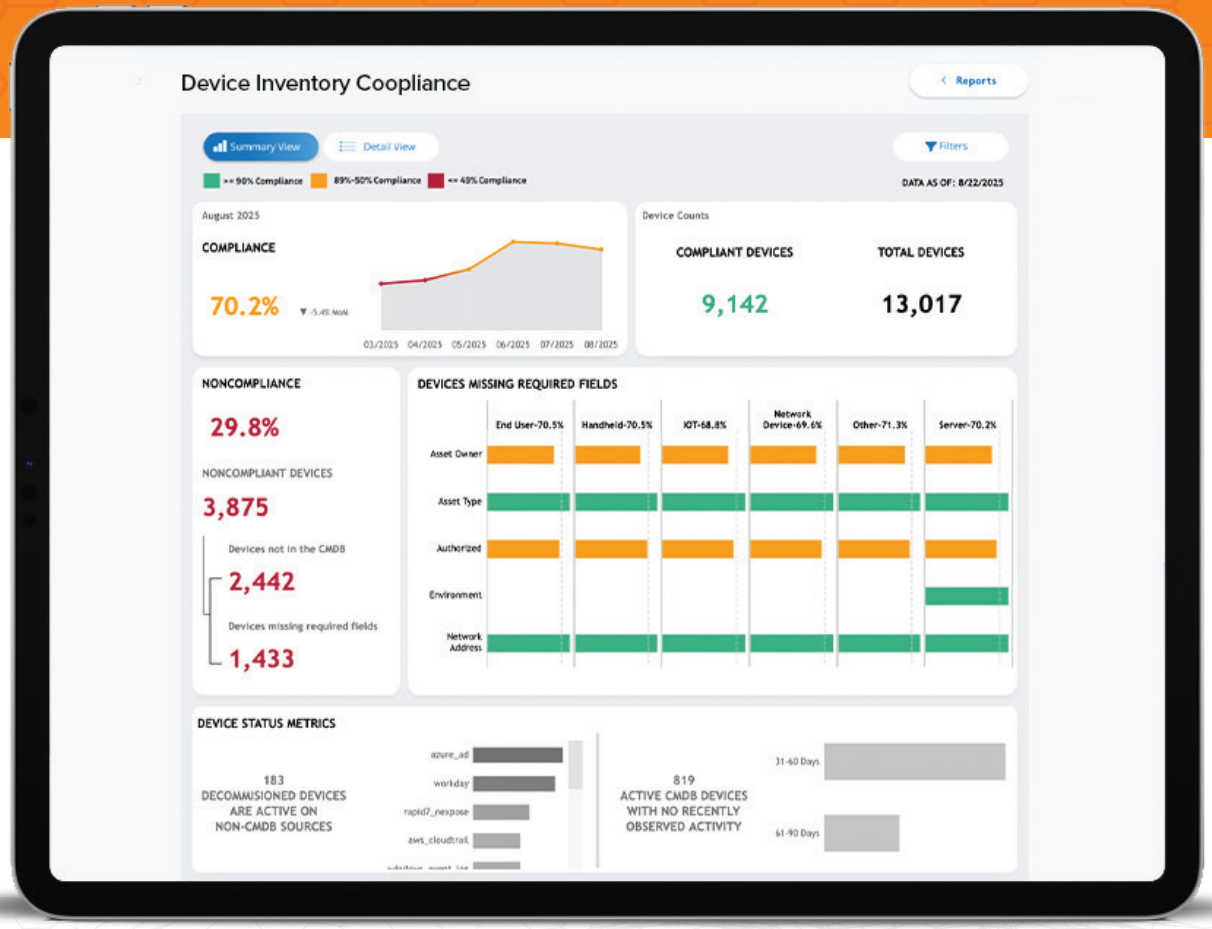


databee.ai

A Solution (cont.)

Easily accessible reporting can help you reduce audit time and costs

Provide fast compliance answers with evidence of adherence to security controls, policies, and procedures. By eliminating time-consuming manual security data mapping, organizations are empowered to improve operational efficiency while reducing audit costs. With year-round insights for real-time and historical insights into controls and compliance trends, organizations enhance communication throughout the compliance lifecycle — from defining controls objectives to evaluating controls implementation, ensuring accountability, monitoring controls effectiveness, and responding to auditor questions.



We Can Help

Get started with DataBee

DataBee meets you where you are with your data — whether that is on-premises, in the cloud, or applications — and weaves together related data points, normalizing to the OCSF format and enriching with business context.

Security operators, analysts, and threat hunters can now use the same time-series dataset rich with business-relevant information for their security workflows.

Inspired and proven at Fortune 30 scale, DataBee unlocks the power of your security data so your enterprise can make data-driven, informed cybersecurity investment decisions based on business and security needs.

Find out how DataBee can help your organization.

Schedule a demo