Teradata and Protegrity – High-Value Protection for High-Value Data

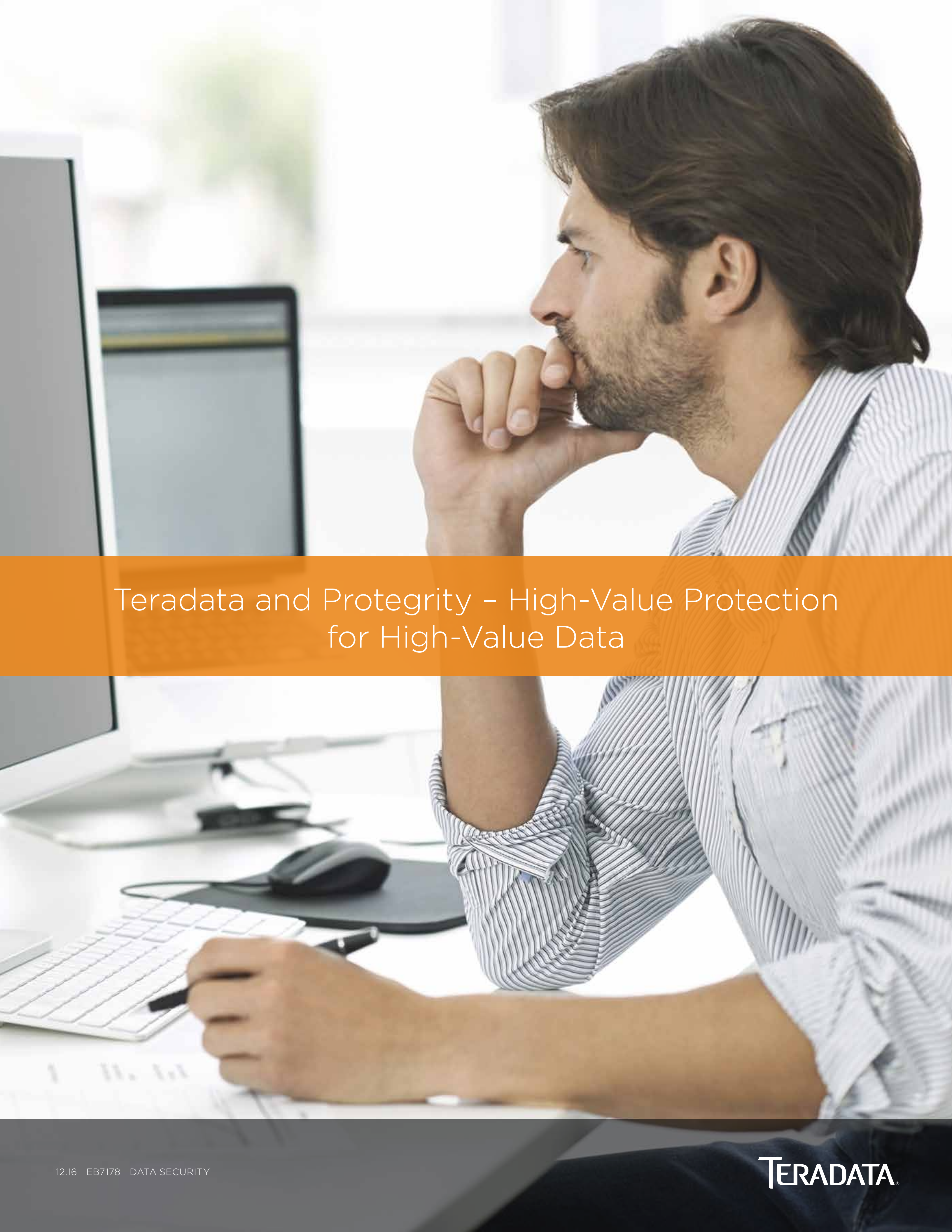


Table of Contents

- Data is a powerful asset used to better know each customer, but the more data there is, the more challenging it is to keep it secure and safe.
- Attacks happen even with powerful perimeter security, which is why it's so important to leverage data centric controls to secure the data itself.
- Centralized security policies, automated logging and monitoring and monitoring of network and user database activity are critical pieces of this effort.
- Protegrity and Teradata have been partners since 2004 when Protegrity first built its data security platform for Teradata from the ground up.
- The Protegrity Enterprise Security Administrator (ESA) client interface provides a real-time dashboard view of connected databases and users, roles, system status, policy deployments, rule-based audits, reports and alerts, and other features.
- Additional safeguards are provided using Protegrity to segregate duties and responsibilities among DBAs and Security Roles.

Data Centric Security: Providing High-Value Protection for High-Value Data

Data is the lifeblood of any organization, but are your data assets secured inside your borders? Especially your highest value data assets? And how do you know they're safe? Do you know what users are doing on your network, in your databases, applications, at all times?

One of the nation's largest health insurers thought its most sensitive data was safe—until it wasn't. Bad actors compromised one of its databases December 10, 2014. The breach was only discovered when a DBA observed his credentials being used to run a questionable query that he didn't initiate. That was January 27, 2015, more than a month and a half after the breach. The hackers accessed names, social security numbers, dates of births, addresses, and more from as many as 80 million patient and employee records.

Retail data breaches have also been well documented over the past few years. One major retailer thought its data assets were safe, until a massive data breach exposed more than 40 million debit and credit card accounts, as well as personal information of as many as 70 million people. Attackers broke into the retailer's network using credentials stolen from an HVAC contractor that did business with the retailer. At least one employee at the contractor fell for a phishing email, enabling malware to be installed with their login credentials. The attack went undetected for almost a month. The estimated cost of the breach to the retailer has been estimated up to $420 million so far.

The more data companies have the better they can know each customer, and the better they can market and sell to them. But there's the rub. More data is more challenging to keep secure and safe, and to identify the highest value sensitive data that needs the highest level of protection. Customers and employees expect their sensitive information to be protected. Internal corporate governance, regulatory organizations, and laws demand accountability in protecting sensitive, high-value data, including financial information, individual privacy, intellectual property (IP), and operational/business data.

As we've seen, attacks happen even with powerful perimeter security, making the best first line of defense the ability to provide protection of the data itself. Security in layers is a best practice and applying security directly to the sensitive data itself assures the data is protected at all times, through such forms as masking, hashing, encryption, and tokenization. Fine-grained security in the form of tokenization or encryption replace sensitive data with useless replacement values that guarantee the data is meaningless even if a privileged account is compromised. Tokenization preserves data types so that replacement tokens are of the same data type. This allows analytics on top of the protected data where referential integrity is preserved. The next line of defense is detection. While an intrusion can happen in milliseconds, the real damage occurs after hackers extend their foothold, move about undetected, and eventually find a way to steal valuable data.

Visibility: What's Happening with Your Data

Threats are external and internal. High-tech hackers have become more sophisticated and organized as they exploit human error and weak security controls. Hackers know that the best way to initially delay or avoid detection is to change logs so user activity monitoring won't show their activities, like gaining access to resources, which is why logs are typically the first place hit. Moreover, employees can unknowingly make high-value data vulnerable in a variety of ways, such as emailing an unencrypted file containing sensitive data to the wrong person, or losing a tablet or laptop computer containing customer records or IP.

The key to identifying attacks: visibility. You can't protect yourself from something if you don't know it's there, which is why automated network logging and monitoring of user activity—what is happening on your network at all times—is so critical. The goal is to detect the good from the bad activity and the right people notified of the bad immediately so decisive, damage limiting action can be taken right then.

A place to start is understanding where the greatest protection is needed—on high-value data. That means understanding and classifying the value and sensitivity of different kinds of data. It also means identifying, understanding, and complying with relevant legal requirements for logging and monitoring user activity. To mitigate risk, many pieces of the information processing environment (applications, databases, operating systems, firewalls, intrusion detection systems, routers, switches, hubs, VPNs, and other solutions) should have logging enabled to capture, aggregate and correlate events. Addition of a data centric security platform complements these sources with an externally maintained tamper-proof record of activity on sensitive data. Organizations can couple these solutions with a security information and event monitoring (SIEM) system to capture event logs from all systems and devices, and normalize the data for aggregation, alerting, reporting., and in some cases, correlation of seemingly unrelated events the provide insight into threats.

Monitoring User Activity: Minimizing Data Risk with Policies

In the past, IT security professionals were primarily concerned with keeping unauthorized individuals out of their network. While this remains a major concern, organizations also need a solution that balances data security and compliance demands with business accessibility needs. IT security professionals must protect their assets while granting different levels of access to a range of individuals, whether full- or part-time employees, partners, contractors, or customers.

Businesses must simply know what their users are doing in each piece of the ecosystem. Robust user activity monitoring and alerting helps this. Plus, flexible data centric security policies provide a means of limiting risk by presenting only the minimal amount of sensitive data required by role. This means, for example, that in a given application, one user may see a fake tokenized SSN, another may see the last 4 digits, while another may see all 9 digits of the SSN. It also means that a user who, for example, repeatedly attempts to access high value data with no need to do so will be discovered by a rule and alert.

Data-Centric Protection Built for Teradata Ecosystems

Teradata ecosystems offer the platforms for organizations to maintain massive databases that support large-scale analytic needs regardless of data structure. With so much data available for analysis, it's critically important to properly protect the most sensitive data in the Teradata environment.

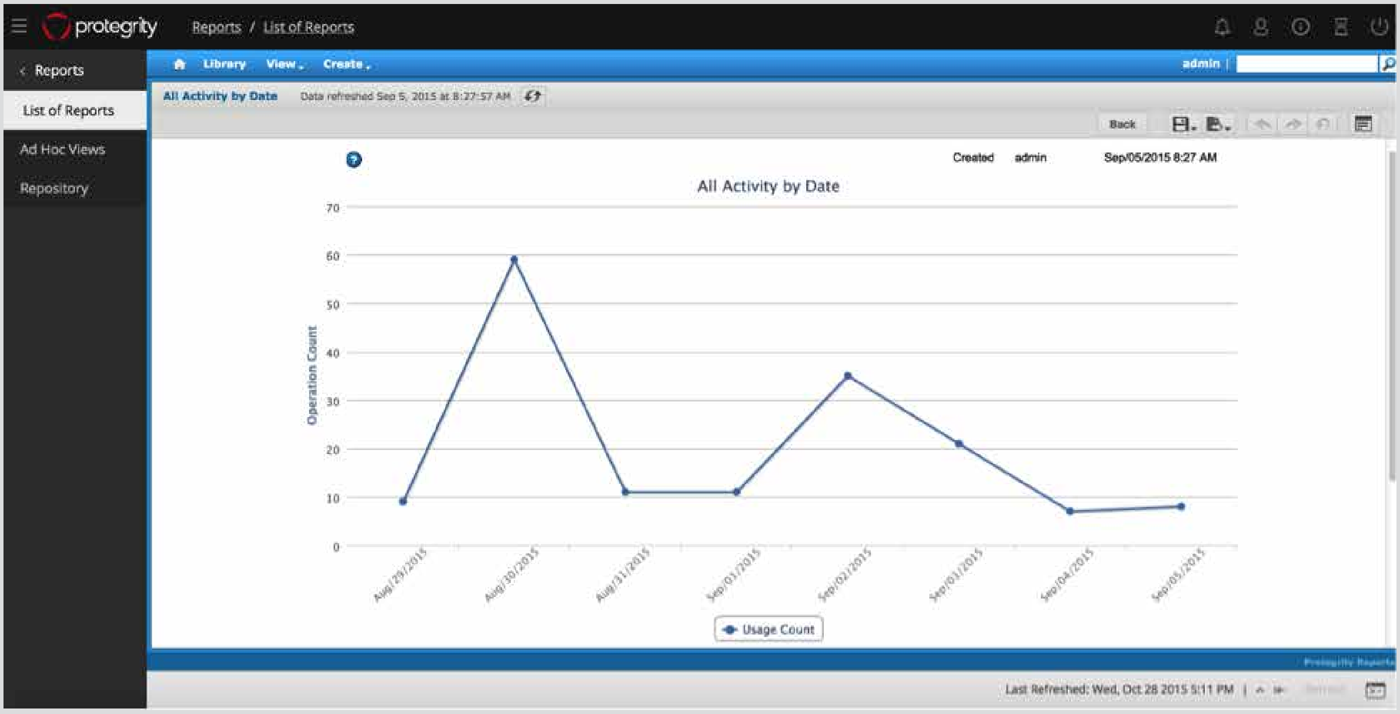
Since 2004, Protegrity and Teradata have partnered to enhance data security in Teradata from the ground up, leveraging Teradata's scalability and massive parallel processing architecture. The result is completely integrated, optimized security for the Teradata ecosystem that provides protection for the unique way Teradata operates.

Unlike other RBBMS, Teradata doesn't store data in files. It stores them in a unique, technical way that requires understanding Teradata at the lowest level of parallelism. The Protegrity data security platform leverages that parallelism to provide the highest performing data centric security available on Teradata. The result is column-level data encryption, tokenization, and masking in database tables, while employing strong access rights and user activity audit controls. Protegrity protects sensitive data in Teradata in transit, in use, and at rest to ensure the data is protected at all times in its lifecycle.

The Protegrity Enterprise Security Administrator (ESA) client interface provides a real-time dashboard view of connected databases and users, roles, system status, policy deployments, rule-based audits, reports and alerts, and other features. All authorized and unauthorized attempts to access or use protected data as well as change to security policies are monitored and logged by the system. Management and compliance reports are standard, custom reports can be created, and a powerful rules engine allows for alerting right when a potential security violation occurs.

The Enterprise Security Administrator (ESA) permits flexible centralized policies to ensure that security policies for sensitive data permit maximum usability with minimal risk. The policies follow the data so that access is consistent regardless of where the data goes or which application is used.

Additional safeguards provided by Protegrity include segregating duties and responsibilities so no single person has all "the missile launch codes," leaving security administration to security officers, and data administration to DBAs and application administrators, who do not need to and cannot access sensitive data in the clear or grant



Data refreshed Sep 5, 2015 at 8:27:57 AM

Last Refreshed: Wed, Oct 28 2015 5:11 PM

Figure 1.

Aspect	Definition
What	Sensitive data to be protected
How	Method(s) of data protection used
Who	Users that are authorized to access sensitive data
When	Time(s)/day(s) when data can be accessed
Where	Systems/applications in which policy is enforced

Table 1. Manage Data Security Policy.

security access to others. Since the data itself is protected, technology roles—DBAs, programmers, or system engineers—can continue administering different aspects of the enterprise IT environments without disruption to business processes, including movement of data without unprotecting it.

Prevent Large-Scale Loss

Commonalities seen in most breaches make it easy and tempting to look back and say, "This could have been prevented." Most attacks begin with credential theft, as was the case in the retail data breach, where contractor credentials were compromised and used. Hackers slipped into their vendor portal, did reconnaissance to learn weak points in the network, and then struck, exfiltrating sensitive data.

Beyond ensuring credentials never get compromised, essential steps include protecting sensitive data for as much of its lifecycle as possible through data centric security with encryption or tokenization, mitigating the impact of attacks by real-time auditing and alerting of user activity, and flexible centralized security policies that permit consistent security wherever the data goes. That would have made all the difference for hundreds of organizations who have experienced a data breach.

To find out more about how Teradata and Protegrity can help you with your security needs, contact your local Teradata representative or visit **Teradata.com**.

About Teradata

Teradata empowers companies to achieve high-impact business outcomes. Our focus on business solutions for analytics, coupled with our industry leading technology and architecture expertise, can unleash the potential of great companies. Visit **Teradata.com**.

About Protegrity

Protegrity is an enterprise data security software solution that leverages scalable, data-centric encryption, tokenization and masking to help businesses secure sensitive information while maintaining data usability. Built for complex, heterogeneous business environments, the Protegrity data security solution provides unprecedented levels of data security certified across applications, data warehouses, mainframes, big data, and cloud environments. Companies trust Protegrity to help them manage risk, achieve compliance, enable business analytics, and confidently adopt new platforms.

10000 Innovation Drive, Dayton, OH 45342 **Teradata.com**

Teradata and the Teradata logo are registered trademarks of Teradata Corporation and/or its affiliates in the U.S. and worldwide. Teradata continually improves products as new technologies and components become available. Teradata, therefore, reserves the right to change specifications without prior notice. All features, functions, and operations described herein may not be marketed in all parts of the world. Consult your Teradata representative or Teradata.com for more information.

Copyright © 2016 by Teradata Corporation All Rights Reserved. Produced in U.S.A.

12.16 EB7178