



Cyber Security

Big Data Integration and Analytics for Cyber Security



Cyber Security Challenges >
The Power and Potential of Big Data >
Using Big Data Analytics for Cyber Security >
Teradata Solutions for Cyber Defense >
Teradata Partner Solutions >
Resources >

TERADATA®



Cyber Security Challenges in Industry and Government

As cyber security challenges continue to grow, new threats are expanding exponentially and with greater sophistication—rendering conventional cyber security defense tactics insufficient. Today's cyber threats require predictive, multifaceted strategies for analyzing and gaining powerful insights into solutions for mitigating, and putting an end to, the havoc they wreak.

Cybercrime costs \$118 billion annually from theft of information assets, disruption of service and more.

Each successful attack takes an average of 18 days to resolve at a cost of nearly \$416,000. These figures are expected to grow as attacks on sensitive data continue to increase.

Cyber-crime is an all too common reality, with directed security attacks hitting a wide variety of industries and government organizations.



With cyber-attacks increasing at unprecedented rates, it's become clear that industry and government organizations alike need to do even more to safeguard sensitive data, as well as their business reputations.

Ponemon Institute Study

The growing concern of widespread cyber-attacks and security readiness was confirmed in a 2013 study conducted by the Ponemon Institute, "Big Data in Cyber Defense."

The study surveyed over 700 Information Technology (IT) professionals and IT security practitioners in government, financial services and manufacturing. While those surveyed agree that cyber-attacks are getting worse, only 20 percent believe their organizations are more effective at stopping them.

For complete Ponemon survey results, [click here](#).

Study participants cite deficiencies in technology and staff expertise as leading obstacles to effective cyber defense.

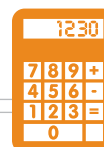
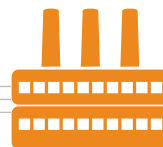
From amateur adversaries to evolving state-sponsored actors and organized criminal networks, cyber-attacks can vary in scope and level of sophistication. Moreover, they can take many forms, including highly sophisticated efforts such as Advanced Persistent Threats (APTs) designed to evade detection by conventional network defense tools, techniques and procedures.


Why Conventional Methods Aren't Working

- Conventional layered defense strategies generate large volumes of false positive alerts, overwhelming security professionals
- Traditional cyber security tools cannot effectively process large volumes of data, resulting in missed signals that should trigger real threat alerts
- Bad actors remain undetected, hiding in plain sight on your network
- What's needed? An advanced, more strategic approach to network security that disrupts adversary tools and techniques, rendering them ineffective



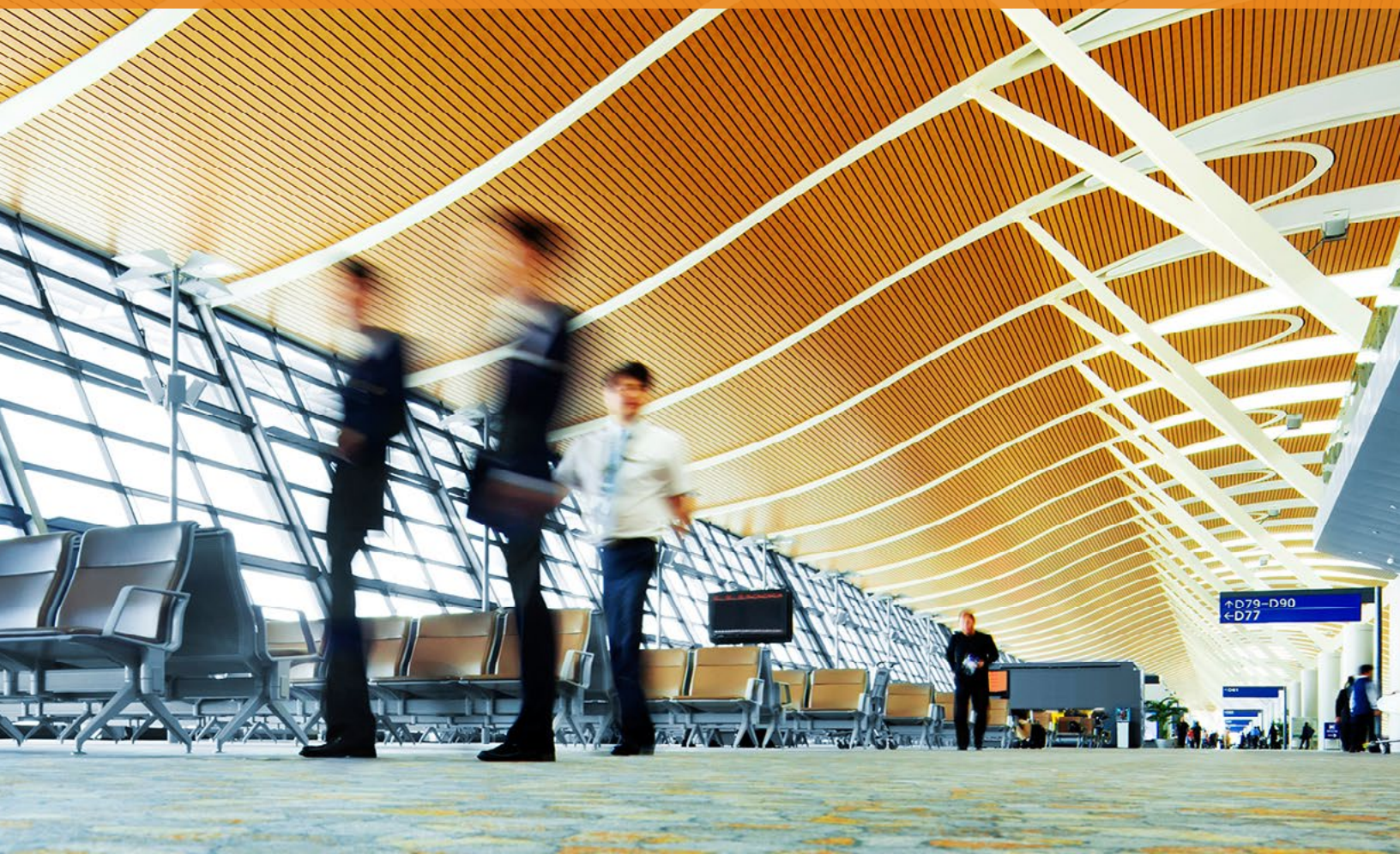
Learn more about the power of big data and cyber defense in creating stronger cyber security in this insightful Q&A, featuring information security systems expert Sam Harris.





Big data is becoming one of the most effective defenses against cyber intrusions.

The Power and Potential of Big Data



Conventional approaches to cyber security are largely reactive and, many times, disparate. The result is that it takes too long from the time of intrusion to remediation—allowing unnecessary and debilitating economic and reputational harm. Fortunately, big data—along with emerging security technology solutions—are joining together as a powerful solution for handling the volume and complexity of cyber-attack detection and prevention, enabling you to stay ahead of evolving threats.

What Is “Big Data”?

Big data is often defined as data sets too large and complex to manipulate or query with standard tools. However, together with today’s security technologies and advanced skills, big data can now be effectively organized, managed and analyzed to provide users a unique opportunity to visualize and draw powerful insights into solutions for stopping cyber-attacks.

With networks growing so large and fast, existing attempts to monitor network activity for threats inherently become a big data issue.

“Cyber security is really a ‘data-centric’ issue because it involves integrating the data you already have; augmenting it with enrichment data; and applying new queries and big data analytics. The result is achieving near real-time network security and awareness.”

– Sam Harris, Director of Cyber Security and Enterprise Risk Management Solutions for Teradata

Leveraging Existing Data

Conventional thinking suggests that network data volumes are too large; therefore, the analysis needed to mitigate cyber threats is too complex and time consuming to be cost effective. However, today’s integrated analytic solutions help organizations leverage structured data, along with big data, to build formidable defenses against cyber security threats.



Read more about hidden cyber security threats in this white paper from Teradata, “The Threat Beneath the Surface: Big Data Analytics, Big Security and Real-Time Cyber Threat Response for Federal Agencies.”





Combined with the latest in security technologies, big data helps build a dramatically stronger cyber defense posture.

Using Big Data Analytics for Cyber Security

Big data analytics for security provide the unique ability to analyze information from multiple sources and data types. This allows near real-time responses to cyber-attacks, improved readiness, and shorter response times to remediation. It can also improve the effectiveness of existing investments in security solutions, and increase the efficiency of your security personnel.

Getting Started with Big Data

High-speed, automated analytics empower organizations to extract more value—and remove malicious software and actors—from current and legacy data environments.

All data and network assets are not necessarily equal in value. As an example, credit card data is extremely valuable, and a high-risk asset, compared to marketing information organizations use to reach their customers

and prospects. For this reason, systems that process credit card data require much higher levels of security than those that process data for external promotions.

Conduct a cyber risk assessment

The first step in integrating big data analytics for security is to complete a cyber risk assessment of the organization's data and network assets to identify the most critical systems to protect. There are a variety of frameworks that should be included in the assessment, such as COSO, COBIT, and others. These frameworks identify organizational objectives; the processes involved in accomplishing those objectives; risks that could prevent their successful execution; controls to manage or prevent risk; testing to ensure the effectiveness of the controls and reassessment; and more.

Develop a roadmap for prioritizing actions

After completing the security risk assessment, the strengths and weaknesses of the legacy cyber defenses should be cataloged, quantified, and used to develop a roadmap for prioritizing actions. This is a crucial step for addressing and aligning the information security risk with the overall risk tolerance of the organization.

Optimize effectiveness of existing security solutions

According to the Ponemon Institute study, over 60 percent of participants agreed that big data analytics will solve pressing security problems. Moreover, introducing integrated security data and big data analytics can also significantly improve the efficiency and effectiveness of existing security solutions—as well as the personnel that operate them. For example, an Intrusion Detection System alert can programmatically trigger a big data query in another system to deliver the actual network session data to an analyst for fast identification,

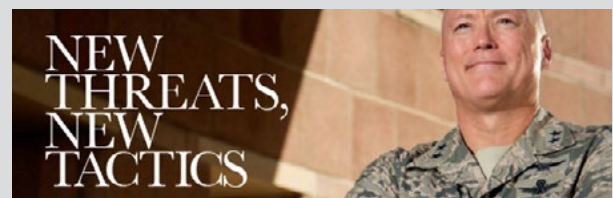
triage and remediation. The session data then enables the analyst to quickly determine if the alert is real or false. If real, session data can also be used to evaluate incident severity to prioritize remediation. In both cases, integrated data and big data analytics make existing systems more effective, and the incident responder more efficient.

The Security Approach—Evolved

Ultimately, the goal is to evolve the security approach to next-generation threat detection and cyber situational awareness. By capturing and visualizing precisely what's coming and going on networks as events happen, organizations can correlate activity through its network data elements as they are generated from each application, transaction, communication or transmission.



Learn how **Teradata enables near real-time detection** and remediation in this video, *Winning the Cyber War*.



Also, **check out the in-depth Public CIO Special Report** on new threats and new tactics in cyber security.



Security professionals need to see more relevant data, so they can do more—faster.

Teradata Solutions for Cyber Defense

A New Approach to Mitigating Security Breaches

Despite limited resources or the apparent complexities that go hand-in-hand with safeguarding sensitive data, achieving a sound defense against cyber-attacks doesn't have to be complicated. Teradata, the global leader in data warehousing and analytic technologies, helps companies get more value from data than any other company—while helping you gain a sustainable competitive advantage.

Teradata delivers a single, authoritative ecosystem integrating InfoSec, cyber security and network operations data infrastructure, analytics and reporting.

Given the ever-evolving strategies for breaching today's security measures, relying solely on traditional approaches isn't enough. Teradata cyber defense solutions are designed to

augment—not replace—traditional enterprise security measures by infusing big data analytics for improving cyber defense in organizations of all sizes.

Teradata Integrated Data Warehouse (IDW)

The IDW provides the foundation for innovative analysis of activity on the network for near real-time detection and remediation. It combines structured, semi-structured and historic data—such as past signatures and intrusion patterns—along with other compliance data for intelligence collection and event correlation.

The structured security product data is stored and analyzed in the IDW. The IDW is also integrated with the Teradata Aster Discovery Platform, which provides out-of-the-box MapReduce functions using SQL syntax for discovery analytics and easy access to Apache™

Hadoop®. Together, they're used to collect, integrate and analyze unstructured data—machine generated data or network data with big data characteristics, such as volume, velocity and complexity—that are otherwise difficult to analyze with conventional tools.

The Teradata Unified Data Architecture (UDA) provides high-speed connectivity between structured and unstructured security data storage and data-driven analytical environments.

Additionally, the UDA environment enables security analysts to simultaneously join and query unstructured and structured data. Once configured, a data-driven discovery of patterns characteristic of relationships between endpoints or the paths to a data breach can be seen. Near real-time detection allows organizations to quickly and iteratively understand network weaknesses, isolate threats, and reveal concealed cyber-attack vectors.

With Teradata cyber defense solutions, you get seamless, single-source access to the critical data you need—when you need it—to gain powerful insights on safeguarding sensitive information and minimizing the risk of cyber-attacks.

Teradata Unified Data Architecture for Cyber Defense

The Teradata Unified Data Architecture™ allows organizations to capture, deploy, support, manage and seamlessly access all their data.



Teradata offers pre-packaged analytic functions and applications that can be uniquely configured to defend against cyber-attacks.



Listen to a podcast with Scott Gnau from Teradata Labs as he discusses various aspects of Big Data and the importance of the Teradata Unified Data Architecture for a high-performance analytics environment.



Learn how Teradata analytics can speed remediation of cyber-attacks in this solution brief, *When Big Data Meets Cyber Defense, Enterprises Win*.



Working together, Teradata delivers next-generation solutions for increased visibility into network behavior analytics for information security and cyber analytics.

Teradata Partner Solutions

Teradata is uniquely positioned to partner with organizations for building strong defenses against the risk of cyber-attacks. Our solutions are designed to augment traditional enterprise security measures you already have in place with big data analytics for improved cyber defense. The result? Our customers gain a keen ability to organize, manage and analyze large-scale data that provides powerful insights into solutions for stopping cyber-attacks.

Novetta Cyber Analytics— powered by Teradata

Teradata is partnered with Novetta Solutions—a leading provider of mission-critical analytics solutions to the U.S. Department of Defense and other government agencies—on data strategies for increasing visibility into network behavior analytics. Novetta's advanced cyber analytic solutions help government and commercial organizations quickly extract value from massive and disparate data sets to make data-driven decisions and meet demanding security requirements.

Novetta Cyber Analytics is a network security visibility and awareness solution that substantially increases the effectiveness of security analysts and infrastructure.

Novetta Cyber Analytics has proven its speed and scalability on one of the largest and most attacked enterprise networks in the world—the U.S. Department of Defense.

The Teradata Integrated Data Warehouse (IDW) and Unified Data Architecture (UDA) provide the dedicated performance required for near real-time processing and storage of network metadata and enrichment data. This powerful combination gives critical support to the Novetta Cyber Analytics solution, helping it effectively defend networks against cyber-attacks.

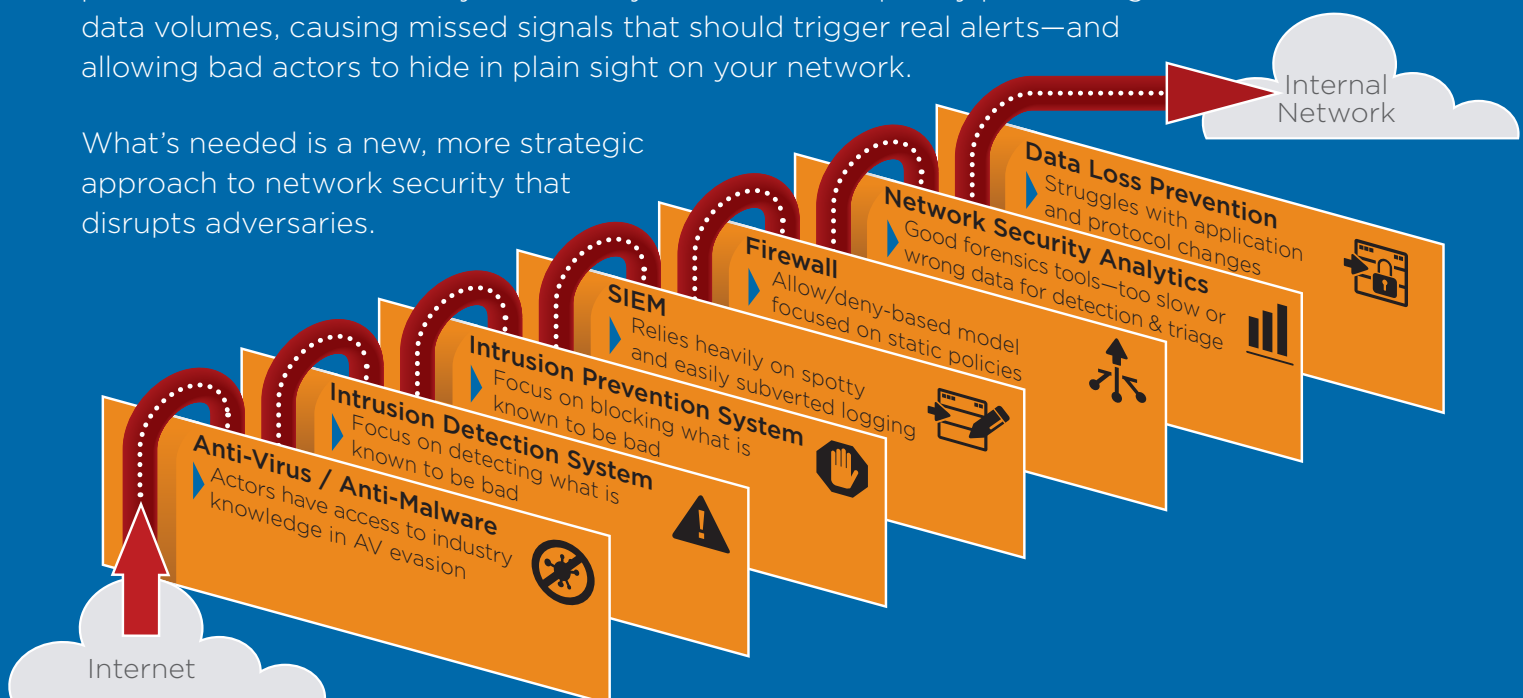
Near Real-Time Network Security Visibility and Awareness


Together, Teradata and Novetta enable organizations to answer the most critical questions about network traffic and advanced persistent threats—in near real-time. Designed with speed and scale in mind, intelligent and selective metadata extraction captures the optimal amount of data for analysis with query responses and full-packet drill-down requests measured in seconds. Instead of wrangling with too much data or struggling with not enough, security analysts now ask and answer subtle questions at the speed of thought—reducing incident response times on suspicious behavior across the entire network from days to hours, or even minutes.

Current Approaches

A conventional layered defense strategy consists of intricately instrumented networks and, as a result, can generate a high volume of false positive alerts that overwhelm security professionals. Traditional cyber security tools can't adequately process high network data volumes, causing missed signals that should trigger real alerts—and allowing bad actors to hide in plain sight on your network.

What's needed is a new, more strategic approach to network security that disrupts adversaries.





The most valuable assets in the fight against adversaries are the talented cyber security analysts who operate the security tools in your organization. They need to be able to respond to the right incidents, at the right time—and at the right speed and scale—or they will not be successful in defending the network. The good news is, with the right tools, cyber security analysts can harness data from your network to identify and defeat the real cyber security threats.

Using Conventional Tools

A cyber analyst is tasked with performing proactive and reactive threat detection. Proactive analysis may include information from an organization's computer emergency response team (CERT), then reviewing known threats to determine relevance. Assuming a threat is credible, the analyst then determines the level of risk and whether it warrants action. If yes, steps are taken to remediate the problem. A reactive threat analysis might include responding to alerts triggered from existing tools or CERT; reviewing data to weed out false positives; determining root cause; then taking steps to remediate. Unfortunately, the entire process can take from several days up to weeks to unfold for

a single incident. Because no one tool provides a complete or truthful picture, the analyst spends most of their time wrangling data from multiple systems. And once complete, it is rare that an analysis yields confident results—as there is just too much that is left unknown.

Using Advanced Strategies and Tactics

Combining big data analytics with security technologies provides a complete picture. Integration of data sources—especially the ground truth: network traffic—offers the ability to answer crucial discovery questions almost immediately. This allows analysts to ask deep, intuitive, and iterative questions without resorting to writing

Approach with Novetta Cyber Analytics | How do analysts now detect what other solutions miss?



The Teradata approach provides an ideal, powerful combination of cyber data and analytics that gets results.

custom, time-consuming code, or spending hours to days wrangling data from multiple systems for a single incident.

Learn more about how advanced Novetta Cyber Analytics assist network hunters in identifying cyber threats, and why it maps so well to the Teradata platform. **Check out the Cybersecurity: Move Beyond the Buzzwords podcast** with Peter LaMontagne, CEO of Novetta Solutions and consultant Ron Powell.

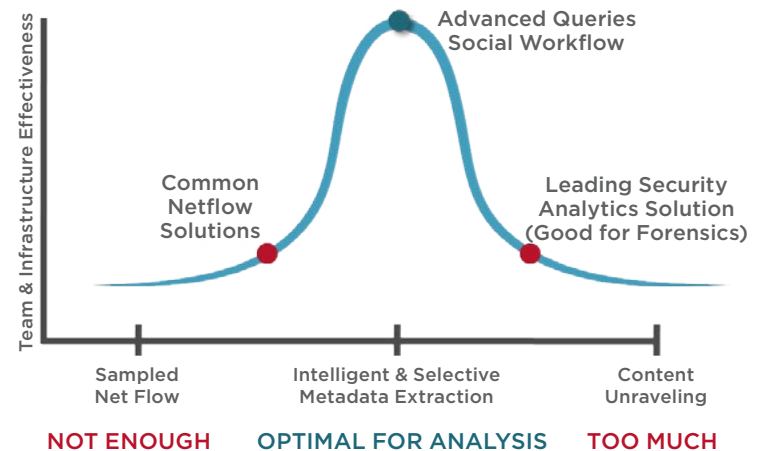
Your Data and Business Reputation: Worth Protecting

Big data analytics combined with today's security technologies hold real opportunities to create big security analytics for a stronger, proactive cyber defense posture.

We Can Help You Do More

Discover how big data, security technologies, and highly-skilled cyber security experts can help you do more to safeguard sensitive information and protect your organization from cyber-attacks. To learn more about Teradata Cyber Defense Solutions—and how we can help assess your areas of potential risk—contact us today to arrange a no-cost, no-obligation consultation.

Novetta Cyber Analytics



Teradata Cyber Defense Solutions



Sam Harris
Director of Cyber Security
and Enterprise Risk
Management Solutions
1-919-341-2463

sam (dot) harris (at) Teradata (dot) com

 www.linkedin.com/in/samharris

Cyber Security Resources

For additional information on cyber security, be sure to explore the resource links below and throughout this document, or visit **Teradata.com/cybersecurity**.

Industry Research and Expert Perspective on Cyber Security

Ponemon Institute “Big Data Analytics in Cyber Defense” Survey

Ponemon Infographic

Public CIO Special Report: New Threats, New Tactics

Defending Data with Larry Ponemon

New Insights on Winning the Cyber War

Q&A with Information Security Systems Expert Sam Harris

Teradata Unified Data Architecture for Big Data Analytics for Cyber Security

Teradata Unified Data Architecture

Technology and Solutions

Big Data and Government: Business Drivers and Best Practices

When Big Data Meets Cyber Defense, Enterprises Win

Big Data Analytics: A New Way Forward for Optimizing Cyber Defense

The Threat Beneath the Surface: Big Data Analytics, Big Security and Real-Time Cyber Threat Response for Federal Agencies

The Threat Beneath the Surface: Cyber Security Executive Summary

Cybersecurity: Move Beyond the Buzzwords

10000 Innovation Drive, Dayton, OH 45342 **Teradata.com** US and Canada: 1-866-548-8348 International: 1-937-242-4030

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 © 2014 by Teradata Corporation All Rights Reserved. Produced in U.S.A.

10.14 EB8528



TERADATA