Hewlett Packard Enterprise | Booz | Allen | Hamilton

Business white paper

Data-centric protection: enabling business agility while protecting data assets

Table of contents

Vulnerabilities abound in data-driven enterprises

Corporate, government, and other enterprises are under relentless attack by cyber criminals determined to steal business-critical data and confidential customer and third-party information. Whether for the purpose of identity theft, corporate espionage, or other malicious ends, hordes of hackers running the gamut from organized crime groups to sovereign government organizations are working around the clock, around the globe to penetrate datastores in virtually every industry sector.

Year after year, organizations have struggled to thwart these criminals and the existential risks they pose to business enterprises. Yet, vulnerabilities continue to abound and the associated attacks are more pervasive, more sophisticated, and more damaging than ever. And, that damage can affect an organization's reputation, bottom line, and impact business success for years.

The incidence of data breaches and thefts is mind-boggling. Consider the following:

- From 2005 to 2014, there have been 5,029 reported data breaches (many more go unreported). In 2014 alone, there were 783 reported data breaches in the U.S. a 27.5% increase over 2013.[1]
- A single data breach, such as the Experian ID theft[2] or the Target breach,[3] can expose and compromise millions to hundreds of millions of confidential records.
- Globally, there are an estimated 556 million cyber crime victims per year.[4]
- Many data thefts can and do go on undetected for years.[5]
- Endpoint protection solutions and even many fairly sophisticated data protection solutions have lost their effectiveness[6] over time.

As the following diagram dramatically illustrates, there are more perpetrators, with more capabilities, using more attack vectors to accomplish their criminal aims than was once imaginable. These folks are tireless, agile, and smart.

[1] ITRC Breach Statistics 2005–2014, **idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html**

[2] **krebsonsecurity.com/2014/03/experian-lapse-allowed-id-theft-service-to-access-200-million-consumer-records**

[3] **krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers**

[4] **go-gulf.com/blog/cyber-crime**

[5] **usa.gov/identity-theft**

[6] **blog.esg-global.com/endpoint-security-market-transformation-in-2014**

scmagazine.com/10-minutes-on-rethink-your-endpoint-security-strategy/article/208390

Keys to an effective data-centric program implementation

Cyber-solution blueprinting
Many organizations start building cyber security programs via extensive technology spending. Often this is supplemented by hiring staff with varying backgrounds and skill sets. While this bottom-up approach to developing a capability can be effective over the longer term, most often it results in significant overspend both on technology solutions, vendors/solution providers, and staff. With no overarching strategy, it is extremely difficult to hire the right people and deploy the right solutions for your cyber security challenges.

Data-centric data protection approach
A data-centric data protection approach calls for de-identifying the data as close to its source as possible, replacing the sensitive data elements with usable, yet de-identified, equivalents that retain their format, behavior, and meaning. This protected form of the data can then be used in subsequent applications, analytic engines, data transfers, and datastores. In other words, the data de-identification process removes or obscures any personally identifiable information from enterprise data so that should a data breach occur, the "data" obtained by the perpetrator(s) will be useless. This approach effectively neutralizes data breaches.

Figure 1: Complexity of cyber attacks continues to increase exponentially; the need for a robust data protection program has never been greater.

Feeling nervous yet? Well, there's more

- According to one recent survey, an estimated 47% of organizations reported suffering at least one cyber attack during the past year. More shocking is the fact that 13% of those surveyed said they didn't know whether they had been attacked!
- Enterprises have grown increasingly borderless due to disaggregated supply chains, and outsourcing and mobile workforces; data is less centralized than ever before.
- Cyber threats don't just originate outside of enterprises, but from inside as well. In fact, approximately 50% of all data breach incidents are sparked by insiders. Organizations should assume cyber criminals have already breached their perimeter defenses.
- Companies that fall victim to cyber attacks not only suffer the initial costs and damages, but continue to experience negative impacts including damage to their reputation, customer churn, and various other hard costs for years after the incident.

It's become clear that implementing basic security controls and traditional security techniques is not enough to prevent data breaches. New approaches to managing risk and neutralizing breaches, while at the same time enabling businesses to operate with the agility required in today's business environments, are required.

Ironically, organizations' successes in harnessing innovative technology to create competitive advantage and drive business growth are often also at the heart of their security problems. IT infrastructures were designed to enable organizations to communicate and collaborate more efficiently—not to keep people out. It's important to keep this in mind when tackling data security challenges because as much as organizations must protect their data, they must also make sure it's available to serve their businesses and continue to drive their growth.

The good news is that companies today can protect critical data through the implementation of well-designed, tested, and proven data-centric protection programs, customized to their unique business requirements and risk profiles.

Additional questions to ask at the outset

- How have you classified your data?
- Is it tagged?
- Is there metadata associated with it that will identify it when it's crawled by a DLP solution or when somebody else opens up that data?
- How do you need to use your business-critical data (e.g., to process transactions, deliver customer service, perform market and customer analytics, etc.)?
- Where is all of your data being stored and used?
- Do you have clearly defined policies and rules in place to govern the handling, processing, and storage of data?
- Do you have a comprehensive knowledge of everyone who has access to your sensitive data?

Cyber-solution blueprinting benefits

- Provides holistic view of the challenges and solution options
- Proven more efficient than ad hoc approaches
- Enables intelligent and planned use of your existing technology infrastructure
- Articulates clearly defined program processes
- Ensures use of best-of-breed technology
- Reduces overall program costs

A successful data protection program begins with questions

Presented with the preceding statistics, the urge might be to build the IT equivalent of thicker and stronger castle walls, deeper and wider moats, and lock down every bit of data. Of course, completely locking down and preventing all access to data would make it impossible to run your business.

Given that you can't count on stopping cyber criminals at the boundary of your organization, you need to focus specifically on protecting your data. That means protecting your sensitive data at the point of origination and throughout its lifecycle, wherever it is being stored, moved, and used. This approach is called data-centric security.

To implement data-centric security, while simultaneously empowering your business to compete and win in today's nanosecond world, you need to understand your data flows and your business needs from your data. Begin by answering some important questions:

- What does your organization need from your data in order to extract the maximum business value and gain a competitive advantage?
- What opportunities might be leveraged by improving the security posture of the data?
- What risks exist based upon your current security posture? What would the impact of a data breach be on the organization? Be specific!
- Have you clearly defined which data (both structured and unstructured) residing across your extended enterprise is most important to your business? Where is it?
- What people, processes, and technology are currently employed to protect your business sensitive information?
- Who in your organization requires access to data and for what specific purposes?
- What time constraints exist upon the organization that might affect the technical infrastructure?
- What must you do to comply with the myriad government and industry regulations relevant to your business?

Finally, ask yourself what a successful data-centric protection program should look like in your organization. What's most appropriate for your organization?

The answers to these and other related questions would provide you with a clearer picture of your enterprise's "data attack surface," which in turn will provide you with a well-documented risk profile. By answering these questions and thinking holistically about where your data is, how it's being used, and by whom, you'll be well positioned to design and implement a robust, business-enabling data-centric protection plan that is tailored to the unique requirements of your organization.

Creating the blueprint

Based on hundreds of client engagements to design and deploy data-centric protection frameworks and programs, Booz Allen Hamilton has found its assessment and diagnostic process—a process called cyber-solution blueprinting—invaluable in jump-starting the design and implementation of customized data-centric protection solutions that match organizations' operational needs, commercial requirements, and the realities of their business environments.

This cyber-solution blueprinting process also significantly reduces development time and expense. Solution blueprints include four key elements, which are illustrated below. These elements then drive program development and implementation.

HPE Security - Data Security data-centric technologies at-a-glance

HPE Security - Data Security provides its data-centric protection through its HPE SecureData solution. The key components of this solution are:

- HPE Format-Preserving Encryption (HPE FPE) is a fundamentally new approach to encrypting structured data, such as credit card or Social Security numbers. HPE FPE makes it possible to integrate data-level encryption into legacy business application frameworks that were previously difficult or impossible to address. It uses a published encryption method with an existing, proven algorithm to encrypt data in a way that does not alter the data format. The result is a strong encryption scheme that allows for encryption with minimal modifications to the way that existing applications work. HPE FPE is a mode of AES, recognized by NIST (see NIST SP-800-38G).
- HPE Secure Stateless Tokenization (HPE SST) is an advanced, patent-pending data security technology that provides enterprises, merchants and payment processors with a new approach to help assure protection for payment card data, with significant Payment Card Industry Data Security Standard (PCI DSS) audit scope reduction. HPE SST technology dramatically improves speed, scalability, security, and manageability over conventional and first-generation tokenization solutions. And it does so while eliminating the need to build and maintain token databases and all of the cost and complexity that goes along with such traditional token databases.
- HPE Page-Integrated Encryption (HPE PIE) encrypts sensitive user data in the browser and allows that data to travel encrypted through intermediate application tiers. Unlike traditional TLS/SSL encryption, this keeps user data private as it travels through load balancers and Web application stacks, only decrypting that data when it reaches secured inner host systems. PIE encrypts data with host-supplied single use keys, making a breach of a user browser session useless to decrypting any other data in the system.

These technologies can be used individually or in combination to provide highly scalable, high-performance data de-identification that is standards based and that has been proven effective in many demanding real-world situations.

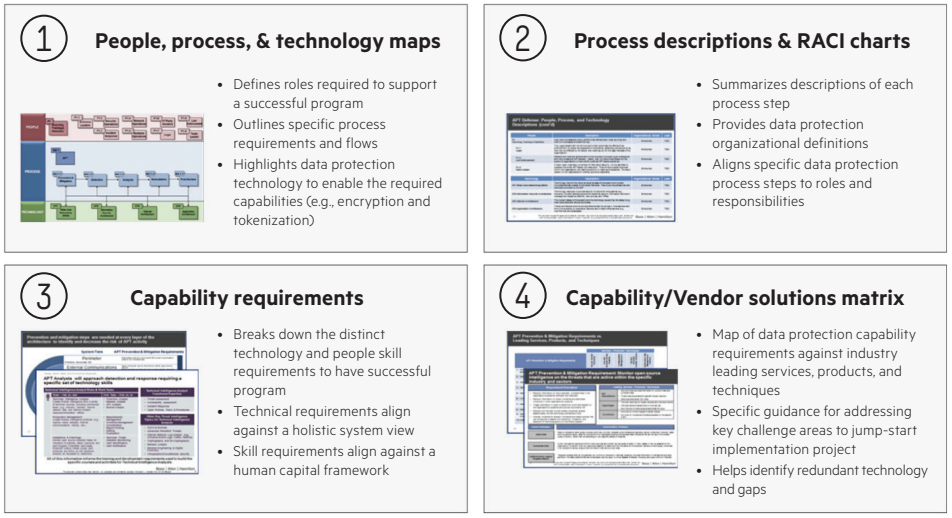

Figure 2: Cyber-solution blueprinting process.

Why implement data-centric protection

Organizations typically employ a layered approach to prevent access to their enterprises and to protect their data. However, even using such a layered approach involving various point solutions, security gaps remain that can be exploited by cyber-criminals. It's quite common for organizations to feel confident that they are well protected, only to be rudely disabused of that notion by a clever, industrious crook.

That's why Booz Allen Hamilton and HPE Security - Data Security have developed and strongly advocate a different approach—a data-centric, data de-identifying approach to data security that enables you to protect data over its entire lifecycle—from the point at which it's captured, throughout its movement across your extended enterprise, all without exposing live information to high-risk, high-threat environments. That's the essence of data-centric security. HPE SecureData solutions, including HPE Format-Preserving Encryption (FPE) and HPE Secure Stateless Tokenization (SST), protect sensitive data as soon as it is acquired and ensures that it is always used, transferred, and stored in protected form. It effectively "de-identifies" data, rendering it useless to attackers, while maintaining its usability and usefulness—its referential integrity—for authorized production and non-production data processes, applications, and services.

Data de-Identification with HPE SecureData quite literally neutralizes data breaches by making your protected data absolutely worthless to an attacker.

Name	SS #	Credit Card #	Street Address	Customer ID
James Potter	385-12-1199	37123 456789 01001	1279 Farland Avenue	G8199143
Ryan Johnson	857-64-4190	5587 0806 2212 0139	111 Grant Street	S3626248
Carrie Young	761-58-6733	5348 9261 0695 2829	4513 Cambridge Court	B0191348
Brent Warner	604-41-6687	4929 4358 7398 4379	1984 Middleville Road	G8888767
Anna Berman	416-03-4226	4556 2525 1285 1830	2893 Hamilton Drive	S9298273

FPE FPE SST FPE FPE

Name	SS#	Credit Card #	Street Address	Customer ID
Kwfdv Cqvzgk	161-82-1292	37123 786354 51001	2890 Ykzbpol Clpppn	S7202483
Veks lounrfo	200-79-7127	5587 0856 7634 0139	406 Cmxto Osfalu	B0928254
Pdnme Wntob	095-52-8683	5348 9209 2367 2829	1498 Zejojtbbx pqkag	G8265029
Eskfw Gzhqlv	178-17-8353	4929 4333 0934 4379	8261 Saicbmeayqw Yotv	G3951257
Jsfk Tbluhm	525-25-2125	4556 2545 6223 1830	8412 Wbbhalhs Ueyzg	B662594

This is an illustration of HPE FPE and HPE SST in use. Note how HPE FPE encrypts the original data without changing the format. HPE SST tokenizes data without the need to build and maintain a token database.

Figure 3: HPE SecureData-data-centric protection with HPE FPE and HPE SST.

Data-centric protection in the real world

Let's take a look at several quite real and quite demanding situations in which these technologies are in use.

Live production data
Protecting live production data is both an obvious imperative and, perhaps, the very definition of mission-critical.

You may have transaction information, for example, that's being captured in a mainframe environment. You want to encrypt that data in a very simple way so you can protect it even as it moves out and into other types of systems—perhaps various Oracle databases for departmental use, or into Hadoop for Big Data analytics, or into the cloud for outsourcing of testing, application development. The data likely contains at least some sensitive data—it may be personally identifiable customer information (e.g., credit card numbers, Social Security numbers, etc.) as well as external, third-party data, perhaps HIPAA regulated data.

Consider the example of a global insurance company that wants to reduce its cost of application development. The company needs to provide its offshore vendor with realistic data in order to do this development work. But it cannot afford to risk providing the vendor with the actual data that application is being developed for. Using HPE SecureData technology, the company can provide the vendor with realistically formatted data that has been completely de-identified. In that way, it can achieve its development cost reduction goal without jeopardizing its live production data.

Or the company may want to do various types of analytics on broad data sets consisting of hundreds of millions of records. In such a case it would extract data from traditional highly trusted data-warehouse environments and move and merge those data sets into low-cost Hadoop ecosystems, you'd also be exposing the data to other downstream systems and tools like Greenplum or DataMirror via ETL tools. Again, protecting the live data requires that it be de-identified, prior to being moved out of the trusted data warehouse environments. Additionally, you might also want to be able to reverse the process after the analytics are performed. HPE SecureData technology provides the ability to analyze the data in a protected form and then under very tight policy control, be returned to its original form once back in the warehouse. This kind of flexible, data-centric protection is extremely valuable and is employed in many organizations.

High-performance Hadoop data de-identification
While many times organizations have the luxury of being able to stage the de-identification process, in other instances the de-identification must be done on the fly.

For instance, a global communications company needs to routinely analyze several hundred million customer records to detect patterns to provide the intelligence needed for retail optimization and other business activities.

Similarly, a healthcare innovator wanted to do real-time analysis of pharmaceutical, healthcare, and third-party data to provide the information and insights it needed to create and offer new, high value services to medical networks.

In these instances, the organizations used HPE SecureData technologies to de-identify event-driven data from multiple sources in real time in order to accomplish their extraordinarily demanding business objectives, while fully protecting sensitive personal, financial, and healthcare data.

Protecting data in the cloud

As organizations extend their enterprises to the cloud—using both public and private clouds—as part of their efforts to reduce costs, all sorts of data protection red flags begin waving. They may be extending their enterprises to the cloud for storage, to run applications such as fraud detection or perform various analytics. The cloud does provide a low-cost environment in which to operate, but that benefit is accompanied by significant data security risks. It's easy enough to send a continuum of data up into cloud platforms like Azure or AWS, but not so easy to exert the level of control over these environments that you can in your own data centers.

For instance, one global finance firm moved its customer data analysis to Azure workloads in order to cut per application costs by 40%. Another organization, a global investment bank, created a private cloud stack to enable it to deliver new services more rapidly. The data being moved to the cloud included CRM, payment card industry (PCI), and other personally identifiable information. These organizations felt confident in making these moves thanks to the business-enabling power of HPE SecureData data de-identification technology.

Protecting sensitive data in test and development environments

Generating data for test and development environments presents serious challenges for enterprise security and risk management. When data is copied from production databases and used directly for application development, large volumes of private data accumulate on unprotected servers and workstations. The use of outsourced and offshore QA and development services further increases the risks and costs of data leakage—potentially resulting in damages affecting reputation, compliance, and revenues.

A nonprofit financial services company that provides financing to rural electric cooperatives in the U.S. faced just this challenge. To reduce the application development and testing costs for a new Web application, the organization decided to offshore the project. It needed, however, to provide the offshore contractor with realistic data for use in development and testing, but not the actual, confidential data, which if stolen, could wreak havoc with the organization's reputation, member relationships, and survival. By using HPE SecureData with HPE FPE, it was able to meet its tight deadline for this offshore project, reduce its application development costs, effectively neutralize data breaches, ensure the security of its sensitive data, and maintain the confidence of its members.

Business empowerment and solid data protection: you can have both

As discussed earlier, security approaches that have attempted to prevent cyber criminals from accessing enterprise data have been less than fully effective. That does not mean you should abandon network security, of course. It's just that you can't rely solely on perimeter defenses to protect your invaluable data assets.

Only by employing a data-centric data protection approach, can you truly reduce your risk profile and render attacks on your data pointless and worthless. By de-identifying critical data throughout its entire lifecycle, you can neutralize data breaches while retaining your data's referential integrity and usability. Most important, implementing a data-centric program does not hamper your organization's ability to access, move, analyze, and use your data to enable business success.

BAH contacts

Stephen Coraggio
Principal
corragio_stephen@bah.com
917-305-8004

Chris White
Senior Associate
white_chris@bah.com
517-524-7175

The unique cyber-solution blueprinting and data de-identification processes described in this white paper—beginning with an enterprise risk assessment, then the development of a cyber-solution blueprint, and the implementation of HPE SecureData data de-identification solutions have proven effective in numerous extremely challenging situations and environments. They provide consistent, robust data protection while also protecting organizations' access to the information they rely upon to run and grow their businesses. And they do this without you having to embark on a lengthy and horrendously expensive project.

In fact, they produce significant cost savings while providing the business with the information it needs to glean critical insights that can lead to formidable growth and enhanced customer loyalty.

To learn how this approach to data protection can allow your organization to deploy your data where, when, and to whom it needs to be deployed while keeping it fully protected visit **voltage.com** and/or contact BAH. For details of the contacts, see left sidebar.

About Booz Allen Hamilton
Booz Allen Hamilton has been at the forefront of strategy and technology for more than 100 years. Today, the firm provides management and technology consulting and engineering services to leading Fortune 500 corporations, governments, and not-for-profits across the globe. Booz Allen partners with public and private sector clients to solve their most difficult challenges through a combination of consulting, analytics, mission operations, technology, systems delivery, cybersecurity, engineering, and innovation expertise.

With international headquarters in McLean, Virginia, the firm employs more than 22,500 people globally, and had revenue of $5.27 billion for the 12 months ended 31 March 2015. To learn more, visit **boozallen.com** (NYSE: BAH).

About HPE Security - Data Security
HPE Security - Data Security drives leadership in data-centric security and encryption solutions. With over 80 patents and 51 years of experience, we protect the world's largest brands and neutralize breach impact by securing sensitive data-at-rest, in use, and in motion. Our solutions provide advanced encryption, tokenization, and key management that protect sensitive data across enterprise applications, data processing infrastructure, cloud, payments ecosystems, mission-critical transactions, storage, and Big Data platforms. HPE Security - Data Security solves one of the industry's biggest challenges: simplifying the protection of sensitive data in even the most complex use cases. For more information, visit **voltage.com**.

Learn more at
voltage.com
hpe.com/software/DataSecurity

Sign up for updates

★ Rate this document

4AA6-3915ENW, May 2016

Hewlett Packard Enterprise | Booz | Allen | Hamilton