IONIC SECURITY

# 9 REALITIES OF PORTABLE AND PERSISTENT DATA PROTECTION IN THE 21ST CENTURY

# INTRODUCTION

***Over the past decade, major data breaches have made headlines, resulting in significant brand damage, costly fines, and exposed social security numbers (SSNs) as well as lost or stolen Personally Identifiable Information (PII) and intellectual property.***

Sophisticated cyber criminals are pros at stealing data and lurk in enterprise networks for months, even years, until they are found, but at that point, much of the damage is already done. When these breaches are discovered, enterprises hire expensive forensics analysts and incident response teams to clean up the breach and return systems to normal. Additionally, for further peace of mind, they'll continue adding more layered defenses and perimeter security technologies that promise to keep them secure. Unfortunately, as we've seen, these technologies will likely fail at some point and this vicious cycle will continue.

To make matters more complex, with the appearance and adoption of new technologies like social, mobile, analytics, Bring Your Own Device (BYOD) and cloud, the perimeter has crumbled. Despite investments in incremental security technologies, valuable enterprise information and data are still leaving the enterprise. As a result, data breaches occur with a detrimental impact on the enterprise and its ability to conduct business.

But what if the stolen data was useless and meaningless to cyber criminals: a world where valuable enterprise information and data could be shared safely and effectively with the right individuals and organizations, under the right context? A world where enterprises could take full advantage of business productivity tools, knowing their data remained safe and secure. What if our world was fearless? What if that was our world…today?

How a Portable and Persistent Data Protection Model Can

# ENABLE YOUR BUSINESS

That fearless world is built by implementing a Portable and Persistent Data Protection model. Enterprises must start securing data at the point of creation and use. By attaching visibility, control and protection to the data at the moment it is created, enterprises enable full control of the data during its entire lifecycle – from data inception to death.

When enterprises have complete visibility and context of who is attempting to access their information, they can control, enable, or revoke access to information based on relevant context in real time. When enterprises can control their most sensitive information and data at any time, no matter where the data resides, an enterprise's biggest fears are removed from the business making process.

Once a Portable and Persistent Data Protection model is adopted, enterprises can fearlessly embrace new, innovative collaboration tools that can enhance their business. With the accelerating adoption of technologies like cloud computing, social media, SaaS applications, data analytics, and mobile devices, fearless enterprises make use of these technologies to drive innovation, consolidate technologies and reduce costs. Enabling technologies let enterprises create new offerings and business models and collaborate with customers and partners much more effectively. Enterprises that aren't able to adopt these technologies due to compliance or business risk, due to the sensitivity of their information and data, risk falling behind their competitors who can.

*we create*
***2.5 Quintillion***
*bytes of data per day*
*and that the amount of data* ***doubles*** *every two years*

# REALITY 1

## The Variety, Volume, and Velocity of Data Being Created and Replicated and Shared Across all Types of Endpoints is Exploding

With billions of Internet users across the globe, big data is exploding. Data is created and consumed at a pace never seen before and the market for big data solutions keeps on growing. In fact, recent research claims that we create 2.5 Quintillion bytes of data per day and that the amount of data doubles every two years.

The term "big data" describes datasets whose size is immeasurable – data that is too big for traditional databases to capture, store, manage and analyze. Today, data sources come from everywhere including mobile devices, apps, log files, the web, social media and more. In fact, according to the *2014 Data Never Sleeps 2.0* infographic, every minute:

- Facebook users share nearly ***2.5 million pieces of content.***
- Twitter users tweet nearly ***300,000 times.***
- Instagram users post nearly ***220,000 new photos.***
- YouTube users upload ***72 hours of new video content.***
- Apple users download ***nearly 50,000 apps.***
- Email users send over ***200 million messages.***
- Amazon generates over ***$80,000 in online sales.***

The velocity at which data is produced makes it difficult for organizations to connect and aggregate data in a meaningful way – they don't have the right platforms or people to manage the data and feel like they are losing revenue opportunities.

In fact, a recent report stated that ***93% of executives believe they are losing revenue by not leveraging available data properly.*** Managing and securing big data in the enterprise is often difficult because it is fragmented and spread across multiple data owners and functions – IT, engineering, finance, sales, etc. Applying a Portable and Persistent Data Protection model to this new reality enables an infrastructure that can scale with this type of growth and enables the business to participate in these new revenue opportunities.

# REALITY 2

## The Borderless Enterprise is Here to Stay

Managing distributed data within the borderless enterprise is one of the enterprise's biggest challenges today. With the advent of software-defined networks (SDN), server virtualization, cloud computing, social media, and mobile networks, the network perimeter has dissolved. All that's left is dispersed data out of IT's control.

There are many benefits that borderless enterprises have, such as better recruiting and retention of talented employees, but still ***75% of companies are deterred from becoming borderless enterprises because of the lack of security.*** With employees increasingly being mobile and using third-party infrastructures for telecommuting, IT no longer has the ability to manage where data goes or who has access to it. IDC reported that by 2015, the world's mobile worker population would reach 1.3 billion or 37.2% of the total workforce – and those numbers continue to rise.

In a borderless enterprise, business operations teams, sales, marketing, human resources and other lines of business can easily procure and implement their own applications, often without IT involvement, opening new doors for many security threats. End users purposefully bypass traditional IT processes, downloading applications onto their mobile devices from third-party infrastructure, creating less visibility and more headaches for IT and security departments.

For borderless enterprises to effectively protect distributed data across all virtual pathways, security will need to be embedded into the enterprise architecture. They need a new cybersecurity framework and a corresponding data protection model that can serve as a guide to implementing cybersecurity strategy and policies in a manner that ensures a consistent, well-integrated and cost-effective approach.

# REALITY 3

## Cloud Services May Equal Cost Savings, But Insecure Data Will Cost You More

The adoption of cloud computing promises major benefits for enterprises including anywhere, anytime access for the growing mobile workforce, reduced IT costs and a more agile workforce who can embrace enterprise applications like never before. It has been reported that by 2016, 100% of the Global 2000 will penetrate the cloud and take advantage of Software as a Service (SaaS) and Platform as a Service (PaaS) delivery models.

However, security still remains one of the number one concerns with cloud adoption, even as vendors have stepped up more recently to address performance, integration, compliance, and security concerns. The Ponemon Institute estimates the cost for an average U.S. organization to remediate from a data breach is $8.9 million, up 6% from 2011. Enterprises need to weigh the cost benefits of cloud computing versus the risks to determine what is best for the business to conduct operations securely, cost-effectively and efficiently. In the end, a data breach that results from insecure data moving to and from the cloud and everywhere in between poses an even greater risk and cost to the enterprise, including irreparable brand damage.

*The Ponemon Institute estimates the cost for an average U.S. organization to remediate from a data breach is **$8.9 million,** up 6% from 2011.*

# REALITY 4

## SMAC is Here to Stay

The emergence of SMAC or Social, Mobile, (big data) Analytics and Cloud has been a game changer for many enterprises who offer "anywhere, anytime" work environments. Commonly known as the SMAC stack, it refers to the growth of these tools and platforms in business technology stacks. SMAC will play a major role in the future of IT and will be a key driver of IT investments with connectivity at the center of it all, driving everything.

SMAC enables dispersed global workforces to easily collaborate on projects, share files, and reach beyond the boundaries of the traditional four walls of an office space. Enterprise mobility – the ability of an enterprise to connect to people and control assets from any location – is quickly becoming the norm for many companies. Why is that? A recent study found that 63% of enterprises are adopting enterprise mobility for cost savings, 51% are adopting it for productivity reasons, 50% are adopting it due to employee requests and needs, and 43% are adopting it for competitive reasons.

While the adoption of SMAC and Enterprise Content Management (ECM) tools has increased, it's also creating new challenges for IT and security departments, as many companies have turned to Box and DropBox for their file-sharing and collaboration needs. Corporate, sensitive data is no longer within the confines of a network that IT can secure, operate and control. The struggle between balancing data security, data availability and enterprise mobility is a hurdle that some enterprises have met head-on by inverting the traditional security model of layered defenses and protecting their distributed data first. This shift in thinking and adoption of enabling data protection technology is allowing them to be agile in an era of SMAC.

**63%**

of enterprises are adopting enterprise mobility for cost savings

**51%**

of enterprises are adopting it for productivity reasons

**50%**

of enterprises are adopting it due to employee requests and needs

**43%**

of enterprises are adopting it for competitive reasons

# REALITY 5

## Data Breaches are Growing in Frequency and Cost

**783** Data Breaches in 2014

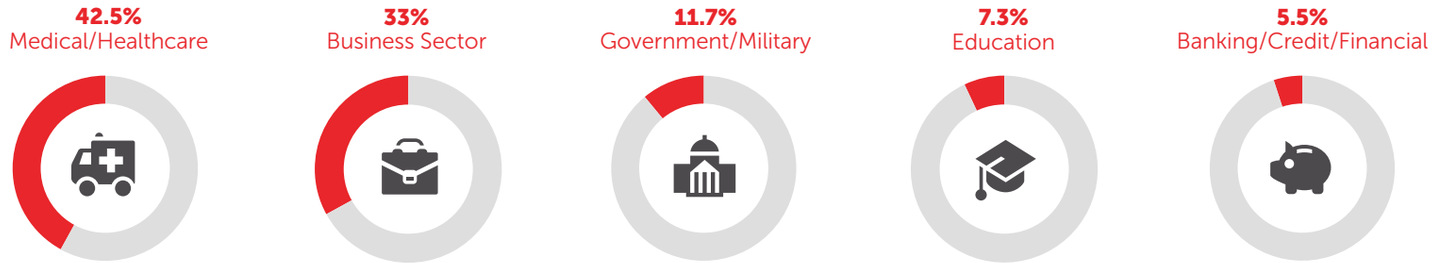
**27.5%**

increase over the number of breaches in 2013

Costly data breaches have impacted nearly every market and enterprises are taking a 'when, not if' attitude about breaches and how they will deal with them when the time comes. According to a recently released report by the Identity Theft Resource Center (ITRC), the number of U.S. data breaches hit a record high of 783 breaches in 2014– a 27.5% increase over the number of breaches reported in 2013. In addition, ITRC reported that 42.5% of breaches identified in 2014 were in the medical/healthcare industry, 33% were in the business sector, 11.7% occurred in the government/military sector, 7.3% occurred in the education market, and 5.5% occurred in the banking/credit and financial markets.

The problem is that many enterprises are not deploying new data security strategies to thwart increasingly sophisticated threats – a 2013 data security survey from SafeNet reported that 95% of security professionals continue to invest in and employ the same security strategies year after year. Furthermore, 59% of respondents also said that if a data breach did occur, high value data would not be safe.

2014 is commonly referred to as the "Year of the Breach" as there was a huge uptick in breaches involving the retail, financial, government and healthcare sectors. With the rise of data breaches naturally comes security concerns surrounding cloud adoption. Recent reports indicate that 63% of enterprises have security concerns with the data in the cloud and 38% are dealing with privacy regulations that prevent data from being stored offsite. What happens when protection is bonded with the enterprises' most sensitive information and data and persists over its lifecycle no matter where it goes? An intrusion no longer equals a breach.




Percentage of Breaches in Different Industries

# REALITY 6

## More and More Data is Shared through Partner Ecosystems

Retail chains, law firms, hospitals, pharmacies, marketing companies, technology providers, banks, and credit unions – the list goes on and on, but what do they all have in common? Every single industry these days relies upon partner and supply chain networks to operate, creating a data supply chain where data passes through several hands before it gets to where it needs to go. From cloud storage providers, to SaaS vendors, to eCommerce platforms and warehouses, to shipping and delivery services, data travels a lot of places during just one single transaction. A good example is an e-Commerce purchase – consider what it takes to go from an online order to payment card processing to shipment and delivery; your personal information and credit card data flows through many places before that product actually ends up in your hands.

***The data supply chain refers to the network of people and businesses that work with your company and have access to your sensitive data.*** This network includes your business partners, vendors, customers, and contractors, and each of them may adhere to different security policies and practices. Each element of the supply chain is a potential area of weakness where sensitive data could be exposed, causing a serious data breach. Shadow IT also creates problems as well. This borderless ecosystem also means that insider threats are no longer limited to threats within your enterprise's network. Now, insiders can be anyone along any part of the supply chain. Further, enterprises are forced to rely on the security measures of each member of the ecosystem to keep all of its information secure – having no control over it once it leaves the enterprise network. With a Portable and Persistent Data Protection model in place, enterprises are learning that an intrusion, whether it is on their network or on the network of a trusted partner and supplier, doesn't have to equate a breach. Their information is still protected, and they can continue moving forward with their business.

# REALITY 7

## Visibility into Data Usage Allows a Better Understanding of Trends and Patterns

A recent Cisco survey revealed that 70% of employees admitted to breaking IT policies with varying regularity.

The importance of visibility has never been greater than today. Understanding what information and data is stored, and where, is a key component of a Portable and Persistent Data Protection model for security. Knowing if data is in the cloud or on an outside network, and which applications are being used and by whom, allows you to identify potential threats more easily.

To help protect against insider theft, accidental exposure, and subcontractor/third party theft, enterprises need the ability to track sensitive data and flag when it has been accessed- even when users bypass the corporate network or VPN and directly access the Internet. Implementing persistent data protection for enterprise information allows identification of the most heavily used applications by client device, location, data context, and operating system, and calls attention to risky behavior or out of norms usage.

Visibility also allows for measuring data security improvements over time. In a Persistent Data Protection model, time-series data from monitoring policies can be used to demonstrate increasing security over time and identify usage outliers.

Leverage complete visibility into:

- Types of devices, operating systems, and browser usage
- Utilization of key web applications
- Geographic location of users and a history of access events with relevant metadata

Persistent Data Protection allows you full visibility into information about your data, where it lives, and who interacts with it. This visibility allows for improved security and simplified threat detection.

Insider theft & accidental exposure follow at just over

**12 PERCENT**

&

Subcontractor/ third party follows at

**11.2 PERCENT**

# REALITY 8

## Control of Data Allows You to Regulate Who Has Access to What Data, When, and Where

Enterprises worry about sensitive data creeping outside of its control with good reason. Whether an employee accidently emails an attachment to someone outside the organization with a mistaken auto-fill, or a partner temporarily stores your customers' PII on an unencrypted drive, threats of data creep are legitimate without even considering malicious attacks. Persistent Data Protection eliminates the worry about data creep because of the levels of control over the data. From the point of creation throughout the data lifecycle, global policies ensure that sensitive data is never shared with unauthorized parties. This assurance is achieved with the control of "who, what, where, when, and how," that controls data access down to the level of individual users or specific devices.

Some of the key benefits of a Portable and Persistent Data Protection Model include:

- Implement and update policies with "one-click" policy updates easily
- Create flexible policy based on data, user, device, application, network and time of day for granular contextual access
- Remotely retire or destroy documents and data without direct access to the file
- Expire access to documents with time based policies to limit exposure to sensitive information
- Control your data

**88%**

*In a 2010 survey, Fujitsu concluded that **88%** of its customers have **significant concerns about data integrity and privacy** in the cloud.*

Remove the worry about data creeping into the wrong hands or on the wrong systems with the knowledge that regardless of what happens to the file itself, the data remains protected and inaccessible to any unauthorized person, place, or device. Maintain compliance by controlling access to business data, regardless of whether it is accessed from a corporate network, directly through 3G/4G wireless, home networks, or Wi-Fi hotspots to maintain compliance and visibility.

# REALITY 9

## Protection of Data at Rest, in Motion, and in Use for Its Lifecycle Keeps You Compliant and Secure

A Portable and Persistent Data Protection model allows you to stay compliant and protect the loss of intellectual property. Enterprises can effectively eliminate reputation damage, fines, breach notifications, or other penalties due to electronic theft of sensitive materials, account compromises, or inappropriate data sharing.

***Because data is protected at the point of creation and stays protected throughout its lifecycle, it remains secure and protected at all times on every endpoint.*** This level of Persistent Data Protection includes the ability to encrypt entire documents or portions of a document based on classification levels, so information can be easily shared across the organization without PII being exposed accidentally. Additionally, if documents are shared beyond the organization's network to an unauthorized user, access to the document is immediately denied. Even restrict access based on geography to comply with data residency laws.

Persistent Data Protection benefits include:

- Encrypt entire documents or portions of a document based on classification levels
- Protect information and data at rest, in use, and in-motion for the lifecycle of the data
- Avoid interrupting user workflows by using transparent encryption that occurs independently
- Protect documents not under your physical control
- Access consistent protection across all endpoints that the information resides on


*Contact Us:*

*Only* **Ionic Security** *provides a unified, scalable distributed data protection platform that lets enterprises protect their most valuable information and data throughout the entire data lifecycle. Contact us to learn how to make your enterprise fearless.*

REQUEST A DEMO

# CONCLUSION

With the explosion of data, the collapse of the perimeter, the rise of the borderless enterprise, and the transition to cloud services, protecting data has become a challenge that paralyzes businesses. The implementation of a Portable and Persistent Data Protection strategy allows companies to be fearless by maintaining control, visibility, and protection of their data all the time, anywhere. The key benefits of a Portable and Persistent Data Protection model are immediate, flexible, and transparent control over sensitive information. Protect the enterprise's most valuable information and data throughout its lifecycle on any network, device, or application, without proxies or gateways or changes in user behavior.

When enterprises have complete visibility and context of who is attempting to access their information, they can control, enable or revoke access based on relevant context in real time. When an enterprise controls its most sensitive information and data at any time, no matter where the data resides, the enterprise is enabled, and becomes fearless.

IONIC SECURITY

WWW.IONICSECURITY.COM