



# Data-Centric Security

New imperatives for a new age of data



# Out-maneuvered, outnumbered, outgunned

Things are not going well. The phones have gotten smarter, the data's gotten bigger, and your teams and customers have spread out to the four corners of the planet. It's everything the enterprise could have dreamed of... with one small exception – no one can be sure the data is secure.

Because while the datascape has evolved, expanded and exploded at the speed of light, the architecture to secure all that data hasn't been able to keep up.



## And the results have not been pretty. In the last two years alone:

Ebay – 145,000,000 records lost.

Target – 70,000,000 records lost.

Adobe – 152,000,000 records lost.

Evernote – 50,000,000 records lost<sup>1</sup>.

Turns out, the hackers have gotten smarter, the breaches have gotten bigger, and the threats are coming in from all directions. Meanwhile, the organizations responsible for all this data have been scrambling to keep up.

In the sheer chaos of secured and unsecured data zipping between borders and policies, it's starting to become clear: existing network-based data security architectures that focus on the perimeter are no longer up to scratch. It's not that there are more chinks in the firewall. It's the perfect storm of bad guys getting better, data migrating farther, and the fact that data no longer lives behind the firewall.

Today, more data moves quicker, farther and between more sources and targets running on completely different technology landscapes than ever before. Which has meant the threats and challenges have multiplied beyond the capabilities of existing data security.



It's time for an update.

# Why you're in trouble

## The limitations of the current data security model and mindset

The existing data security architecture was built on the presumption that data will live in a data center and be consumed on premise. It presumes that the data is small, constantly monitored, and usually at rest. And it presumes that remote employees are accessing it by logging onto the corporate network using all the right security controls (which don't always work).

It's about building a perimeter around the data and then fortifying that perimeter.

## Meanwhile, in the real world

In reality, data is pouring out of millions of apps in the cloud and being sent to the billions of mobile devices in your employees' and customers' pockets. Which makes the data anything but small and the challenge to secure it anything but simple. What was once centralized, controlled, and tame is now proliferated, uncontrolled, and completely at risk.

In 2013, there were as many bits of data in the digital universe as there are stars in the physical universe<sup>2</sup>. (And let's not forget that organizations are discovering data far quicker than scientists are discovering stars. Because data is the new gold.)

So no matter how strong the perimeter around the data center, the security it offers is purely theoretical – because it ignores two crucial points:

### 1. It ignores the movement and proliferation of data.

Nothing characterizes the new age of data better than the explosion of new data sources and targets. The widespread adoption of cloud services and mobile technology means organizations are moving data at an exponential rate and in exponential volumes. And none of it is protected by the firewall.

Even worse, it ignores serious questions about compliance. National regulations are wildly different from country to country. So when data moves from the head office in London to the development center in India, it runs the risk of breaking any number of data privacy laws.

### 2. It ignores what's happening inside the perimeter.

When as many as 50% of security breaches can be attributed to people inside the organization<sup>3</sup>, a fortified firewall around the data center is practically useless.

Whether it's through criminal intent, or just plain old human error, the administrators and external contractors inside your perimeter can do serious damage when they have access to all your data.

Importantly, you can't stop them dealing with your data – it's what you hire them for, after all. In effect, your current data security architecture forces you into a position where the more data you deal with, the higher your risk.

## Breaking the vicious cycle

Because it ignores such foundational characteristics of the new datascape, the existing security architecture cannot protect the organization against sophisticated threats coming from increasingly determined attackers. If the enterprise is to break this reactionary cycle of measures and counter measures, it will take a whole new approach to security.





# Data-Centric Security

## A vision of security for the new age of data

The current security architecture has failed so often and so dramatically because it's a reflection of an outdated view of how organizations interact with their data. So if the model is going to be updated, it has to reflect the mindset that data is the living, beating, ever-proliferating lifeblood of the organization.

We call it Data-Centric Security. And we define it this way:

Data-Centric Security protects the data itself – rather than just the endpoints, networks, and applications it moves between.

It means the security moves with the data so the data can move as much as the organization needs it to. So instead of slowing down progress and inhibiting the proliferation of data, security can empower the organization to make the most of its data – wherever it's stored and wherever it's going.



# What Data-Centric Security looks like

To adopt this new approach to data security, companies will have to become very good at four processes that they're just not very good at today. You're going to have to learn how to:

## 1. Know where your sensitive data resides.

Only 16% of organizations today can confidently say they know where their confidential data resides<sup>4</sup>. They might represent a worryingly small minority, but they're also the only ones who'll be able to appropriately profile their data and classify it into different levels of sensitivity.

The ability to connect to, discover, locate, and classify your sensitive data is a critical process. And it needs to be set up so that it's repeatable and agnostic of technology or geography.

## 2. Assess its security posture.

All data is not created equal. In a Data-Centric Security model, you need to determine the level of risk your sensitive or confidential data is subject to. It means always knowing who has access to the data under your watch, what they are doing with it, and what type of security controls you have in place to protect it.

## 3. Protect it.

Data-Centric Security means defining unique rules for different data. At the finest level, it'll mean masking the data for certain users and blocking it entirely for others – but what it will really mean is learning how to apply a rigorous data governance policy that can follow the data no matter where it gets proliferated to.

## 4. Detect infringements.

A Data-Centric Security model means knowing when your data's in a state that is not complying with a policy when it's in breach. Relying on old log files to find out where things went wrong takes far too long. Proactively detecting infringements is critical.



Even though the move to Data-Centric Security can compliment existing measures, it will involve a significant shift in both approach and technology for most organizations.

Fortunately, you can already start doing some fairly basic things to make your security model more data-centric:

### 1. Stop using production data in non-production environments.

When production data isn't persistently masked before being used for testing and training purposes, the risk of that data leaking multiplies. Especially when your testing team is composed of contractors, outsourcers, and off-shorers. Importantly, you can't stop them dealing with your data – it's what you hire them for, after all. In effect, your current data security architecture forces you into a position where the more data you deal with, the higher your risk.

### 2. Prevent unauthorized access to data.

70% of database administrators still have access to all the data. Your Data-Centric Security model can begin with dynamic, role-based masking of data so that your DBAs and external contractors only see what they're authorized to see. Put another way, they only see what they need to see to do their job.

### 3. Monitor access to sensitive data.

Just 41% of organizations currently control access based on role and location<sup>4</sup>. So your first steps towards data centricity should include processes to constantly audit and monitor who has access to sensitive data based on where they are and where the data is. That way, you can automate actions for when the access patterns change to something suspicious.

# The collaboration imperative

## Why data architects and security architects need to start hanging out at the same water cooler

As organizations move to data centricity, a common trend is the shattering of silos. It's because silos – data or departmental – are the leading cause of fragmented views of the truth.

And the shift towards a Data-Centric Security model will bring together two traditionally separated parties – the data architect and the security architect.

Their paths didn't need to cross when the security architect was building impenetrable perimeters around the data architect's work. But with that model being so publicly exposed in this new datascape, they can no longer afford to work without consulting one another.



## Exchanging notes

On the one hand, the security architect will need to develop an appreciation of the flexibility needed for the movement of data in the open enterprise.

On the other hand, the data architect must develop an understanding of what it's going to take to secure all that data, wherever it is. So that security policies can be enforced as data proliferates between apps and users.

The earlier these two leaders can start to build together, the stronger the enterprise's foundation will be.

# Beating the next breach

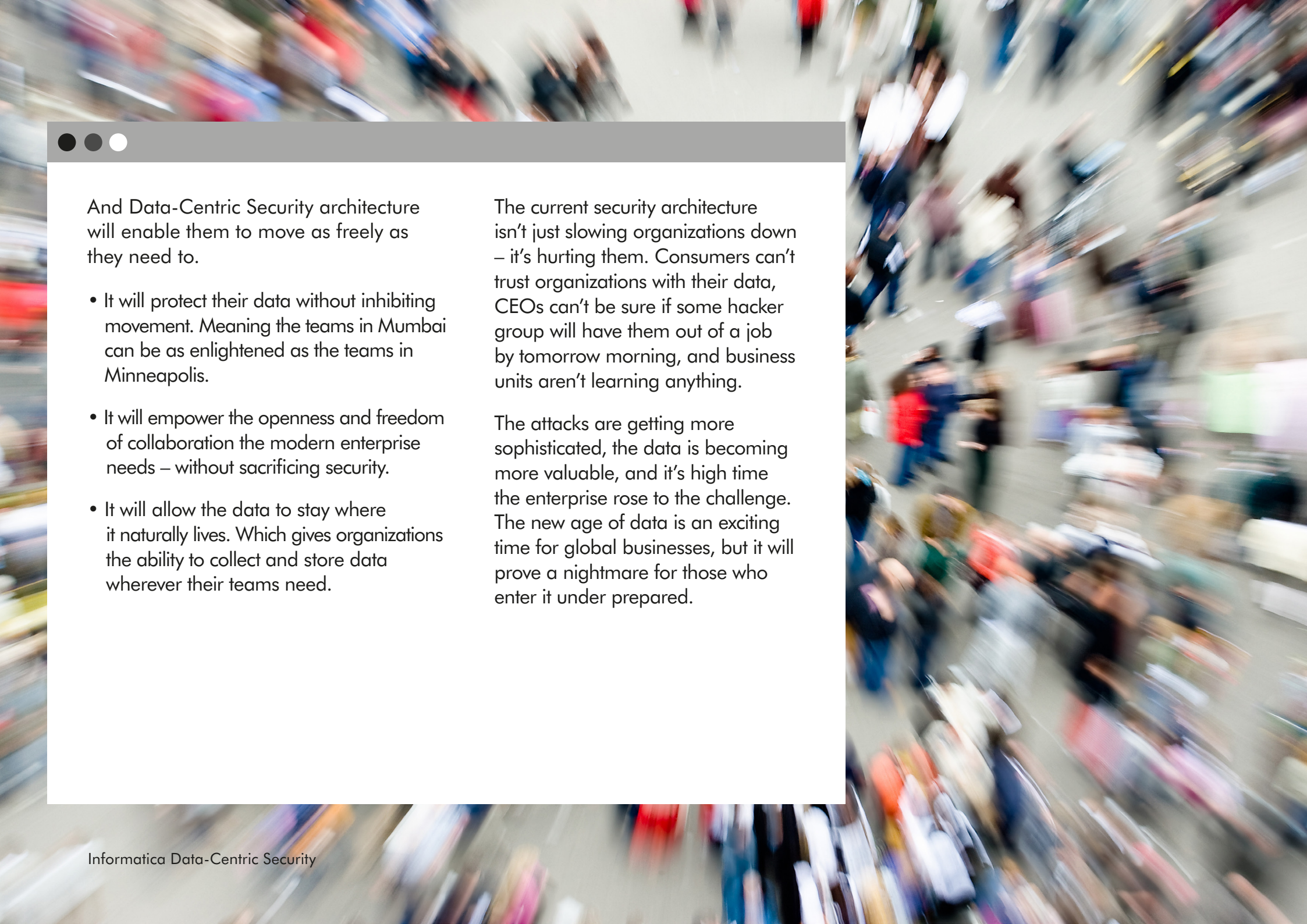
## Why Data-Centric Security matters

The datascape has changed overnight. And it isn't going to slow down.

Organizations will use more sensors, departments will become more mobile, and the fire hose will become ever more intense.

The companies that learn how to handle it without compromising compliance and security will be the ones that dominate this new paradigm.



A blurred, high-angle photograph of a large crowd of people moving through a space, likely a transit station or a busy public area. The motion blur is significant, creating a sense of dynamic activity and movement. The colors are muted and blended together due to the blur.

And Data-Centric Security architecture will enable them to move as freely as they need to.

- It will protect their data without inhibiting movement. Meaning the teams in Mumbai can be as enlightened as the teams in Minneapolis.
- It will empower the openness and freedom of collaboration the modern enterprise needs – without sacrificing security.
- It will allow the data to stay where it naturally lives. Which gives organizations the ability to collect and store data wherever their teams need.

The current security architecture isn't just slowing organizations down – it's hurting them. Consumers can't trust organizations with their data, CEOs can't be sure if some hacker group will have them out of a job by tomorrow morning, and business units aren't learning anything.

The attacks are getting more sophisticated, the data is becoming more valuable, and it's high time the enterprise rose to the challenge. The new age of data is an exciting time for global businesses, but it will prove a nightmare for those who enter it under prepared.



# Sources

1. World's Biggest Data Breaches, Version 1.07, May 2014,  
<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>
2. The Digital Universe of Opportunities, EMC Digital Universe, IDC,  
<http://www.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf>
3. Data Security Statistics, Kroll Cyber Security, 2011,  
<http://www.krollcybersecurity.com/resources/data-security-resources/data-security-statistics.aspx>
4. The State of Data-Centric Security, Ponemon Institute, June 2014