IDC PERSPECTIVE

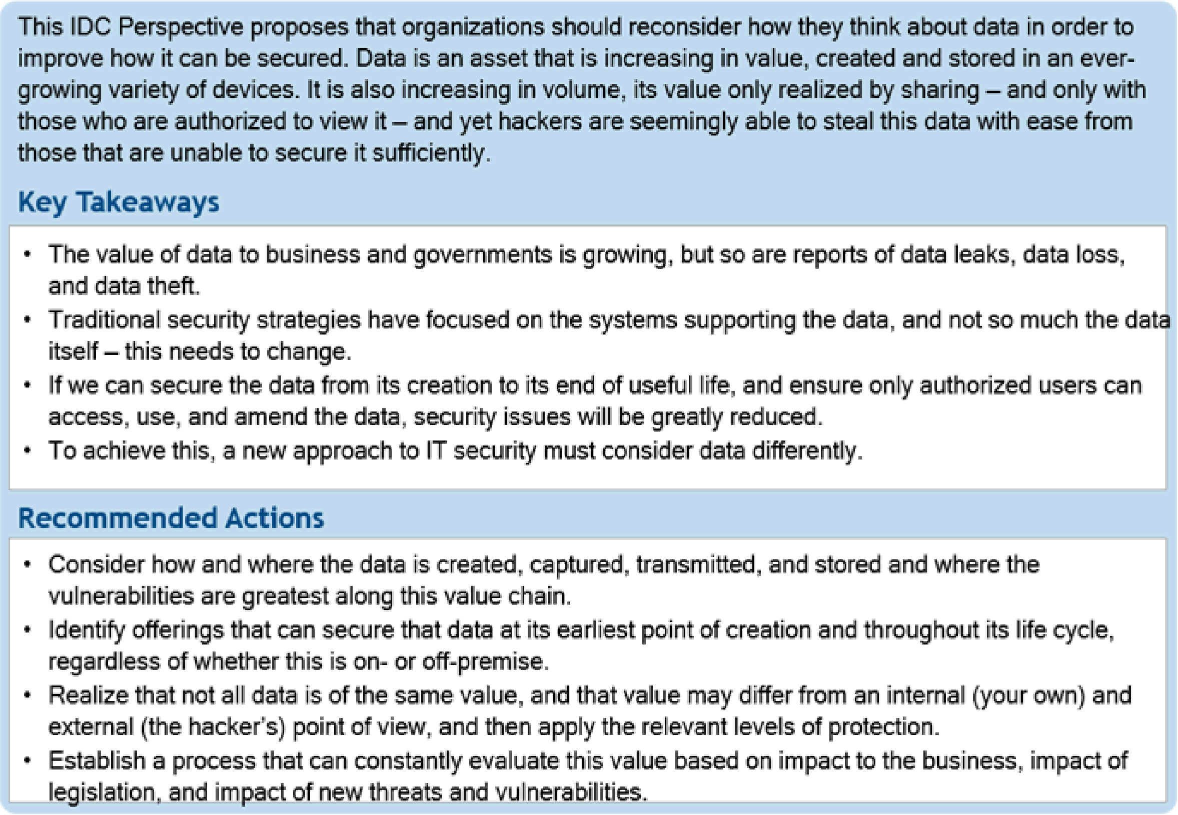
Is Data the New Endpoint?

Simon Piff Hugh Ujhazy

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Is Data the New Endpoint?



This IDC Perspective proposes that organizations should reconsider how they think about data in order to improve how it can be secured. Data is an asset that is increasing in value, created and stored in an ever-growing variety of devices. It is also increasing in volume, its value only realized by sharing – and only with those who are authorized to view it – and yet hackers are seemingly able to steal this data with ease from those that are unable to secure it sufficiently.

Key Takeaways

- The value of data to business and governments is growing, but so are reports of data leaks, data loss, and data theft.
- Traditional security strategies have focused on the systems supporting the data, and not so much the data itself – this needs to change.
- If we can secure the data from its creation to its end of useful life, and ensure only authorized users can access, use, and amend the data, security issues will be greatly reduced.
- To achieve this, a new approach to IT security must consider data differently.

Recommended Actions

- Consider how and where the data is created, captured, transmitted, and stored and where the vulnerabilities are greatest along this value chain.
- Identify offerings that can secure that data at its earliest point of creation and throughout its life cycle, regardless of whether this is on- or off-premise.
- Realize that not all data is of the same value, and that value may differ from an internal (your own) and external (the hacker's) point of view, and then apply the relevant levels of protection.
- Establish a process that can constantly evaluate this value based on impact to the business, impact of legislation, and impact of new threats and vulnerabilities.

Source: IDC, 2017

SITUATION OVERVIEW

Overview

In this day and age, hardly a week goes past without news of a new data breach. More interestingly, the news is no longer just about the size of the breach, but the quality of the data that is being accessed, whether that data was stolen or deleted. Consider the September 2017 announcement of the Equifax breach. At 143 million records, it is significantly smaller than the 500 million records lost by Yahoo in 2014. However, the quality of the data is so much richer than in previous hacks and will be significantly more impactful than previous breaches.

The move to the digital era has been marked by billions of dollars of spend worldwide on various forms of IT security. Regretfully, those dollars and keeping data and systems safe appear unable to stop the threat actors from profiting. It begs the question, "Why are data breaches still occurring?"

As the Internet of Things (IoT) becomes more prevalent across both the industry and the consumer worlds, the number of endpoint devices that need securing will increase by an order of magnitude. Combined with the velocity of cloud adoption, the amount of data stored outside the traditional data center implies that the scale and import of this issue will only get worse.

Why Data Security and Why Now?

To fully understand the challenges of IT security, a number of harsh realities must be considered:

- **Device connectivity breeds risk.** The most significant — and yet overlooked — reality is that it is almost impossible to maintain secure systems in this day and age. Connections to the internet exposes ports and protocols that could be attacked by the world at large. Over time these are locked down and access to systems and networks are slowly reduced, but this leads to the second aspect of the problem.
- **It's the devices, not data.** For much of the past 20 years, the focus has been on securing systems, the attempt to deny access to any but authorized users and systems. The theory was that a secure perimeter implies secure data. This is clearly not the case. Indeed, the goal of many would-be hackers is to beg, borrow, or steal the credentials of an authorized user to then be able to act freely across the internal systems, as they know that the IT security focus has been, for the longest time, on securing the perimeter, which assumes the threat is only external to the network.

In the world of cloud and IoT, these approaches fail since so much data and information will be external to the traditional view of the network edge. Therefore, protection strategies must evolve if we are to have any chance to improve overall security.

The Value of Data

In 2012, a leading Silicon Valley venture capitalist was quoted in Forbes magazine as stating, "Data is the new oil." This sentiment was echoed in The Economist early in 2017, acknowledging that organizations that are best able to define the value of the data they own and can acquire (legally, we trust) are emerging as the best-performing businesses in the information economy. IDC has also revealed through our own Digital Transformation practice that advanced data management capability is impacting all organizations, both in the public and private sectors, across all industries.

Hackers have long known this. The Equifax breach targeted high-value data and should act as a wake-up call to businesses and government on just how valuable data can be and how it needs to be better protected. There are no trusted players — there is only trusted data.

Understanding what data we have and to whom it is valuable is fast becoming a critical need in the information economy. Often, organizations focus on what data is valuable to themselves, forgetting they have data that is valuable to third parties. This requires a change in our thought process.

Why Consider Data as an Endpoint?

For many years, we have been trying to secure network endpoints. That process has always been one step behind the next attacker. It is time to shift the conversation and consider data itself as an endpoint — one that must be secured and offered only to authentic use cases.

In the past, organizations took a defense-in-depth strategy, layering firewalls intrusion prevention systems in an attempt to protect the perimeter of the organization. But with the introduction of mobile and cloud computing, that perimeter becomes a dispersed environment, no longer a traditional perimeter. As we shift to an IoT environment, we must acknowledge that the endpoints are now inherently insecure, in some cases both physically and virtually.

Take the life cycle of different data assets across many organizations. Increasingly, customer information (whether B2B or B2C) is obtained via online and mobile solutions long before any point of sale has taken place. This collection and creation is imitated beyond our traditional network endpoints and yet all too often it does not fall within the security controls until it is collected and properly curated. Consider how this will change as we move to a world of IoT. Not only are we now collecting data from environments where we cannot be certain about the physical safety, let alone the digital safety, of the device, but the need to analyze and refine much of this data at the edge is going to lead to the need to secure edge analytical solutions far from the traditional datacenter.

Cloud computing is another environment where we can consider data as an endpoint, especially since for most software as a service (SaaS) offerings, the data is the only component of the solution that organizations actually own. The remainder of the solution (the hardware, network, storage, and software) are all owned by the service provider and simply leased out to customers. Clearly there is a need to change how we think about securing this type of data, and so perhaps we should reconsider our overall security strategy.

Data has traditionally been seen as the passive result of transactional systems, to be surrounded, protected, and secured in systems that take an active part in the overall security perimeter of an enterprise. As that perimeter decomposes and becomes more fluid (e.g., cloud, mobile, IoT), data must be elevated so that each data object can itself participate in the security portfolio. Some of the characteristics of data as an endpoint include:

- **Data decides access rights**. A data object (whether in flight or at rest) can initiate a secure conversation with someone seeking to interact with that object rather than authenticated access to an application or transaction translating to data access.
- **Data is independent**. This secure conversation must be held independent of an application or piece of infrastructure as data can migrate across infrastructure and be accessed by one or more applications. Regardless of how often it is copied, duplicated, or moved, data retains the rules around who can use it. Therefore, if an attacker were to copy the data from a customer database and try to access it on an unknown network (from the owner's standpoint), that data would be useless to the attacker.
- **Data understands itself**. The data object must be self-describing and understand its own schema, so it can advertise how applications can interact with it, most likely through a series of APIs that are inherently based on authenticated use.
- **Data appreciates its value**. The data object can inherit a series of rules, governing when, where, how, and why it might be accessed. Given, viewing customer information on the corporate network might be allowed but viewing that same data on public WiFi may be forbidden.

Defining the Data Security Market

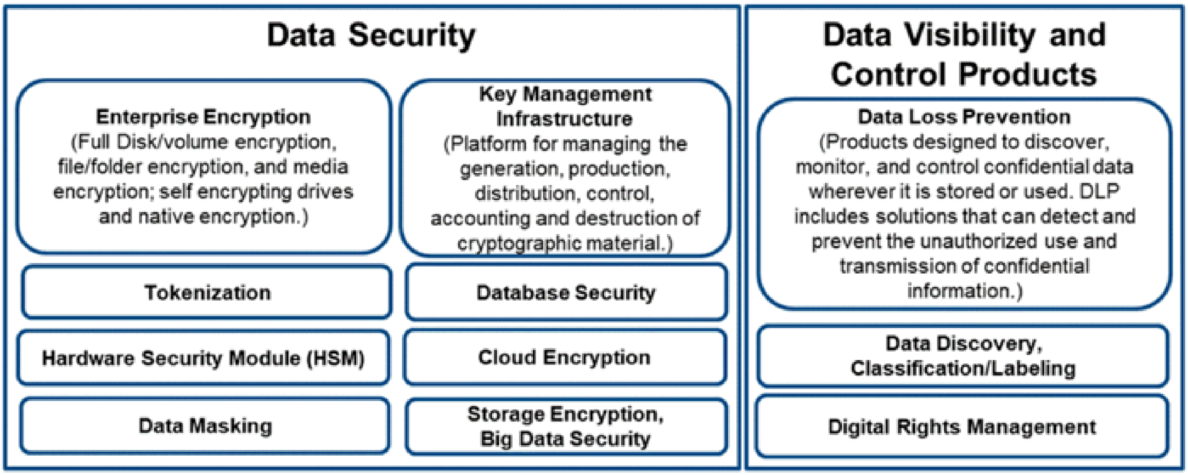
Within IDC, the data security markets are defined as software and hardware products and services associated with the discovery, classification, obfuscation, monitoring, and control of structured and unstructured enterprise data. Data security is a competitive market with products spanning multiple security product functional markets. These functional markets include endpoint, web, messaging, networking, identity and access management, and security and vulnerability management. The data security market has three primary segments:

- Enterprise encryption and data protection
- Data visibility, control, and alerting
- Secure content and collaboration

Within these primary segments are several subsegments, more details of which can be found in the *IDC Data Security Taxonomy* document (IDC #CA40532916) but are summarized in the table below.

FIGURE 2

Data Security Market Defined



Data Security

Enterprise Encryption (Full Disk/volume encryption, file/folder encryption, and media encryption; self encrypting drives and native encryption.)

Key Management Infrastructure (Platform for managing the generation, production, distribution, control, accounting and destruction of cryptographic material.)

Tokenization

Database Security

Hardware Security Module (HSM)

Cloud Encryption

Data Masking

Storage Encryption, Big Data Security

Data Visibility and Control Products

Data Loss Prevention (Products designed to discover, monitor, and control confidential data wherever it is stored or used. DLP includes solutions that can detect and prevent the unauthorized use and transmission of confidential information.)

Data Discovery, Classification/Labeling

Digital Rights Management

Source: IDC, 2017

Market Size, Main Players, Growth Potential, Impact on Adjacent Markets

Due to this overlay, IDC tracks the size of this market through two distinct functional markets: the data loss prevention (DLP) software market and the endpoint encryption and key management infrastructure market.

According to the most recent data security report published by IDC, the DLP market was valued at US$784.6 million at the end of 2015, which was a growth of 6.8% over the previous year. The top 3 vendors in this space were Symantec, Intel, and Forcepoint with market shares of 32.8%, 14.6%, and 11.1%, respectively.

DLP products are increasingly adopting support for data located in cloud services and extending policies to mobile users. The impact of DLP as a feature, the integration of SaaS products, and the adoption of cloud security gateways with data loss prevention functionality could impact the forecast, decreasing revenue associated with traditional DLP deployments. Countering this is the growth in compliance legislation across the globe, notably the European General Data Protection regulation (EU GDPR), which is due to come into force in 2018.

In the same report, the worldwide Endpoint Encryption and Key Management Infrastructure market stood at US$1,248.8 million in 2015 and is forecast to grow by 9.7% to 2020, surpassing US$2 billion in 2019. Within this segment, key management infrastructure is forecast to almost double with file and folder encryption growing from US$886.2 million in 2015 to $1,299.3 million by 2020.

Driving this growth is, in part, the move toward digital transformation, as more organizations realize that data is of greater value and spend more time and effort securing the data assets they own. Once again, the EU GDPR is also going to have a significant impact on the forecast, potentially resulting in higher growth than initially forecast.

Top Drivers and Inhibitors

Drivers

- **Data collection and analysis.** Enterprises are engaged in the digitization of everything and the demand for data capture, management, and analysis is driving interest in mitigating the risk of exposing sensitive or confidential data. The rising volume of IoT-related data and unstructured data is contributing to interest in and adoption of data security and data visibility and control products.
  - **Impact:** These factors will increase data visibility and control products that enable organizations to discover, classify, and control the most sensitive information.
- **Cloud adoption.** The continued adoption of SaaS collaboration products and cloud service provider solutions emphasizes the need for data migration oversight and the ability to monitor employee access and changes made to corporate data assets residing in services platforms, virtual environments, or on-premise repositories.
  - **Impact:** These requirements are driving purchasing for a range of tools that support a hybrid data security strategy, extending data governance policies to the cloud and maintaining on-premise key management infrastructure.
- **Compliance.** Data encryption continues to be the key driver of data security projects and IDC believes regulations governing data breach disclosure and minimum data privacy and data security controls will increase significantly in some regions.
  - **Impact:** Data security, residency, and privacy concerns will influence enterprise risk mitigation strategies and increase organizations' spending on data security products for compliance with regional rules.

Inhibitors

- **Cloud, virtualization, and architecture influences.** The adoption of cloud infrastructure and SaaS-based business solutions, file sharing, and collaboration platforms will accelerate and increase the adoption of encryption, but this introduces innovative architectural changes that complicate enterprise key management strategies.
  - **Impact:** The adoption of containers, NoSQL databases, and rise of microservices architectures can add management complexity and create encryption implementation weaknesses. This can slow the adoption of centralized key management infrastructure as organizations attempt to support a variety of services in cloud and virtual environments by implementing a hybrid approach.
- **Embedded security solutions.** Platform as a service (PaaS) providers are increasingly adding security components into their platforms and/or offering their own line of security products that address identity and access management, data protection, and other common security essentials.

- **Impact:** Revenue-based market growth will be inhibited because of this trend as enterprises adopt PaaS provider solutions and eliminate point solutions to reduce complexity. This trend is slightly different from cloud provider models that include a marketplace where security products and other software solutions can be adopted.

ADVICE FOR THE TECHNOLOGY BUYER

Data has never been perceived as having a value as high as it does today, and it looks as if this value is only going to grow over time. The headlines from Forbes and The Economist linking data to oil completely miss one crucial difference — data is not in short supply nor is it likely to become so in the near future. However, the analogy around the value of data must not be ignored.

So, understanding this, organizations need to reconsider how to secure this data that is being created outside of the traditional secure environment; how to securely capture, manage and share this data; and how to securely collaborate around data with trusted partners.

Clearly the security solutions we have in place today are not sufficient to protect the data stored within systems, hence the plethora of high-profile data breaches in the news. It is time to rethink how we secure the data by considering it as an endpoint with an active role in the overall security strategy rather than as a passive element in transactional systems.

We need to find a simplified yet efficient way to securely manage data. This data will be both on- and off-premise, mobile and static, in the cloud and on a mobile or IoT device. We also need to be aware that data security is not a silo; the value of data is only realized after it is — to use the oil analogy — refined using analytics to better understand the patterns that deliver value to the business. As a result, it is not simply about statically securing data, but also about being able to secure it in a more fluid manner, one that still permits usability both at rest and in flight.

In June 2016 IDC published a document entitled *Distributed Integrity: A New Security Model to Replace Perimeters* (IDC #US41478616), which posits the common security strategy of defense in depth (layered perimeters) as but the first of four stages of security strategy. The model focuses on users, data, and applications, and fully embraces the idea that the data needs to be encrypted (and key controlled) and then traced throughout its life cycle. In hindsight it's easy to point out that if Equifax had at least encrypted its data, the implications to the market would not have been so severe, although this fact is true for many organizations that have yet to experience such a breach.

Through discovery, classification, monitoring, containing, and encrypting through to its ultimate disposal or deletion, data is prolific and almost impossible to protect by relying on traditional network and host security solutions. To be successful, organizations must develop a program that focuses protection capabilities on the data itself.

LEARN MORE

Related Research

- *IDC's Worldwide Data Security Taxonomy, 2016* (IDC #CA40532916, December 2016)
- *IDC PlanScape: Data Security Principles and Practices for Digital Transformation* (IDC #US42067416, December 2016)
- *Market Analysis Perspective: Worldwide Data Security, 2016* (IDC #US41764116, September 2016)

Synopsis

Twice in the past five years, leading global business publications have described data as having the same characteristics as oil, in relation to its increasing value in the global markets. Unlike oil, however, data is not a finite resource; indeed, it is growing at ever-increasing rates. Furthermore, the value of this data is widespread and the ability to lose, misplace, or have data stolen or seen by those that should not increases almost daily.

"Strategies to protect data must evolve if we are going to successfully protect this valuable resource in the future," says Simon Piff, Vice President, Security Practice for IDC Asia/Pacific. "It's clear from the almost constant barrage of headlines announcing the latest data breach that we are not all able to secure this asset with the strategies we have used in the past. Perhaps by reconsidering our approach to how we think about data, we can create improved strategies to secure this increasingly valuable asset."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Asia/Pacific Headquarters (Singapore)

80 Anson Road, #38-00
Singapore 079907
65.6226.0330
Twitter: @IDC
idc-community.com
www.idc.com