Data Classification in Hybrid Clouds: An Overlooked but Critical Step in Data Protection

A TrendLabs℠ Primer

¬Securely moving to the cloud is a top concern for enterprises, especially since each journey is different for every organization. Today, most organizations are operating hybrid environments, where data is continuously flowing through physical components, virtual endpoints or servers, and private or public clouds. Therefore, paying attention to the nature of recent attacks against data is more important than ever–as attackers can get into networks through a breach and subsequently move laterally inside the network to go deeper into protected areas and even the cloud.

As evidenced by the damage caused by recent data breaches and targeted attack campaigns, data security has been proven to be a critical factor to a company's survival. But despite that, the reality is that enterprises cannot protect each and every bit of their data.

Strategies must be in place to address threats and new data regulations that affect a company's approach in handlingdata. This primer discusses data classification,data protection guidelines, and security technologies that can help companies keep their data secure as they make their journey to the cloud.

Many moving parts

The Internet of Things, mobile banking and payment systems, and other computing advancements enable companies to automate some business processes. However, these new software, platforms, and environments can also expand the attack surface by introducing gaps in the system which threat actors can exploit in order to steal confidential information. Modern data centers–which are using a mix of physical, virtual, and cloud-based endpoints and servers– need to protect their networks against these improving threats.

Cyber-attacks against data

Data breaches, for instance, can put data in harm's way–no matter where the data is created, transformed or processed. Based on our paper entitled Follow the Data: Analyzing Data Breaches by Industry, portable device loss (particularly device theft) is one of the major causes of data breaches among the companies we've examined. However, in addition to device loss, data breach incidents attributable to hacking or malware are also on the rise.

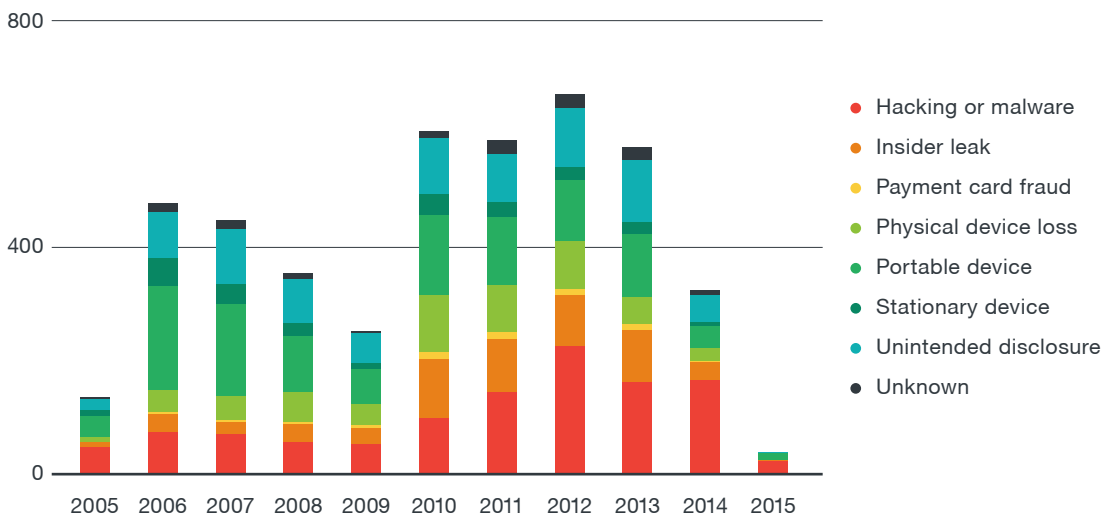


Figure 1. Breach methods observed from 2005 to April 2015

Source: Follow the Data: Analyzing Data Breaches by Industry by Trend Micro

Threat actors are becoming better at customizing cyber-attacks against enterprises–whether it's a small-time score meant to milk a small business's bank accounts dry or a long-running cyber-espionage operation meant to steal mission-critical information like nuclear launch codes or competitive strategies. Threat actors have had years of practice through trial-and-error methods used to fine-tune their operations. From business email compromise (BEC), exploit kits, and to lengthy targeted attack campaigns, enterprises have to grapple with the possibility of facing a cyber-attack at any given moment.

Tangible costs of cyber-attacks

Nearly all the reported data breaches carried with them some measure of business impact. The scope of damage often has to do with the nature of the information that has been stolen or leaked.

For instance, in the case of the hacking incident involving the United States Office of Personnel Management (OPM), the lives of intelligence assets, their records, personal and contact information, among others, were exposed–thus weakening their and the state's ability to operate as covertly as it wants for decades.

Sony, on the other hand, got sued for demonstrating poor security practices that allowed hackers to release up to 100TB of data, including unreleased films, confidential email, and employee salary information.

J.P. Morgan, among several other big-name banks, suffered data breaches that have allowed hackers to earn up to US$100 million in pump-and-dump scams, resulting in its commitment to double security spending to US$500 million in 2015.

Premera Blue Cross, a healthcare insurance company, had to offer two years of free credit monitoring to its account holders after a breach exposed 11 million customers.

New rules, new game

In response to the different threats raised against data privacy, the EU Commission, in December 2015, made a landmark update to the Data Protection Directive with its new General Data Protection Regulation–a change that will impact the data management landscape for global companies in years to come. The regulation now covers even non-European Union entities as long as they are handling data belonging to EU residents.

The regulation also outlines:

- updated definitions for what constitutes personal data
- more accountability for data controllers and data processors
- stricter guidelines for the acquisition of consent
- reminders for data breach notifications to be made within 72 hours from the discovery of a breach

While other countries like Japan and the United States, for instance, have prescribed their own data protection policies, the General Data Protection Regulation also presents one of the harshest penalties for violation. According to the new rules, data controllers can face fines–ranging up to 4% of the global gross revenue–for failure to comply. This is yet another important consideration enterprises must look into when coming up with a comprehensive data management strategy that encompasses data in physical and virtual endpoints and servers, and even the cloud.

Data protection in hybrid clouds

Trend Micro CTO Raimund Genes encourages enterprises to start thinking about this pervasive security challenge in terms of 'core data'. When navigating through these new data protection challenges, enterprises must evaluate their next steps using this framework:

1. Identifying and classifying core data
2. Protecting core data

While the protection of core data is where real security operations and solutions come in, the identification and classification of what data matters the most to your company is crucial in making decisions on resource allocation and priority.

Not all data is the same

The broad landscape of data being created, processed, and stored in modern data centers demands varying treatments for different kinds of data. For instance, data controllers will be much more concerned about a company's list of prospective clients being leaked to competitors, or about who accesses payroll information within the company, than they would be about marketing material related to the company's products.

> *Obviously, you have to protect your data. However, neither can enterprises just try and protect everything with the same rigor.*
>
> ~ ***Raimund Genes,***
> *Trend Micro Chief Technology Officer*

Microsoft offers guidance in its Data Classification for Cloud Readiness with regard to terminologies a company might use to describe the importance of a certain document or data set.

Sensitivity	Terminologies	Description	Examples
High	Confidential, Restricted	Data that, when lost, can be catastrophic to one or more individuals	Personally identifiable data, intellectual property, authentication data
Medium	For internal use only, Sensitive	Internal information that will not be catastrophic when lost	Email, documents, files that do not contain confidential data
Low	Public, Unrestricted	Data that is not critical to operations	Press announcements, public company information

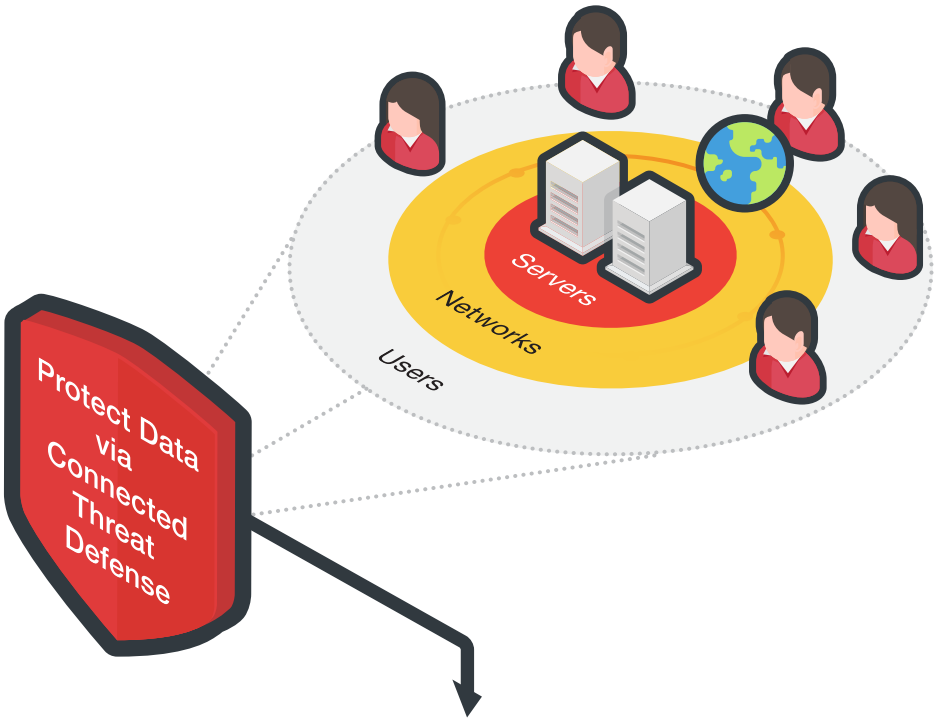
Given the above guidelines, it also becomes clear why a risk assessment exercise will be useful in determining what the company really values. Such an exercise can also raise possible scenarios where the leakage or loss of data may harm employees, clients, contractors, visitors or the general public.

Protecting what matters

Security is a shared responsibility between a cloud vendor and a cloud customer. The cloud provider is in charge of securing the global infrastructure and foundational services like computing, storage, database, and networking in the cloud. However, many organizations don't realize that they, the cloud customer, are in charge of securing everything else above this stack: network traffic, platforms, applications and content.

Protecting core data is also two-pronged. On the one hand, network defenders must employ security technologies that can detect malicious activities in the network as they happen. Then on the other hand, the results of the data classification exercise must also empower network defenders to secure the flow of data automatically, if possible, especially for data with high and medium sensitivity.

Data classification resets the modern enterprise's expectations about its ability to safeguard its assets. The following security capabilities will allow organizations to protect, detect, and respond to threats against core data–but a full understanding of what constitutes high-value secrets that are critical to a company's survival will fuel the efficiency of each step.



Encryption & DLP	Anti-Malware & Content Filtering	Behavior Monitoring & Sandboxing	Application Control	Intrusion Prevention	Integrity Monitoring	Response & Containment
Deploy data security on endpoints, network gateways, and cloud	Detect and block malicious components and URLs that aim to steal data	Work with black lists to detect unknown threats	Complement black lists and behavioral strategy by whitelisting critical apps	Prevent exploitation of zero-day/ unknown bugs leading to data stealing threats	Monitor the network for unauthorized/ unexpected or suspicious changes	Act on findings in a timely and efficient manner to minimize impact

A layered security approach can best address the challenges of data protection. Critical information is often stored on servers that could either be inside the company or in the cloud. Data is always moving throughout the network and users could be handling data using different devices and applications.

What enterprises should do

The changing security landscape will only produce more challenges on data protection. Part of a fortified data protection strategy is data classification, the ability to identify what company data is considered public, internal, or confidential. Data protection itself must rely on a connected threat defense that can protect enterprises from as many threats as possible, detect advanced threats and threat activities, and respond in a timely manner.

The security capabilities that enterprises should look for are encryption, anti-malware and content filtering, behavior monitoring and sandboxing, application control, intrusion prevention, integrity monitoring and response, and containment. Security solutions must be able to do all these without hampering speed and efficiency, and by also complying with data privacy and security requirements like PCI DSS, HIPAA, NIST, SSAE16 and others.

Created by:

TrendLabs

The Global Technical Support and R&D Center of **TREND MICRO**

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver topranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO™

Securing Your Journey to the Cloud

www.trendmicro.com