WHITE PAPER

Data Privacy and Security in the Cloud Era

Introduction

Data protection has undergone a dramatic transformation with the increasing use of multi-tenant, public cloud computing resources. If you are not currently processing workloads with sensitive data on public cloud infrastructure, that may soon change. The RightScale 2018 State of the Cloud Survey found that 38 percent of enterprises are specifying public cloud as their top deployment platform in 2018, up from 29 percent in 2017.[1]

38%	3 of 4	25%
Report public cloud is top platform	**Run more than 20% in public cloud**	**Spending > $6M on public cloud**

Once you begin using public cloud infrastructure, you lose the control you once had over your data and its physical location. Data once secured in private data centers can end up moving between virtual servers on geographically-dispersed hardware, as cloud providers strive for operating efficiency. Traditional security practices cannot be applied in such an environment. So how can you maintain data protection and regulatory compliance?

This whitepaper looks at how a total network visibility platform can help organizations strengthen security and maintain data privacy, even as they relinquish physical control of their infrastructure to cloud providers.

- Data owners must be proactive about protecting data privacy.
- Cloud computing creates blind spots that prevent total network visibility.
- A visibility platform can overcome blind spots and facilitate cloud monitoring.
- Visibility with cloud-native scalability, application intelligence, and active Secure Sockets Layer (SSL) decryption makes monitoring more efficient.

1 RightScale, 2018 State of the Cloud Survey, February 2018, available online.

KEYSIGHT TECHNOLOGIES

The Role Of The Data Owner

Sharing data is essential for modern commerce. Each entity in a supply chain may have a legitimate need to receive and store sensitive customer or company data. When these entities use cloud services to run their business, that sensitive data can end up being maintained in hundreds of different locations. This distributed environment has a significant impact on the responsibility of data owners.

In hosted environments like a cloud, responsibility for security is shared between the hosting provider and the data owner. Although this policy is clearly stated in the standard contract of major cloud providers, customers often overlook this critical fact. In a 2017 study, Veritas Technologies found that 69 percent of organizations incorrectly believed that data protection, data privacy, and compliance were the responsibility of the cloud service provider.[2]

Unfortunately, industry practices for maintaining digital security have not always kept pace with technology. Data breaches in cloud environments have been frequently reported. Many large enterprises have had sensitive data stored in the public cloud compromised due to inadequate testing of web-based applications and configuration mistakes. In one high profile case, Deloitte had its cloud-based global email server breached, and thousands of emails with sensitive data were exposed.[3]

These breaches can cause serious harm to individuals and organizations. For example, consumers reported $905 million in losses due to identity theft in 2017, a 22 percent increase from 2016.[4] The cost to organizations is also rising. The 2018 Ponemon Cost of Data Breach study found the average total cost of a breach rose 7 percent from the prior year, rising to $3.86 million per incident. Headline-grabbing mega breaches have cost tens or hundreds of millions.[5]

2 Veritas Study: Alarming Majority of Organizations (69 percent), Export Full Responsibility for Data Protection, Privacy, and Compliance onto Cloud Service Providers, October 25, 2017, from online news release.
3 Arden Rubens, Recap: The Biggest Data Breaches of 2017, CheckMarx, December 31, 2017.
4 Matt Tatham: Identity Theft Statistics, Experian.com, March 15, 2018.
5 Ponemon: 2018 Cost of a Data Breach Study, July 2018, sponsored by IBM and accessed online.

Compliance Regulations and Consequences

The increasing threat to infrastructure, data, and applications by either inadvertent exposure or cyberattack has made compliance a top priority for IT organizations. Penalties for non-compliance to privacy regulations are increasing. Organizations that do not consistently comply with PCI-DSS may lose the ability to accept credit cards. In the U.S., any HIPAA violation will result in a large fine from the Department of Health and Human Services.

Beyond the official penalties, there is the threat of a lawsuit charging negligence when IT practices fail to protect privacy. For example, if there is lax security on personally identifiable information, victims can sue a company for damages associated with identify theft. The most significant consequence of non-compliance can be the negative publicity and loss of reputation associated with any lapse or violation.

The best way to prove compliance is to implement strong internal security practices and be ready to show how your company follows up on alerts and anomalies. Continuous monitoring and validation are best practices. Table 1 lists the privacy and security provisions of three key pieces of legislation.

Prove compliance with security monitoring and consistent follow-up.

U.S. Health Insurance Portability and Protection Act (HIPAA), 1996	Payment Card Industry Data Security Standards (PCI-DSS), 2004	European Union's General Data Protection Regulation (GDPR), 2016
Protects the medical records and other personal health information of U.S. residents	Applies to all global entities that process transactions for JCB, American Express, Discover, MasterCard, and Visa	Applies to all entities doing business with individuals located in the European Union
Last updated 2009	Last updated August 2018	Penalties activated May 2018
The Security Rule specifies the duty of care for entities that interface with electronically transmitted 'protected health information' (PHI): • Ensure confidentiality, integrity, and availability of all personal health data • Identify and protect against threats to security or integrity • Protect against unauthorized use or disclosure • Ensure compliance by their workforce Non-compliance: Large fines levied by the Department of Health and Human Services, Office of Civil Rights	Standards related to technical and operational systems: • Build and maintain a secure network and systems • Protect stored cardholder data and encrypt transmission across public networks • Maintain a vulnerability management program to protect systems against malware and viruses • Implement strong access control measures • Regularly monitor and test networks • Maintain an information security policy Non-compliance: Revocation of authority to process credit card transactions	GDPR places equal responsibility for data security on data controllers and data processors. Key provisions include: • Proactively embedding privacy into any new technology or service • Implementation of data security measures such as encryption • Timely notification of breaches • Prevention of unauthorized data transfers Non-compliance: Fines up to a maximum of 20 million Euros or 4 percent of total worldwide revenues, whichever is higher
Source: U.S. Department of Health & Human Services website: Health Information Privacy	Source: PCI Security Standards Council website	Source: SANS Institute: "Preparing for Compliance with GDPR; A Technology Guide," accessed online

Table 1. Summary of key digital privacy regulations

The Role Of Cloud Providers

The high cost of violating data privacy requires organizations to understand the role cloud providers play in protecting their data. Contracts with cloud service providers should define data protection standards and establish Service Level Agreements (SLAs) that specify security and privacy measures, including the use of data encryption, notification procedures, and response times.

Understand what your cloud provider will do in the event of a breach and work with them to protect your customers.

However, for these contractual agreements to have a practical effect, organizations must also actively manage and monitor them. It is essential to understand policies in the following situations:

Security Breach. Be clear on your cloud provider's disclosure policy. The majority of U.S. states have security breach disclosure laws that require the data controller to notify the data owner if a personal data breach occurs. The European Union's General Data Protection Regulation (GDPR) specifies notification must occur within 72 hours of discovery. Similarly, if you believe your enterprise data has been breached, you should notify your cloud provider immediately.

Disaster Recovery. There have been a number of instances where a data center has suffered a catastrophic outage, resulting in a loss or disruption of services to many websites and customers. Disruption is not only caused by physical issues like natural disasters, but also by software errors and denial of service attacks. Consider the possible scenarios and have a plan for recovering your data and relocating your workloads to another provider, if required.

Data Protection. Understand how your cloud provider will protect your data. Check their policies for data retention and destruction. Data encryption is a specific service your cloud provider may offer. Encryption can operate at a number of levels, depending on your requirements, application, and desired approach. You will need to consider the impact on end-user performance, as different encryption techniques may have a significant impact on the user experience.

Secondary Use of Data. In some cloud environments, you may need to consider whether your data is going to be mined or shared with other third-parties. Examples include government officials approaching your cloud provider for access to your data or your provider choosing to share data with one of its business partners without obtaining your permission. You may want to ensure your contract prohibits or limits this type of activity.

Remember, you and your cloud provider have shared responsibility for security of customer and proprietary data. Implementing basic monitoring is essential to helping you detect suspicious behavior or unsafe conditions.

Vulnerabilities Of Public And Hybrid Clouds

As breaches in cloud environments are regularly exposed and analyzed, we are learning more about the most significant areas of risk to cloud users. Here are three areas of top concern:

1. Lack of Access to Network Packet Data

Cloud environments differ substantially from an on-premises environment where physical and virtual network taps and SPAN ports are used to directly access network packets. Cloud providers don't let their customers tap multi-tenant infrastructure due to privacy concerns. Without visibility to packet data, interactions in the cloud are blind spots where malware can potentially enter without detection or large amounts of data can leave without oversight.

Advanced security solutions need packet data to diagnose and isolate the source of security issues.

A survey of cloud adopters conducted last year revealed that some organizations are taking a calculated risk by not addressing this issue. Fourteen percent of respondents admitted they are not monitoring network traffic in their clouds at all. Even among those with monitoring programs in place, 37 percent reported experiencing a delay in resolving a security alert due to lack of visibility, and 26 percent reported missing a security threat or attack.[6] With the increasing sophistication of cyberattacks, organizations must monitor their clouds.

The advanced security solutions available today use the contextual details in packet data to identify threats and detect anomalous behavior. Without packet analysis, you increase the risk a security attack will go unnoticed for a longer period and cause more damage.

6 EMA Network Security Survey, January 2017, sponsored by Ixia and available online.

2. Weak Cyber Hygiene

Cyber hygiene is necessary to protect any computing environment, but the cloud expands the potential for poor hygiene to cause serious harm. An incorrectly configured access control list, for example, can inadvertently provide administrator level rights to millions of people via the internet. Table 2 offers examples of companies who recently suffered from a lapse in cyber hygiene.

Standard Cyber Safety Practice	Reported Breach
Least privilege access control	Sony was the victim of hackers who obtained admin level access to systems with sensitive customer data.
Micro-segmentation of network	In the Target breach, after initial intrusion into the HVAC system, hackers were able to move laterally into the payment systems.
Encryption	After a data breach at Royal & Sun Alliance Insurance PLC, investigators determined the company had not adequately encrypted sensitive data.
Multifactor authentication	The LinkedIn breach exposed inadequately protected access to 100 million users' accounts.
Timely system patching	The WannaCry ransomware exploited a known software vulnerability for which a patch was available.
Proper configuration	Verizon and World Wrestling Entertainment exposed personal data due to misconfiguration of AWS cloud repositories.
Source: VMware, *Core Principles of Cyber Hygiene in a World of Cloud and Mobility*, August 2017	

Table 2. Recent breaches linked to poor cyber hygiene

Application Programming Interfaces (APIs)

The rise of cloud computing has increased the possibility of API attacks. By definition, APIs allow external people, applications, or services access to your internal systems, data, or other resources. Most applications today use APIs to increase flexibility and enable integration, and this is particularly true for cloud applications. In fact, integration with other services is often a reason for migrating to cloud in the first place. According to a 2018 study by Imperva, the average organization now manages 363 APIs and more than two-thirds of organizations expose their APIs to the public in order to enable supply-chain and ecosystem partners.[7] These interfaces, however, also increase the risk of an unauthorized person accessing your network by exploiting an unprotected API.

Security researchers are focusing more on the vulnerabilities associated with APIs. Last year, the category of under-protected APIs made the Open Web Application Security Project (OWASP) Top Ten list for the first time.[8] High profile breaches caused by poor API security have been reported at Panera Bread, Venmo, and Salesforce.[9] According to Gartner, by 2022, API abuses will be the most-frequent attack vector resulting in data breaches for enterprise web applications.[10] This is an issue that cuts across company sizes and industries.

---

7 One Poll API Security Survey, conducted for Imperva, published January 25, 2018, accessed online at SlideShare.

8 Ericka Chickowski, *Expect API Breaches to Accelerate*, DARKReading, August 7, 2018, accessed online

9 Ibid

10 Mark O'Neill, Dionisio Zumerle, Jeremy D'Hoinne: *How to Build an Effective API Security Strategy*, Gartner, December 8, 2017.

Strategies For Protecting Data In Your Clouds

Improving your cyber hygiene practices and deploying an API security gateway can reduce threat surface and risk. However, in security, nothing is impenetrable. Customers and regulators expect organizations to have multiple layers of security to identify breaches and limit losses as quickly as possible. After you deploy the standard firewalls and DDoS prevention solutions, consider these additional five strategies to strengthen security and data privacy in your clouds:

1. Monitor All Your Network Traffic

Traditional security monitoring involves screening network packets entering or leaving the organization, as well as looking for known threats, unauthorized egress, or suspicious behaviors. Though the techniques are sometimes different, it is crucial to maintain the same level of security in your cloud environments. A network visibility platform with the ability to tap or capture traffic from physical, virtual, and cloud infrastructure is the foundation. Key functions of the visibility platform are:

Eliminate blind spots. In virtualized and cloud environments, network traffic can move without crossing a physical barrier and being observed by network taps. Since taps are the primary way you provide traffic to your security monitoring tools, they will not see virtual and cloud traffic, leaving you "blind" to what is happening in key parts of your enterprise. Your security solutions need to see all of the traffic in your network to eliminate attacks and prevent breaches. For this reason, it is crucial to eliminate blind spots associated with virtual and cloud environments and establish 100 percent visibility to all traffic in your network. A network visibility platform with the ability to tap or capture traffic in physical, virtual, and cloud environments is the foundation of effective security in the cloud.

Real World Lesson #1

- Multiple financial institutions throughout 2017
- Carbanak/Fin 7 attacks bypass antivirus tools and net millions of dollars.
- RSA post-incident analysis concluded lack of visibility and inadequate threat detection enabled attacks.
- **Takeaway: Detection and analysis are critical to data protection.**

Source: Anatomy of an Attack: Carbanak, RSA blog, Dec 4, 2017

Examine all segments. Certain network segments are isolated and protected behind firewalls to reduce the risk of an unauthorized breach in one part of the network from spreading. Even though sensitive data and applications may reside on a remote network segment, it is important to monitor the data flowing through that segment. Total network visibility — to every network segment — and robust monitoring are the only ways to reduce the risk of an undetected breach or compromise.

Access application detail. Cloud providers may provide customers with log files that contain time-stamped documentation of specific events related to their cloud services. Administrators have long used log files like these to trigger security alerts for further investigation. Unfortunately, while log events are useful for identifying when a condition was triggered, they do not provide enough detail to find the source of that activity.

The increasing sophistication of cyberattacks demands more in-depth analysis with packet data to determine where a request originates, the users that access the data, which applications are in use, and what data is accessed. Packet data is not part of the standard offering of cloud providers. Fortunately, cloud visibility solutions are now available that provide packet data from your cloud traffic to enable faster and more accurate security analysis.

Deliver the right data to the right solutions. Once you capture traffic, you need a fast and efficient way to deliver the right data to each security monitoring solution. A network visibility platform simplifies the process of sorting packets and scheduling delivery to your desired security solutions by giving you a single-pane, drag-and-drop interface for setting up filters and delivery instructions. Also, you can establish rules for passing packets from one solution to another (serial chaining) to increase monitoring efficiency.

2. Adopt Strong Encryption Policies

After ten years of consideration and 28 drafts, the Internet Engineering Task Force (IETF) approved a new set of secure socket layer (SSL) protocols for secure network communications, known as transport layer security (TLS) 1.3 in March 2018. TLS 1.3 makes it harder to eavesdrop or intercept communications because encryption keys are negotiated anew for every client-server pair in a secure session, rather than being than reused. To participate in secure communications, organizations using TLS 1.3 must be active participants in the encryption process. For this reason, the new standard is also called "active SSL."

It will take a while for web server owners to adopt the new encryption standards and for TLS 1.3 to become widely deployed. In the meantime, you can prepare your organization by verifying that your network visibility and security solutions support active SSL decryption and re-encryption.

Keep in mind that decryption is process intensive. Though some firewalls and other security solutions may offer on-board decryption, that may not be the most cost-efficient approach. Your visibility platform can decrypt secure traffic more cost-efficiently than sophisticated security solutions, whose processing power is better devoted to deep packet inspection and analysis. Plus, your visibility platform can easily route decrypted traffic to multiple monitoring tools at the same time, increasing the overall efficiency of security monitoring.

Real World Lesson #2

- Taringa Social Network, Sept 2017
- Cloud database with 28 million customer passwords was stolen.
- Passwords were encrypted with a notoriously weak algorithm (MD5). Breach investigation service claimed to have cracked 27 million in a few days.
- **Takeaway: Encrypt sensitive data with a strong cipher.**

Source: Calyptix Security blog

3. Shield Sensitive Data with Masking

As packets containing sensitive data enter the network, IT can protect selected data fields by masking — or overwriting — the confidential information, while retaining the data format such as in the case of a social security number replacement with "xxx-xx-xxxx." With sensitive data fields obscured, packets can be forwarded to any number of security monitoring solutions without fear of disclosure. Masking is especially important because even though you can ensure security during data transfer, monitoring tools may store the data for extended periods of time. Protection mechanisms of this type are required to achieve regulatory compliance under PCI-DSS, HIPAA, and GDPR.

With the wide availability and use of applications-as-a-service, IT is no longer aware of all the applications running on the network and the data they use. For this reason, a network visibility platform with the ability to see inside packets to identify unfamiliar applications and to flag sensitive data is key to maintain compliance with privacy rules and regulations.

Real World Lesson #3

- InterContinental Hotel Group, February 2017
- Point-of-sale malware infected about 1,200 web properties. The breach spanned three months.
- Investigation found malware captured unshielded credit card data.
- **Takeaway: Mask sensitive data in motion.**

Source: Calyptix Security blog

If you have deployed a cloud visibility platform with application intelligence—the ability to understand the context of traffic from packet details — data masking can be deployed as a feature, and you do not need an additional device. This capability allows you to set predefined masking templates for common fields such as credit card numbers, email addresses, and social security numbers and also offers the ability to define custom masks to protect other types of sensitive information.

4. Inspect All Secure Traffic

At one time, it was common to skip monitoring encrypted packets because there was not a solution available that was powerful enough to perform fast real-time decryption. When encrypted traffic was only 10 percent of overall volume, the risk of a breach may have seemed low. Unfortunately, attackers discovered that encrypting their malware helped them to avoid detection and it is now standard operating procedure for them. Plus, half of all network traffic is now encrypted, and the percentage is rising.[11] If you haven't already begun decrypting secure traffic, consider the following:

> "Encryption does not protect us from all threats and, in fact, can make it easier for the adversary. Enterprises must be aware of and concerned if they are not decrypting and inspecting SSL traffic from untrusted sources."
>
> Jason Brvenik,
> Chief Technology Officer at NSS Labs

Security solutions require plain text. The deep packet inspection performed by next generation firewalls, intrusion prevention systems, and other security solutions requires plain text. To keep your defenses strong, you need an efficient solution for converting encrypted packets into the format your security tools need. Many of your monitoring solutions will need access to the same data, so you need an efficient way to decrypt the packets once and deliver plain text simultaneously to multiple solutions to save time and processing cycles.

11 Sarah Perez EFF says: *Half of Web Traffic is Now Encrypted*, TechCrunch, Feb 22, 2017, accessed online.

Processing power counts. No matter what solution you use for decryption, it needs to be powerful. Decoding requires intense processing, and encryption algorithms are becoming more complex with longer key sizes to strengthen their ability to withstand hacking.

A more robust solution is to offload decryption to a visibility platform. You can use a packet broker to automatically decrypt and route secure traffic through each of your security solutions according to rules you set up. Once the inspection is complete, a packet broker can also re-encrypt traffic, to maintain security as it travels to its final destination in your network.

Simplify visibility management in hybrid environments to free up resources for threat detection and alert investigation.

Active SSL will eventually be the norm. Once TLS 1.3 becomes the norm, organizations will need active SSL encryption and decryption capabilities. If you are searching for a decryption solution now, make sure to find out if the solution offers active SSL decryption. Solutions that are already designed to support dynamic SSL decryption give you a better return on investment (ROI).

5. Simplify Hybrid Cloud Monitoring

In hybrid clouds, which are used by more than 50 percent of today's organizations[12], achieving total network visibility is more complicated and requires multiple traffic capture technologies. However, if you simplify visibility management in your hybrid environment, you can increase the management resources available for threat detection and alert investigation.

Single-pane monitoring. Even if you use multiple packet access technologies, you do not necessarily need to use different interfaces for configuring traffic capture, filtering, and delivery. Look for management platforms that support multiple environments. Two things to look for are:

1. A drag-and-drop graphical interface that is intuitive and easy-to-use
2. The ability to source traffic from physical, virtual, and cloud environments

A single management platform with these characteristics will reduce training costs, speed configuration and setup, and reduce errors. Do not underestimate the savings in time and accuracy that come from choosing a visibility platform designed to support hybrid environments.

Support for on-premises monitoring. When it comes to security monitoring using a comprehensive suite of security features and real-time processing is critical. Unfortunately, many of the newer, cloud-based solutions do not yet provide the level of functionality delivered by mature, on-premise solutions. Many enterprises intentionally combine cloud-based security solutions with on-premise solutions to avoid the risk of

12 RightScale, 2018 *State of the Cloud Survey* February 2018, available online

outage resulting from downtime in a cloud-based solution. Look for a network visibility platform that gives you the option to send filtered data to either cloud-based or on-premises monitoring tools for the highest value.

Summary

The use of public and hybrid clouds requires changes to our practices for security monitoring and data privacy. As a cloud user, you are jointly responsible for protecting data and applications in the cloud, along with your cloud provider. Not only do your customers expect you to protect their sensitive information, but regulations and laws are now in place to sanction organizations that do not do enough to prevent data exposure and breaches.

While cloud providers offer useful services to assist you, it is important to implement packet-based traffic monitoring to alert you to suspicious behavior or unsafe conditions. Improving cyber hygiene and carefully monitoring your APIs can help reduce your risk, but you need to have multiple levels of security monitoring in place to identify breaches and limit any potential damage.

To meet the challenges of the cloud era, organizations in every industry are establishing a strong network visibility platform that allows them to monitor 100 percent of their cloud and encrypted traffic, and keep their data secure.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES