imperva

iSMG
INFORMATION SECURITY
MEDIA GROUP

Securing Data Before the Cloud

Imperva's Terry Ray on Reducing Complexity and Improving Compliance

Terry Ray

In this new era, every enterprise is suddenly "cloud first." But there are significant data security gaps to avoid before putting critical data in the cloud. Imperva's **Terry Ray** shares strategies to maximize simplicity and regulatory compliance.

In an interview on cloud security with Tom Field of Information Security Media Group, Ray discusses:

- The biggest cloud security gaps;
- How to secure data before it goes to the cloud;
- Factors that are reshaping enterprise data security.

Ray is senior vice president of strategy for finance and healthcare at Imperva Inc. Ray applies his decades of security experience to these industries and their cybersecurity challenges. As a technology fellow, he supports all of Imperva's business functions with his more than two decades of security industry experience and expertise.

'Cloud First'

TOM FIELD: Suddenly every organization now is "cloud first." We know as organizations have rushed to the cloud over the last quarter or so, there are some things that they've overlooked in terms of configuration and where some of their critical data is stored. What security gaps are most overlooked as organizations suddenly become cloud first?

TERRY RAY: The reality is, we're trying to do a lot of the same things with the cloud that we did on premises, including applying the same networking configuration and applying the same host configuration. One of the problems that this creates is organizations have yet to really define a strong data and application security strategy, even on premises.

And as you move from on premises to the cloud, those specific problems are exacerbated given that everything's based on applications. Off premises, the infrastructure is no longer managed by you. So you wind up with these gaps in visibility.

Compliance Risks

FIELD: What do you see as the biggest potential security and compliance risk for these organizations as they lose this visibility?

RAY: Again it comes down to the fact that if you can't see what's going on, it crosses a boundary of compliance and security. For compliance, you have very explicit pieces of information you must answer basic questions on: Who accessed it? When did they access it? Should they have accessed it? From where did they access it? Traditionally, those were already difficult questions to answer, because to answer those questions, you have to be monitoring that data.

Regulators are asking far more complex and in-depth questions about your data, yet most organizations are moving to a world where they're actually monitoring less of that data than they were on premises. And that becomes worse when we start to talk about the security world. The fact is, you don't know where you're going to lose data. And losing data isn't just a potential regulatory problem; it's an issue for a business. And so you have to monitor even more when you think about the security aspect of it, because you don't know where you're going to get breached, and incident response could need to happen absolutely anywhere. So that lack of visibility is by far the biggest gap that organizations have.

Data Hygiene

FIELD: What should organizations be doing to secure data before they even put it in the cloud?

RAY: First, you've got to know where the data is. You're not going to secure much if you don't know where it is. So there's a data hygiene process that you need to go through. For example, if you have credit card data and there are more users accessing that credit card data than need to be, clean it up. If you have applications that have been developed for the cloud that have extreme rights on the data with the idea that you were going to reel those rights back once they went to production, most of the time, those rights don't get reeled back. So it's time to clean it up and do that data hygiene. And a lot of businesses tend not to do that.

When we try to think about how they're solving that kind of problem, that's really what it comes down to. It's about being able to understand and close those gaps.

> **"First, you've got to know where the data is. You're not going to secure much if you don't know where it is."**

Achieving Compliance Simplicity

FIELD: How can organizations achieve simplicity in compliance, and what are the business benefits?

RAY: Simplicity and compliance aren't two words you usually see together. Typically, compliance is a pretty broad set of requirements depending on where you go with it. Luckily, most regulations tend to be modeled after prior regulations. And so if you take the most restrictive compliance and the most restrictive security framework and combine those two together, usually you're covered for pretty much everything.

Businesses that have taken that approach, usually don't have an issue when it comes down to trying to solve the problems. However, when you think about simplicity and complexity, the complexity comes in how broad these compliance efforts are when you get to the application and data sides of it. Compliance is in place because organizations have lost some things that impacted other people and institutions. Losing credit cards impacts a bank or a financial institution. Losing private data impacts individuals. Because businesses didn't do the right thing out of the gate, there had to be some controls put in place. Now we see businesses saying, "All right, well tell me the minimum I need to do to meet the compliance" so they can do just that.

As you move to the cloud, it's a restart when it comes to data security. All of the databases in the cloud are new. So nobody's putting a 10-year-old version of Microsoft in the cloud. For on premises, the complexity was, you've got versions of databases that roll back into the '90s, and sometimes in the '70s with mainframe and others. When you move to the cloud, it becomes a little bit easier because the scope of what you have to secure is significantly smaller.

The way you monitor those systems has also changed. On premises, you can install an agent. In the cloud, you can't install an agent because it's a managed database. So what you're left with is native logging or monitoring traffic on the wire. And this is what you see in the cloud now today.

To simplify all of this, one of the things we're doing specifically, is saying, don't put a proxy in; don't put an agent in. Be able to monitor all access to that data, but be able to do it without impacting the performance of it, by not having infrastructure installations of proxies and agents. At Imperva, we're monitoring every database you have; we're classifying the data and we don't need to scan the system.

So what you wind up with is an instant regulatory compliant environment that includes both the regulatory side, as well as the security side to get what you expected out of the cloud: A simpler world for being able to secure what's most critical to you.

Cloud Data Security at Imperva

FIELD: Talk a bit more about what you're doing at Imperva to help customers secure data for the cloud.

RAY: We introduced a technology called Cloud Data Security (or CDS), a cloud-native data security solution.

Imperva has been doing data security for almost 20 years. Our on-premises product was designed to solve all those problems we talked about a minute ago. But for the cloud, we built this technology - cloud data security - working with financial institutions, healthcare organizations and others to streamline it down to what you specifically need.

You don't need to be a data security or cloud expert. All you need to know is that you have a problem and that problem is you don't have visibility into where your data is in the cloud. And you want that visibility without having to install anything and without having to wait months or years to get results.

So if you turn on native logs in the cloud, we can collect those native logs, do the classification and then do the analytics behind that. What it means is we know where your data is. We know everybody who's touching it when they touch it. And we can tell you whether they are supposed to touch it.

And we're not going to keep your data. We simply take that data, analyze it, give you the results of it and then we pass back the data into the customer's own Amazon S3 bucket stored in their own environment. ... The idea is simplicity. You don't need to install anything. You don't need to be an expert, and you can get it up and running in minutes.

> **"Compliance and security are two sides of the same coin. So once you have that compliance piece, you tend to move that into a higher level of importance where security is going to come into play."**

The Future of Data Security

FIELD: As you look toward 2021 and beyond, how do you see enterprise data security evolving?

RAY: If you asked me that question two or three years ago, I'd probably give you the same answer. Data security is one area where most organizations are not very forward thinking. In my opinion, most organizations wouldn't be solving the data security problem if they weren't forced to do regulatory compliance.

We're seeing some changes of that with CCPA [California Consumer Privacy Act], the EU's GDPR [General Data Protection Act], the Nevada privacy law, the Washington state privacy law and other privacy laws. These consumer privacy laws are going to drive a lot more activity in terms of protecting personally identifiable information, which means a lot more businesses and industries are going to find themselves in the crosshairs of regulatory compliance. And that's a first step in moving the problem of data security out of a DBA's hands. DBAs are great people, but at the end of the day, they're not security.

Compliance and security are two sides of the same coin. So once you have that compliance piece, you tend to move that into a higher level of importance where security is going to come into play.

"You need to monitor all of this and you need to secure all of that," sounds like the same solution to me. So in 2021 and beyond, these privacy laws are going to drive a lot of overall data security. And I also see the two markets of data privacy and data security collapsing into each other. ■

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANKINFO SECURITY® CUINFO SECURITY® Just for Credit Unions GOVINFO SECURITY® HEALTHCAREINFO SECURITY®

infoRisk® TODAY CAREERSINFO SECURITY® Data Breach® Prevention. Response. Notification. TODAY CyberEd.io

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io