Skyhigh Security

Data Protection: Data Has No Jurisdiction

Skyhigh Security's Rodman Ramezanian on Securing Data From Devices to the Cloud

ISMG INFORMATION SECURITY MEDIA GROUP

Rodman Ramezanian

Ramezanian has over 11 years of cybersecurity experience. At Skyhigh Security, he is responsible for technical advisory, enablement, solution design and architecture, and he primarily focuses on Australian federal government, defense and enterprise organizations. He specializes in adversarial threat intelligence, cybercrime, data protection and cloud security. Ramezanian has a passion for articulating complex matters in simple terms to help the average person and new security professionals understand the what, why and how of cybersecurity.

"Data is the new oil" is an increasingly popular refrain, and there's no doubting data's importance in keeping the wheels of business in motion. Today's data also is highly prized by cybercriminals, said **Rodman Ramezanian**, global cloud threat lead at Skyhigh Security.

In fact, over 80% of data breaches are instigated by financial motives, according to Verizon's 2022 Data Breach Investigations Report.

Nowadays, Ramezanian said, data flows from devices through the web to the cloud. It is accessible everywhere, anytime, and is constantly growing as it moves throughout an organization. Vast amounts of data are flowing from internal and external sources, and as a result, data has no jurisdiction, he said.

"Imagine how difficult the task of protecting that data across all these different scenarios becomes, especially when security teams don't have a standardized platform or methodology to get visibility, governance and control of their data wherever it goes," Ramezanian said.

In this podcast with Information Security Media Group, Ramezanian discussed:

- The underlying threats to data and why they continue to pose risks;
- How security teams can ultimately defend themselves and remain secure;
- The mindset security leaders must embrace in the future.

“When data was only kept and accessed within the company’s walls, it wasn’t so onerous to stay on top of where it existed in an organization. But now, you’ve got data flying around all over the place, being accessed anytime, anywhere, from any device and any user.”

Data Protection Challenges Today

CAL HARRISON: 2023 is now well underway, and data breaches show no signs of slowing. What’s so challenging about protecting data in this day and age?

RODMAN RAMEZANIAN: Data has always been the lifeblood of any organization. There’s no denying how important data continues to be in the context of keeping a business operational, productive and functional. Data has always been in the crosshairs for the threat actors, who have always been hunting down data for their own personal or financial gain. And thanks to the pandemic over the past few years, major digital transformation projects have accelerated all the enterprise migrations to cloud platforms. A growing number of organizations are adopting multiple clouds to complement their strategies.

Businesses all over the world are taking a multifaceted approach to using, sharing and storing data across their users’ devices, corporate web servers, applications, platforms and storage services. There are so many ways to create, edit, distribute, access and save data. Some data may need to be classified differently or handled in a certain way for regulatory reasons – perhaps catering to devices that are used to access that data from certain places that might not be as secure as you’d like them to be. Imagine how difficult the task of protecting that data across all these different scenarios becomes, especially when security teams don’t have a standardized platform or a methodology to get visibility, governance and control of their data wherever it goes.

‘Data Has No Jurisdiction’

HARRISON: Why do you think organizations have struggled with this issue?

RAMEZANIAN: Data plays such a huge role in keeping an organization alive, and it typically flows to wherever it needs to go for productivity to keep on pumping. You could say that data has no jurisdiction. It will go to wherever it needs to be shared to fuel business operations. When data was only kept and accessed within the company’s walls, it

wasn't so onerous to stay on top of where it existed in an organization and to know what it consisted of, how it was classified, who was accessing it and on what devices. But now, you've got data flying around all over the place, being accessed anytime, anywhere, from any device and any user. That's the whole premise of cloud computing. You've got the public cloud. Data isn't within the company walls, and it requires a very different approach.

We can't use the tools and methodologies of yesteryear to tackle the problems of today. Security should aim to be a business enabler, not an inhibitor. Security teams shouldn't try to limit the flow of data; they should enable data to be used to its fullest potential and go where it needs to go to help the business thrive. But in the absence of a unified platform for security teams to have end-to-end visibility of where their data is going and who's accessing their cloud apps and services that may contain corporate data and to control safe use and sharing of that data, it's easy to see why organizations continue to struggle with these issues.

Who Is Responsible for Data?

HARRISON: In an environment where data knows no boundaries, who is responsible for that data?

RAMEZANIAN: It's important to remember that cloud service providers provide some security protection. The shared responsibility model outlines where the responsibilities lie, but that doesn't mean that the cloud data is fully secure. Cloud service providers correctly point out that the responsibility isn't theirs alone, hence the concept of the cloud security shared responsibility model. For example, Microsoft publishes their model for their cloud computing resource, which is Azure. Amazon has

a similar approach for Amazon Web Services. Both of these models point out that a secure infrastructure relies on the customer playing their part to make the system truly secure and compliant.

Ultimately, the customer's own data that goes into these cloud environments is still their own responsibility. And as a result of that, the user, device and data controls need to work together with cloud computing, especially as that data moves to the clouds and between clouds and goes from on-premises to hybrid environments. In all these different scenarios, the customer needs to keep in mind that the data is still ultimately their own responsibility.

Enable Business Without Sacrificing Security

HARRISON: At Skyhigh Security, you see the threat landscape changing every day. Do you see this problem worsening as time goes on?

RAMEZANIAN: It's definitely not getting easier. There's no shortage of new devices coming online that enable access and productivity, such as mobile devices, tablets and IoT devices. The average user owns about four or five devices nowadays. And there are more and more cloud platforms and services that offer leading-edge features for data usage and sharing among peers and business partners. The more cloud services and infrastructures expand and adoption keeps increasing at huge scale, security teams need to keep up with the flow of data to make sure that it's secure wherever it goes, at any point in time.

Security teams can't afford to get complacent with data protection. In 2022, there were some high-profile data breaches across the globe. Some really big tech firms unfortunately fell victim and had their data breached. When you consider that data has no jurisdiction or bounds, you can either be the security leader who holds back the business by restricting data accessibility and trying to put tethers on how data can react and where data needs to go, or you can be the leader who securely enables the entire business to thrive without compromise and without sacrificing the security of the data.

Set Guardrails for Safe Data Use

HARRISON: How can organizations turn the tide and make positive progress toward protecting data?

RAMEZANIAN: Organizations cannot afford to view data protection as a one-off or a deferral expense because of the abundance

of opportunities for data leakage and data theft nowadays. The first step to solving any problem is knowing what you're dealing with. And before you can protect anything, you need to know who's storing what and where. The amount of data that's kept by most enterprises, whether it was migrated from on-premises or originally stored in the cloud, is vast, and it's critical that security teams get a handle on what they're up against.

But since data can flow practically anywhere, security teams can't put all their eggs in one basket – for example, by just having cloud protection. There is a wealth of data sitting on corporate laptops and devices. It's flowing through their internet gateways and many other realms beyond cloud buckets, blobs and other storage services. A quick win for a security team is to set guardrails that predicate safe data usage. There are so many potential leakage points for data – plugging in removable media devices, taking print screens, posting data on a public forum through a web vector, accidentally leaking out something to freepdfconverter.com for a business report that's coming up, or emailing something to your personal account to work on it later, from home.

It's important to have a unified, standardized approach that gives security practitioners end-to-end visibility of everything – from the point of data creation to where data has been copied and shared, whether it's been accessed from an unknown location at a suspicious time on a device you've never seen before, whether it's a storage device that's configured a certain way, or perhaps someone's taken a photo of some sensitive data and uploaded a screenshot or used optical character recognition to spot a leak. Security teams need to set guardrails on what constitutes safe usage and what doesn't.

Adopt a Converged Platform

HARRISON: 2022 was a pretty rough year in terms of data protection. A number of high-profile organizations felt the brunt of some large data breaches. Looking to the future, what do organizations need to do to remain safe and keep their names out of the news headlines for the wrong reasons?

RAMEZANIAN: Security features within public cloud platforms and public services like AWS and Azure will get better as time goes on. They will get stronger and more feature-rich. But there are a number of fundamental nonnegotiables that security teams and organizations cannot neglect. They need to identify and classify their data; know where and how their data is being stored, shared and used; and determine how it needs to be protected across all these vectors at all times. Attackers know how valuable your data is in their own hands. They have ample opportunities to try their skills to get access to it. ChatGPT is actively assisting threat actors in their efforts to attack systems. It is helping attackers craft phishing emails and formulate exploit attacks.

“Our entire portfolio and our platform is underpinned and converged with data protection across devices, web, and cloud vectors. We give security teams end-to-end visibility so they can see where data has flowed, across any vector.”

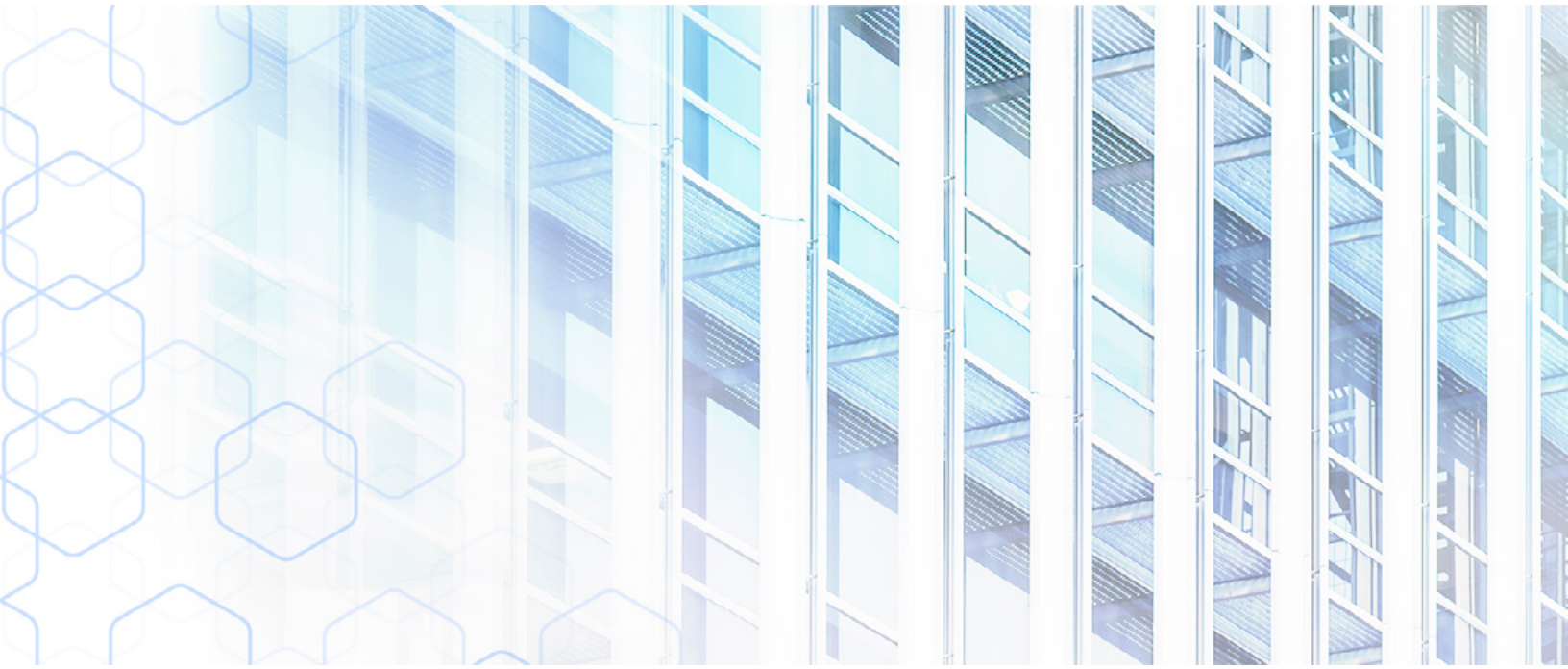
The attack surface is intensifying. We’re not just up against highly skilled attackers anymore. Gartner predicts that by the end of 2024, 75% of the world population will have its personal data covered under modern privacy regulations. So on the privacy and regulatory front, organizations have to continue their efforts to remain compliant and uphold their own protections. Security leaders need to get the basics right. They should be looking to adopt a converged platform that will not only protect their data without compromise across any jurisdiction but will give them the ability to do that everywhere it goes, whether it’s on devices, going through their web infrastructure or on their cloud platforms.

The Skyhigh Security Approach

HARRISON: What are you hearing from your customers about data protection challenges, and what advice are you giving them?

RAMEZANIAN: What was old is new again. Back in the day, it was all about social engineering and tricking people into doing something that they weren’t aware of. Then the threat landscape moved into more sophisticated things like zero-day threats and leading-edge viruses. But social engineering has been rearing its ugly head again, and many organizations have been struggling with it, especially at a time when businesses have modernized their digital workspaces and are using the web and cloud from all sorts of locations, with different devices, at different times.

Skyhigh Security helps protect these organizations with cloud-native security capabilities that are data-aware. They’re aware of data wherever it may go and how to mitigate threats, and they’re super simple to use. Gartner and Forrester have said we’re leaders in the security service edge space. Our platform goes beyond data access to data usage, which allows businesses to collaborate from any device without sacrificing security. What makes Skyhigh Security different is that our entire portfolio and our platform is underpinned and converged with data protection across devices, web, and cloud vectors. We give security teams end-to-end visibility so they can see where data has flowed, across any vector – not just cloud or devices that are locally present.



We know data. It's who we are.

Discover Skyhigh Security for your business.

Skyhigh Security goes beyond securing data access—it secures how sensitive data is used. We extend the security control point beyond the network to the data itself. As it moves across the web to software-as-a-service applications, cloud applications and platforms, and even endpoints, we protect it with a single policy that moves with your data instead of being tied to each access technology. Our easy-to-use, integrated platform enables organization-wide data protection, streamlines data security operations, and reduces complexity.

More information at www.skyhighsecurity.com.

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

BANK INFO SECURITY® CU INFO SECURITY® (Just for Credit Unions) GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY (Prevention. Response. Notification.) CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

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