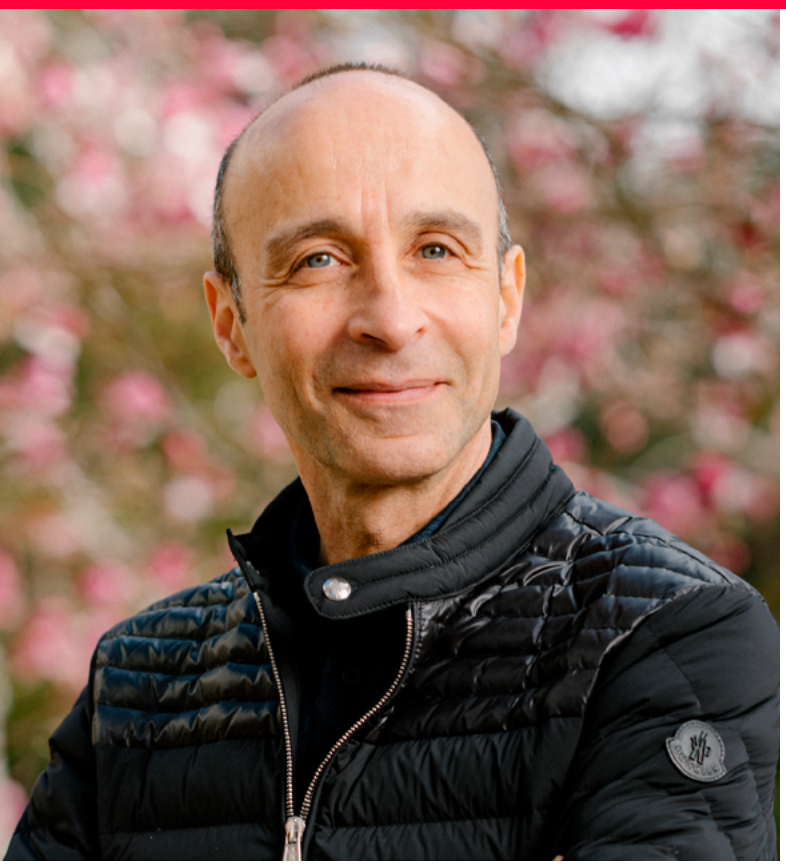
Normalyze™

Evaluating Cloud Security Across the Enterprise

Rapid Cloud Adoption Created New Businesses With More Security Challenges

ISMG
INFORMATION SECURITY
MEDIA GROUP



Normalyze™

Amer Deeba

Deeba has extensive experience in driving product, marketing and sales go-to-market strategies for enterprise and cloud technologies and driving company growth in fast-moving technology fields. Previously, he worked with Moogsoft and Qualys. In his 17-year stint at Qualys, he led all aspects of marketing, business development, strategic alliances and global enterprise accounts.

The transition to the cloud at a very fast pace during the pandemic affects information security to this day, said **Amer Deeba**, co-founder and CEO at Normalyze.

"Companies wanted to innovate and create new business processes to serve the customers better and faster. And with all that came a lot of innovation, a lot of building in the cloud, and a lot of data moving into the cloud," he said.

But the move to cloud introduced new security risks. Many organizations face challenges in understanding where the data is going in cloud environments and how to implement measures to secure it. Fortunately, companies are now evaluating these concerns and looking for ways to address these challenges, he said.

In this video interview with Information Security Media Group at RSA Conference 2023, Deeba also discusses:

- The most challenging aspects of cloud visibility;
- The importance of building the right security skills;
- How Normalyze helps customers secure their data.

"Security teams need to have the right framework and the right architectural point of view to get visibility and control on an ongoing basis so they can stop threats and be able to be proactive and stay ahead of the game."

Post-Pandemic Cybersecurity Challenges

ANNA DELANEY: What has changed the most in this post-pandemic world in the cybersecurity landscape?

AMER DEEBA: The pandemic changed a lot of things, but what impacted information security the most is the fast move into the cloud and all the transformation that happened at a very fast pace. Companies wanted to innovate and create new business processes to serve the customers better and faster. And with all that came a lot of innovation, a lot of building in the cloud, and a lot of data moving into the cloud. All of that created a lot of opportunities, but a lot of challenges came with it from a security perspective. And companies now are taking a step back and trying to look at all of that and figure out what's the best way to address it – how to secure these cloud infrastructures and all the data that's piling in.

Normalyze is a 2-year-old company. We were born and built in the cloud. A lot of our customers are facing the challenge of trying to understand where their data is going into these cloud environments and how to secure it. Some of the basic questions we hear from them are: Where's my sensitive data? Who has access to it? What type of access do they have? How can I manage all the risk that the data contains and the compliance challenges that come with it? It's a big problem, especially if you're trying to do it across multi-cloud, and every company these days is in a multi-cloud environment. So they have to get the visibility and control of the data that they had when the data was on-premises, and security teams are trying to solve this problem at scale.

Achieving Visibility in the Cloud

DELANEY: What's the most challenging aspect of visibility? Where are organizations struggling to get that full view?

DEEBA: Data in the cloud got spread in so many ways across structured and unstructured data. You've put some of it in a platform as a service or infrastructure as a service or in block storage. It's hard to discover, and it's hard to find where the sensitive data is. It's hard to understand where the risk paths are that can lead to a data compromise, breach or ransomware. And figuring that out as it's happening in real time is a challenge for businesses. Security teams need to have the right framework and the right architectural point of view to get visibility and control on an ongoing basis so they can stop threats and be able to be proactive and stay ahead of the game.

Why Visibility Is Needed

DELANEY: What missteps do organizations make when it comes to accessing data in the cloud?

DEEBA: The main issue we hear from customers is the lack of visibility that they need to have so they can make decisions in real time – getting the telemetry from the various components within their cloud infrastructure – the assets, the data, the access – and bringing all these pieces together and connecting them in a way that gives them intelligence and allows them to make decisions quickly. If data exfiltration or an attack is happening on your data, you need to immediately know that it's happening and act upon it in real time, or even be proactive and figure it out before it happens. This needs to be done in an intelligent, scalable, efficient way so you can bring all this information into one place and have visibility on an ongoing basis.

Steps to Improve Visibility

DELANEY: What's your advice to organizations on practical steps they can take to gain visibility and proactive security status?

DEEBA: Companies should start with the basics: They moved into the cloud. They have all these cloud environments that they are innovating, and now they need to figure out where everything is and get a clear inventory of all the data and the infrastructure pieces that connect to it, who has access to that data and what type of access they have – so they can make decisions based on that. Once you get that visibility, it becomes much easier to make decisions and then to make the right proactive choices. For example, if you learn that you have access to a data store in the cloud that contains sensitive information, but you haven't touched that data store for six months, why should you have access to it? Having that information makes the decision-making simple and prevents a lot of expensive data breaches from happening in the future.

Skills Required for Cloud Security

DELANEY: The cloud environment is quite new for companies. What skills do the security teams require?

DEEBA: Cloud security teams are heroes these days because they have a lot to do and manage, and the changes in the cloud and CI/CD cycle are happening so fast. They need to understand how to build and scale in the cloud and then build the right framework around it from a security perspective, using the right tools to build the right solutions that can help you manage the problem in a systematic, organized way and stay ahead of the game.

Mostly Multi-Cloud Environments

DELANEY: What are your thoughts on one-cloud providers versus multi-cloud environments?

DEEBA: These days, we very rarely hear that customers are in one cloud environment. Pretty much everyone is in a multi-cloud environment because of cost and compliance and because some environments are better than others, for example, by providing better tools for AI and machine learning. So it depends on your use cases and the application that

“Be open to this new innovation and to exploring new ways to do things out of the box. Think differently so you can solve problems better and faster and have more security for your company, your customers and your data.”

you’re building, but more organizations are moving into multi-cloud environments. Whatever you’re building in the cloud needs to understand that type of environment and be able to innovate in that fashion. Of course, with that comes the other challenge: It makes things more complicated because you have to do it across multiple clouds. But again, if you build the right framework for your security and you bring the right tools that can work in a multi-cloud environment, then you’re approaching it the right way and you’re going to be fine.

Compliance and Regulation

DELANEY: How do you see the space evolving over the next year, particularly when it comes to compliance and regulation?

DEEBA: Compliance and regulation are not going away, and that is a good thing for information security because it helps bring the rigor. It makes organizations look for visibility and bring control back so they can see where things are and how to secure them and how to scale that in a multi-cloud environment. We have to prepare ourselves so we can provide data to our data officers and compliance officers at any time.

Staying One Step Ahead

DELANEY: What’s your advice to organizations on staying one step ahead of what’s coming?

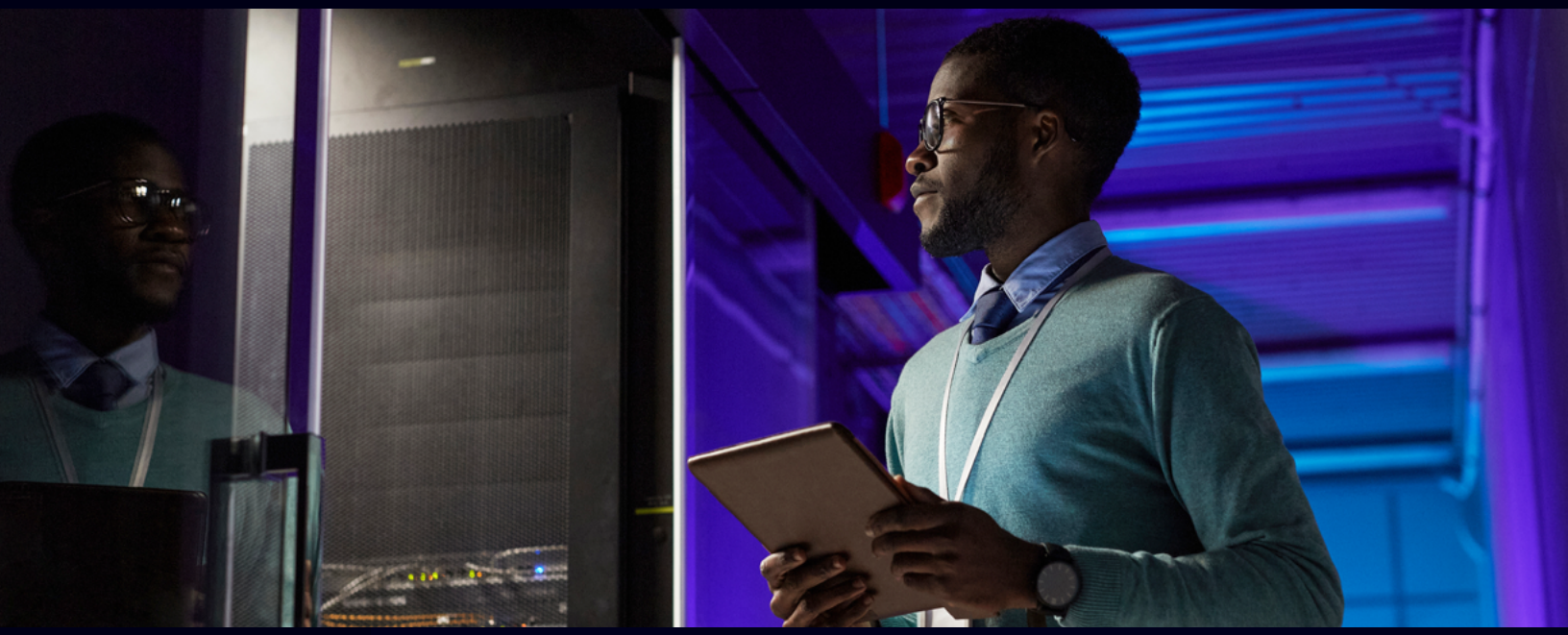
DEEBA: Don’t try to do everything yourself. There’s a lot of innovation out there and a lot of solutions that can really help you do it faster, more efficiently, and better in some cases. Be open to this new innovation and to exploring new ways to do things out of the box. Think differently so you can solve problems better and faster and have more security for your company, your customers and your data.

The Normalyze Approach

DELANEY: How does Normalyze help its customers?

DEEBA: We are a data security platform for everything you build and run in the cloud. We cover on-premises too. We help customers discover where their sensitive data is and how to secure it, and we do that for data at rest and data in motion across all types of cloud environments, in the most effective way possible right now. We’re constantly innovating. We help organizations solve problems at scale.

Normalyze™



About us

The rise of cloud computing and the resulting data sprawl is creating many security and compliance challenges for organizations across the world. Today, enterprises find their most important asset - their data - scattered throughout multiple cloud environments, and security teams are hampered by limited visibility and control. More data movement means more exposure and risk, so both data security posture management and around-the-clock monitoring of this movement across the environment is key to securing the data and preventing expensive breaches from occurring. With Normalyze you can discover, visualize, and secure all your cloud data in minutes. You can respond to data threats immediately and prevent damaging data breaches - without spending days on manual discovery or drowning in alert noise. The Normalyze cloud-native platform manages data security posture and compliance by automatically tracking all risks to sensitive data, visualizing who can access what, and quickly blocking unauthorized access or vulnerable points of attack. With data-in-motion, data lineage, and anomaly detection capabilities, security teams can continuously identify cloud-resident sensitive data, both at rest and in motion, to secure access paths and reduce the risk of breach.

Click to learn more: **normalyze.ai**

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 Just for Credit Unions INFO SECURITY® 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