Introduction

With enterprises of all sizes embracing hybrid cloud infrastructures, knowing where the most sensitive company data resides is key to creating a secure environment.

In healthcare, knowing where data is, who has access to it and how it's protected is a crucial part of keeping up with myriad regulations and compliance checks. With zero trust, healthcare CISOs will have a better sense of the attack surface as newer technologies, such as IoT devices and sensors, are introduced.

To learn more about how a zero-trust framework can secure your enterprise, please join me for an exclusive executive roundtable on **How Zero Trust Can Secure Your Hybrid Cloud Environment**.

Guided by insight from Sandy Dalal, director of IAM at the pharmaceutical company Allergan, this invitation-only luncheon will draw from the experiences of the attendees who will offer their insights on the zero-trust model. Among the discussion topics:

- How can zero trust improve your identity and access management practices when moving to a hybrid cloud model?
- Why is a zero-trust approach essential as healthcare organizations undergo mergers and acquisitions and security teams deal with the risk and exposure that brings?
- How can healthcare organizations improve the on-boarding and off-boarding processes, especially as they look to automate more of these interactions?

You'll have the opportunity to discuss zero trust with a handful of senior executives and market leaders from the healthcare industry in an informal, closed-door setting, from which you will emerge with new strategies and solutions you can immediately put to work.

Discussion Points

Among the questions to be presented for open discourse:

- As more healthcare organizations move to a hybrid cloud model, how does the zero-trust model and identity and access management technologies ensure that data is protected?
- As organizations consolidate, how can zero trust help reduce risk when integrating infrastructures?
- How can new technology help healthcare organizations improve the on-boarding and off-boarding process for employees?

About the Expert

Joining our discussion today, to share the latest insights and case studies is:

Sandy Dalal

Director of IAM
Allergan

As head of I&AM services at the pharmaceutical company Allergan, Dalal is accountable for global service delivery and lifecycle management of identity, account management and end-user access management processes. He has over 15 years of diversified experience serving clients within the commercial and public sectors, specializing in IAM, cybersecurity strategy and data governance and protection. Prior to joining Allergan, Dalal was a senior manager in PwC's advisory cybersecurity and privacy practice, focusing on helping companies architect, design, manage and implement complex security transformations across multiple industries.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to both secure and manage their extended enterprise and transform their customers' experiences. With over 5,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely adopt the technologies they need to fulfill their missions. Over 4,350 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to securely connect their people and technology.

For more information, please visit www.okta.com.

About the Moderator

Leading our discussion today is:

Scott Ferguson

Managing Editor, News
Information Security Media Group

Ferguson has been covering the IT industry for more than 13 years. Before joining ISMG, he was editor-in-chief at eWeek and director of audience development for InformationWeek. He's also written and edited for Light Reading, Security Now, Enterprise Cloud News, TU-Automotive, Dice Insights and DevOps.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 the 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 cyber security challenges.

For more information, visit www.ismg.io.

CONTEXT

How Zero Trust Can Secure Your Hybrid Cloud Environment

Q&A With Sandy Dalal of Allergan

NOTE: In advance of this event, ISMG's Scott Ferguson spoke about zero trust with Sandy Dalal of Allergan. Here is an excerpt of that conversation.

Healthcare Challenges

SCOTT FERGUSON: What are some specific challenges that healthcare organizations and pharmaceutical firms are facing today?

SANDY DALAL: Allergan is the second most targeted pharma company from a threat perspective because Botox, which is owned by Allergan, is highly targeted. We see brute force attacks, phishing, etc. Allergan intelligence estimates 150 credentials are stolen per month.

And to do that, we need to protect the company reputation and brand recognition. The way we approach networks has changed over time as well.

Because we look at collaborative R&D partnerships, protecting this IP is increasingly difficult. It's important to make sure people are comfortable dealing with your products and services. And to do that, we need to protect the company reputation and brand recognition. The way we approach networks has changed over time as well. Historically, we had a security perimeter and firewall to determine what is trusted. Now we're going for digital initiatives and we have remote workers in the field and a distributed network.

The traditional security perimeter with a "moat and castle" approach no longer works. So we need to find a security model that works for a hybrid enterprise, and we're doing that with a zero-trust framework.

Zero Trust

FERGUSON: What does it take to implement a zero-trust architecture?

DALAL: In order to achieve better security outcomes at Allergan, we looked to see how we could modernize how access works. We're not a DevOps organization, so we needed to modernize and work with partners, rather than build something ourselves.

Looking at the zero-trust maturity curve, we started our zero-trust architecture with an IAM [identity and access management] ecosystem to make sure the right people had the right access at the right time, which we built with Okta. It's important to start with SSO [single-sign on] and PAM [privileged access management]. We have 400 plus apps connected to Okta SSO and require MFA [multifactor authentication] to access Okta. MFA is required for all VPN access to our network.

Sandy Dalal

In order to "Never trust, always verify," we need technologies that include:

- Workday, making HR as the single source of truth to automate provisioning and deprovisioning;
- SSO across Web-based apps;
- Privileged access management;
- ServiceNow for ticketing;
- Identity governance with RSA.

Stage 2 of the Zero Trust Maturity Curve includes implementing MFA to all employees and contingent workers, starting with adaptive policies (i.e. on/off-network). For Stage 3, which will happen over the next six to 12 months, we'll move toward an adaptive workforce with risk-based access policies. As part of this, we're working to eradicate passwords. We will, of course, still have apps that require passwords, but we're looking for ways to reduce friction for the users where possible.

The key takeaways, for me, are that it's important to work with a partner who has a zero-trust mindset and supports the different tools you use to easily integrate with your landscape.

> "Real-time synchronization is huge for security. If you change roles or leave the organization, your level of access also needs to change, especially if someone is leaving the organization.."

Securing Hybrid Environments

FERGUSON: In a hybrid cloud environment, how can security leaders protect sensitive data, especially as it moves from on-premises to service providers' infrastructures?

DALAL: The move to the cloud and being comfortable with it comes down to ensuring you have controls in place. Fundamentally, we can't expect that cloud apps support field-level encryption. We look at technologies, such as RedLock and Palo Alto Networks, to give you better visibility for the cloud. I believe a cloud-first model is more secure, and if cloud vendors don't focus on security, they'll go out of business.

We use a number of best-of-breed tools that integrate with Okta. Exabeam as our SEIM [security event information management]. Palo Alto Aperture as our CASB [cloud access security broker] can detect anomalies to report back to Okta.

There are challenges when moving to the cloud, but by partnering with security-minded vendors that understand our companies' challenges, we can move to the cloud securely. If we can move an app to the cloud, that's our first choice. We have a massive cloud transformation program going on right now that moves some of our legacy systems to the cloud.

We also have a strong R&D and a lot of on-premises investments that we can't move away from. We've hooked in Okta MFA to our VPN so that anyone connecting to our VPN will be prompted with MFA to secure access as best as we can.

We're also working on threat insights and threat monitoring for security incident response and endpoint management. We work with best-of-breed vendors to support this and can integrate with Okta not just for SSO but also from a security perspective for visibility.

We're a global company and are subject to different compliance requirements (i.e. GDPR). The audit teams ask us to provide a list of sensitive fields that may have PII data, and so we're thinking about the data we're storing and how we can secure that.

Security After M&A

FERGUSON: When it comes to mergers and acquisitions, how can organizations protect themselves from security issues they inherit?

DALAL: In the last five years, have done about 50 acquisitions – it's a big part of our culture. When we acquire a new company, we don't give them access to our networks right away or create trust between our networks right away. We use tools to identify network vulnerabilities and make sure we get to a standard acceptance level of trust before we give them access between networks.

We need to make sure we're not introducing vulnerabilities through an acquired company. If a company we acquire uses cloud apps, we connect them to Allergan's Okta instance right away. If they're on-premises, we integrate into our network. User accounts become part of Allergan infrastructure, so we're not maintaining separate apps and security policies separately. And we lift and shift applications to Allergan's network over time

Automating the Process

FERGUSON: How are you automating and securing employee on-boarding and off-boarding processes?

DALAL: We've deployed Workday as a master, which is where our HR system (Workday) is the source of truth. This allows us to translate an HR event to the level of access an individual has.

Real-time synchronization is huge for security; if you change roles or leave the organization, your level of access also needs to change. Especially if someone is leaving the organization, we need to ensure access is immediately revoked.

All users in AD are mastered by Okta, and any identity is sourced out of Workday, so we don't have orphan accounts laying around. With a zero-trust strategy, you definitely need to manage this access. And it's very important to manage what people can see and do. ■

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 cyber security challenges.

Contact

(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. Prevention. Response. Notification. TODAY · CyberEd.io

iSMG
INFORMATION SECURITY
MEDIA GROUP

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