

# AGENDA

Cloud Security

# Cloud Security

## SPEAKERS



**Stephen Alexander**  
BISO  
MassMutual



**Alan Pawlak**  
VP Information  
Security  
Johnson & Johnson



**Richard Daigle**  
CIO  
Griffin Health  
Services



**Hari Subramanian**  
IT Managing Director  
Cigna



**Al Koch**  
Account Executive  
Veracode

# VERACODE

[Click Here to Register](#)

## CLOUD SECURITY



**March 31, 2022**






5:30 PM-9:00 PM

Eastern Time

According to Gartner 79% of companies have experienced at least one cloud data breach during the pandemic. Remote work is here to stay, and the concept of securing a perimeter has essentially ended. Traditional application security measures are broken. The need to innovate faster and shift to cloud-native application architectures isn't just driving complexity, it's creating significant vulnerability blind spots also. Under the thumb of the pandemic, enterprises and IT leaders had to look for tech solutions that were

resilient and agile to empower the remote workforce. To sustain business continuity plans, organizations shifted workloads to the cloud. As much as cloud adoption offers flexibility and productivity, it also exposes organizations to cyber threats and data breaches. So the question remains if moving to the cloud is the right thing to do and if so how to protect it from the new risks given that most organizations believe that application security should be completely automated to keep pace with dynamic clouds and rapid software development practices.

## PANELISTS

				
<b>Alan Pawlak</b> VP Information Security Johnson & Johnson	<b>Hari Subramanian</b> IT Managing Director Cigna	<b>Richard Daigle</b> CIO Griffin Health Services	<b>Stephen Alexander</b> BISO MassMutual	<b>Al Koch</b> Account Executive Veracode

IN PARTNERSHIP WITH

**VERACODE**