DAY 1 Oct.21

10:30 AM ET
Conference opens

11:00 AM - 11:45 AM ET
Keynote: Mixing Old and New: Shoehorning Legacy Apps Into Cloud Environments
Frederick “Flee” Lee, Chief Security Officer at Gusto
Most organizations have at least a few legacy systems and applications at any given time that they can’t seem to part from. And while they pose a security challenge in any IT environment, they can be doubly problematic when attempting to transition to the cloud. So can organizations hold tight to those legacy apps, while still taking advantage of all that cloud has to offer – without introducing new vulnerabilities or sacrificing functionality? And then when organizations bite the bullet and decide to update, or even transition from, a legacy app operating within the cloud, what must they keep in mind to ensure data is not compromised? This keynote presentation will show attendees how to securely mix the old with the new in a cloud environment.

11:45 AM - 12:00 PM ET
Visit exhibit hall

12:00 PM - 12:30 PM ET
Evolve Your Cybersecurity in the Cloud
Richard Beckett, Senior Product Manager, Sophos Public Cloud Security Team
Recent high-profile incidents have shown that more cyberattacks are targeting cloud environments. In these scenarios, hackers have taken advantage of gaps in protection, team responsibilities, and cloud security knowledge. Now more than ever, organizations must fully understand the security responsibilities they share with cloud providers.

Join us to learn how to:
• protect users,
• safeguard applications, and
• protect data across every cloud.

12:30 PM - 12:40 PM ET
Visit exhibit hall

12:40 PM - 1:10 PM ET
Solid Cloud Security in An Unpredictable 2020
Rodrique Boutros, Cloud Security Architect, Check Point Software
Cloud adoption continues to increase in 2020. However, getting a grasp on properly securing your cloud footprint comes with its own unique challenges. For example: How do you ensure
data privacy and confidentiality in an everchanging, dynamic environment? Are your existing security tools still effective when used with cloud platforms? This session will cover these topics and trends, while also providing some insights to ease your transition from on-premises to cloud technologies.

This session will:
- review some key findings from Check Point Software’s “2020 Cloud Security Report;”
- discuss current cloud threats; and
- provide best practices to secure your multicloud environments.

1:10 PM - 1:20 PM ET
Visit exhibit hall

1:20 PM - 1:50 PM ET
**Knock Your SOCs Off: Modernizing Security Operations**
**Kat Sweet,** Technical Evangelist, Capsule8
As infrastructure and organizational structures evolve, so too must the teams responsible for keeping the lights on evolve their people, process, and technology. So what does this mean for security operations teams? From the brain of a former security analyst building out operations in a cloud-first, zero-trust environment (bring your own buzzword bingo cards), we’ll reflect upon what problems we’re trying to solve in security operations and how to reimagine solutions for the environment in front of us, whether it’s a newly-distributed workforce, shiny new cloud infrastructure mixed with old servers in the basement, or a fleet of unmanaged endpoints.

1:50 PM - 2:00 PM ET
Visit exhibit hall

2:00 PM - 2:30 PM ET
**CASB: Better Security and Compliance in 30 days**
**Chris Stack,** Cloud Security Solutions Architect, Proofpoint
This year, more that 75% of companies’ workforces are working from home, and many are accessing sensitive data via personal devices. To ensure security and business continuity, companies must digitally transform and accelerate adoption of cloud applications and services. Your people are your new perimeter. So how do you protect them from cloud threats and secure sensitive data?

Attend this presentation and learn how to:
- prevent, detect, and remediate cloud account compromise and post account takeover activities;
- secure sensitive data in cloud apps and IaaS buckets/containers;
• discover and govern cloud apps, including third-party apps; and
• identify misconfigurations and compliance issues across your IaaS environment.

2:30 PM - 2:40 PM ET
Visit exhibit hall

2:40 PM - 3:10 PM ET
When to Use Provider Encryption: Bring Your Own Key and Bring Your Own Encryption for Public Clouds
Charles Goldberg, Vice President of Data Protection Product Marketing, Thales
The 2020 Thales Data Threat Report found that 100% of surveyed organizations have sensitive data in the cloud and 57% of it is encrypted. That is a lot of encryption! Furthermore, the trend shows we are encrypting more often to protect brand reputation, authorize data use, and to meet regulations. However, selecting the right encryption and key management solutions for different cloud use cases isn’t always obvious.

In this webinar we will discuss:
• the available options and tradeoffs, and
• how to streamline supporting the ultimate mix of solutions most organizations need to deploy across their multicloud and hybrid cloud environments.

3:10 PM - 3:20 PM ET
Visit exhibit hall

3:20 PM – 3:50 PM ET
Shift Identity Left: Enable Secure Velocity at Scale
Ivan Dwyer, Group Product Marketing Manager, Okta
To keep up with the rapid pace of innovation, more organizations are adopting the cloud operating model via DevOps practices, building automation pipelines and managing infrastructure as code. The challenge, however, is how to move fast without breaking things. Automating the delivery of software and operations of cloud infrastructure is essential to keep up with the pace and scale of the business, but what about security? With a modern approach to identity, security is no longer an afterthought, but rather part of the process, enabling velocity at scale without compromising your challenging compliance requirements.

This session will cover:
• best practices for securing automated DevOps pipelines, and
• the key role identity plays to ensure the right guardrails are in place.

3:50 PM – 4:00 PM ET
Visit exhibit hall

4:00 PM – 4:45 PM ET
Keynote: Developing a Roadmap Toward Zero Trust in the Cloud
Steve Lukose, Cloud Security Architect, Clari
Zero Trust means different things to different security leaders. But, at the end of the day, it’s a network that relies on identities and not the trust of IPs. Taking a Zero Trust approach to your organization’s cloud environment allows you to implement guardrails that results in definitive user and service directories that are identifiable and managed by policy. At its core, Zero Trust isn’t smoke and mirrors in a cloud environment. There are no false walls placed in the system. But as a security leader managing complex and high-velocity environments, where do you begin to take the steps to reach an ideal state of Zero Trust in the cloud? Attend this keynote presentation to find out.

4:45 PM – 5:00 PM ET
Visit exhibit hall

DAY 2 Oct.22

10:30 AM ET
Conference opens

11:00 AM - 11:45 AM ET
Keynote: 5G and the Run – But Not Sprint – Toward Cloud
Daniel Kroese, Deputy Assistant Director, Cybersecurity and Infrastructure Security Agency, National Risk Management Center
Advancements in technology have made cloud computing more accessible to organizations with critical workloads that previously questioned the reliability of bandwidth, data security, and privacy. But for all the potential of such things as 5G, security containers, and automation, new risks emerge without proper implementation in a cloud environment. So how do organizations strike the proper balance? This keynote presentation addresses ways to ensure threats to the critical infrastructure are properly managed amid efforts to modernize.

11:45 AM - 12:00 PM ET
Visit exhibit hall

12:00 PM - 12:30 PM ET
Who Accessed Your Data in the Cloud? Your Bosses and Auditors Want to Know
Ran Rosin, Director, Product Management, Imperva
Dror Shemesh, Engineering Director, Data Security Cloud and Insights, Imperva
Your business is moving data to the cloud without all the security controls mandated for on-premises deployments. After all, the promised economics and business agility are far too attractive for business leaders to ignore. But attackers are after data, auditors demand evidence, and security is still responsible for protecting data. You need to catch up with that data before attackers and auditors find it, and you need to catch up right now. Join this webcast
to learn how to reconcile Security’s need for visibility with the business’s need for speed and agility – in minutes.

This session will include:

- the fast path to getting control of your data already in the cloud;
- capabilities you will have to bring to make cloud DBaaS secure and audit-ready; and
- how cloud-native data security can be frictionless to the business’s need for speed.

12:30 PM - 12:40 PM ET
Visit exhibit hall

12:40 PM - 1:10 PM ET
**Completing Security Visibility with NDR**

**Steve Porcello**, Senior Security Engineer, Gigamon

As SOCs have matured, they have employed a number of solutions to combat cybersecurity threats. Traditionally, SOCs have relied on SIEM and EDR tools for their detection and investigation needs. While these tools are critical to security operations, they have their visibility limitations. As such, modern security teams have turned to the network for added detection visibility. Network Detection and Response (NDR) solutions provide the necessary visibility not available in SIEM or EDR solutions, and help SOCs complete their security architecture.

This session will discuss:

- traditional security architectures, and
- how to create a modern security architecture using NDR.

1:10 PM - 1:20 PM ET
Visit exhibit hall

1:20 PM - 1:50 PM ET
**The Right Incident Response**

**Abhik Mitra**, Product Marketing, Code42

Despite having a data protection solution in place, most organizations are looking for better threat intelligence, better detection and response, and faster time to mitigation. Policy-driven approaches have left organizations blind to the data security threats that are hard to tag and categorize. To detect and respond to insider threats effectively, companies must deliver better data context to make data protection solutions smarter. Right-size response is all about having the right data context.

Attend this session to:

- learn about common insider threats;
- understand market forces that are challenging today’s security efforts; and
- see how to speed up detection and response to data risk caused by insider threats.

1:50 PM - 2:00 PM ET
2:00 PM - 2:30 PM ET
The Future of Remote Work: Simplify Distributed Operations and Accelerate Response
Tom Kellermann, Head of Cybersecurity Strategy, VMware
Rick McElroy, Cybersecurity Strategist, VMware
Taree Reardon, Senior Threat Analyst & Shift Lead, VMware
Due to remote work environments, CIOs, CISOs, and the teams they lead are faced with the combined challenges of an expanding risk surface area, a disparate staff, and a complex set of tools and workflows. The cloud offers some solutions to these problems, but also exposes vulnerabilities.
This strategy discussion will unpack:

• the cyberattack playbook that attackers have embraced in a remote environment;
• common risk scenarios for a distributed workforce, like a dependence on cloud VPN;
• how to establish coordination and context across workspace security control points.

2:30 PM - 2:40 PM ET
Visit exhibit hall

2:40 PM - 3:10 PM ET
Understanding and Combating Credential Stuffing Attacks
Jamie Hughes, Lead Solutions Engineer, Auth0
Credential stuffing attacks are common threats that can lead to fraud, loss of reputation, and ultimately loss of revenue. In these attacks, threat actors use stolen credentials from one breach to take over users’ other accounts. This is effective because 65% of people reuse passwords across multiple accounts. On some days, these attacks originate from more than 50,000 IP addresses and may account for half of all login attempts. Fortunately, preventative measures exist.

Join this session to learn:
• how credential stuffing attacks work;
• what effect they can have on your company; and
• steps to detect and mitigate these attacks.

3:10 PM - 3:20 PM ET
Visit exhibit hall

3:20 PM - 3:50 PM ET
You Must Address Visibility Gaps to Manage Risk
Lisa Wallace, Field Engineer, FireMon
The proliferation of public clouds adds more complexity and diversity to already complex infrastructures, requiring security teams to enforce network security policies with multiple tools and little to no visibility or automation. You must see your cloud deployments the same way you see your on-prem infrastructures, even when security configurations differ widely. That’s why a unified view that provides a single lens for cloud visibility is needed.

Attend this session to learn how to:
- get a consistent, consolidated view of all systems with context to avoid replicating rules and processes;
- enforce policy-driven control consistently across multi-cloud hybrid environments from a unified platform; and
- make fast, accurate decisions about network security policies without the added risk of misconfigurations.

3:50 PM – 4:00 PM ET
Visit exhibit hall

4:00 PM – 4:30 PM ET
Secure Connectivity Through SASE – Zero Trust Network Access and Protecting Remote Workers
Paul Martini, CEO, CTO, and Chief Architect, iboss
Gone are the times when everybody was bound to their headquarters. Today, the typical network perimeter no longer exists, as the majority of employees work remotely. This requires companies to combine their network and security architectures into a Secure Access Service Edge. Join this session for a technical discussion on best practices in securing connectivity for remote workers, SASE, and ZTNA.

Attendees will gain a better understanding of:
- different cloud architectures;
- cutting edge approaches to ZTNA; and
- best practices when implementing SASE.

4:30 PM – 4:40 PM ET
Visit exhibit hall

4:40PM – 5:25 PM ET
Keynote: How Privacy and Security Go Hand in Hand in the Cloud
Umesh Yerram, Cloud Security and Data Protection Expert
The age of on-prem that featured boundaries is quickly disappearing as organizations are being forced to digitally transform. More often than not, the result is a complex cloud environment that features limitless opportunities, however, it also translates to an expanded attack surface. The benefits that cloud computing provides are too big to ignore for organizations, but as many security leaders know, they’re not inherently secure. Understanding your security and privacy
requirements is essential, but knowing to stitch the two together is part of the foundation of a secure cloud strategy. In this fireside chat, learn tips to build cybersecurity programs and how privacy and security must go hand in hand in the cloud.

5:25 PM – 5:35 PM ET
Visit exhibit hall

DAY 3 Oct. 23

10:30 AM ET
Conference opens

11:00 AM - 11:45 AM ET
Keynote: Developing a Roadmap Toward Zero Trust in the Cloud
Tee Patel, Founder, Iron Oak Security
Cloud environments present enormous opportunities for organizations, especially as many have had to rapidly evolve this year. But with the promise of scalability, mobility, and efficiency, come challenges for the security organization. While technical obstacles seem to receive a lot of attention, one of the biggest challenges is on the governance and compliance front. When you move sensitive information to the cloud, there’s a lot to consider. Depending on your organization, there are a slew of compliance requirements from a data regulation and residency standpoint. So, who should you involve within the business to overcome these challenges? How do you comply with your local state legislation? From a global standpoint, what factors should you consider? Find out the answers to these questions in this fireside chat.

11:45 AM - 12:00 PM ET
Visit exhibit hall

12:00 PM - 12:30 PM ET
Overcome Vulnerability Management Challenges in a Dynamic, Ephemeral Cloud Environment
Scott King, Senior Director of Security Advisory Services, Rapid7
Chris DeRamus, VP, Technology of Cloud Security Practice, Rapid7
Many companies struggle with ephemeral cloud environments. Containers, cloud services, and virtual devices are often spun up and down without the security team’s direct involvement, which is great for moving quickly, but creates risk and leaves security teams unable to monitor or defend their environments. To improve their security posture, companies can design safeguards into cloud services in advance, allowing IT sysadmins to move quickly and safely in support of the business.

Join this webinar and learn how to:
• gain visibility into your multicloud infrastructure;
• allow IT to prioritize the business needs; and
• leverage cloud resources more securely.

12:30 PM - 12:40 PM ET
Visit exhibit hall

12:40 PM - 1:10 PM ET
Packets — A New Hope: Defending the AWS Cloud Using Network Detection and Response
Jeff Deininger, Principal Cloud SE, ExtraHop
Securing cloud workloads present unique challenges, including friction to make native telemetry sources actionable. Using network packets to drive detection and response workflows offers a way forward. Cloud providers offer log-based event and configuration monitoring tools, but real-time detection and response requires the richness and authority of full packet data. The cloud's event-driven-automation paradigm presents new opportunities.

In this webcast, learn how you can:
• streamline the deployment and use of an NDR system;
• ingest and analyze data at scale; and
• contain attacks before they become headline-grabbing breaches.

1:10 PM - 1:20 PM ET
Visit exhibit hall

1:20 PM - 1:50 PM ET
Understand Today’s Changing Network and Application Threat Landscape
Pascal Geenens, Director of Threat Intelligence, Radware
As the world migrates applications to new hemispheres and the Internet becomes more ubiquitous in business, bad actors are smelling new opportunities and attack vectors are forming like a dark storm cloud that is menacing digitalization initiatives. As you moved to remote work and accelerated your digitalization journey, a clear understanding of the threats helps you to better assess the risk and find the right balance to secure your assets and resources.

Join this session to:
• spot the threats to your businesses;
• understand who the bad actors are behind the threats; and
• learn about the tools they can use to disrupt your business.

1:50 PM - 2:00 PM ET
Visit exhibit hall
How AI Can Protect Your Email Cloud Environment from Socially Engineered Attacks
Roman Tobe, Product and Marketing Strategist, Abnormal Security
As your infrastructure, including email, moves to the cloud so do Business Email Compromise (BEC) attacks that target your employees. For enterprises, especially those with multitenant environments, it can be a challenge to bring your email security under one roof, while also protecting against these modern attacks that reach your employees.

Learn how advanced AI techniques can help you:
• analyze and normalize data across thousands of dimensions within your cloud email environment, and
• prevent costly and highly targeted socially engineered attacks, such as internal and supply chain account compromises.

Visit exhibit hall

Cloud(y) With a Chance of Data Breach
David McNeely, Chief Strategy Officer, Centrify
Organizations are increasingly moving their workloads to the cloud to achieve greater agility, flexibility, and cost savings. However, this shift has not gone unnoticed by threat actors. In fact, data breaches in the cloud, due to misconfigurations and privileged credential abuse, have increased in the past few years, and the resulting costs of the ensuing customer churn, incident remediation, and reputation damage remain significant. Thus, it is vital for organizations to enable secure migration of workloads to the cloud to seize the advantages provided by cloud computing without compromising security or compliance. Doing this successfully, however, requires a security strategy supported by effective identity and access management.

This presentation will explore:
• the strengths and shortcomings of common enterprise strategies and
• how businesses should migrate data and applications safely to the cloud.

Visit exhibit hall

New Approaches to Foundational DNS, DHCP and IPAM Services
Michael Katz, Security Specialist, Infoblox
COVID has sparked unprecedented changes in security and IT architectures. Through all the changes, IP address and DNS name resolutions are common across physical, virtual, cloud, and remote work environments. These basic services are the foundation of your digital infrastructure and therefore provide unique audit, security, and inventory control points.
This discussion will outline how to:
• make it easier and cheaper to audit, control, and secure distributed digital architectures and
• leverage SaaS delivered DNS, DHCP, and IPAM services.

3:50 PM – 4:00 PM ET
Visit exhibit hall

4:00 PM – 4:30 PM ET
Leverage Passwordless and Cloud-Based Identity for the New Era of Work
Jenn Markey, Product Marketing, Entrust
Where and how we work are forever changed. In a recent Entrust customer survey, 84% of respondents expect the recent shift to a sizeable remote workforce to be permanent. As perimeter-based security models give way to digital workforce identities, now is the time to make sure your authentication implementation is up to the challenge.

Join this second webcast in the Passwordless series to learn best practices for a secure remote workforce, including:
• high assurance credential-based authentication;
• passwordless authentication with enhanced SSO; and
• cloud-based identity for flexible and scalable workforce security.

4:30 PM – 4:40 PM ET
Visit exhibit hall