PartnerEquip: Live – Washington, D.C.

Exclusive technical event for Specialized Partners

August 26-28, 2025
Washington, D.C.

Security

The Security track at PartnerEquip: Live is designed to empower partner teams with cutting-edge knowledge and skills to build, maintain, and optimize secure cloud environments in an ever-evolving digital landscape. Over three intensive days, participants will delve into critical areas of cloud security, including AI Security, Data Protection, Identity and Access Management, Network and Application Security, and Threat Detection and Incident Response.

This year's track places a special emphasis on the security challenges and opportunities presented by generative AI and other emerging technologies. Through a combination of expert-led sessions, hands-on labs, and interactive Q&A discussions, attendees will gain practical insights into securing generative AI applications, leveraging advanced threat detection capabilities, and implementing robust data protection strategies.

Designed for technical experts in security-focused partner organizations, this track caters to professionals such as Security Architects, Cloud Security Engineers, CISOs, Security Operations Leads, Compliance Managers, and AI/ML Security Specialists. Participants will leave equipped with the latest knowledge, best practices, and hands-on experience necessary to enhance their customers' cloud security posture and address the most pressing security challenges in today's rapidly changing technological environment.

Agenda

Tuesday, Aug 26:

Time (EDT)	Level (1-400)	Section Title	Abstract/Description
8:00 am	Breakfast		
9:00 am	Welcome Keynote		
9:45 am	200	Security, Identity, and Governance Roadmap Transparency	AWS Service team presents key innovations and upcoming features for security services. Session highlights new tools and enhancements designed to strengthen cloud security, improve threat detection, and streamline incident response across AWS environments.
10:30 am	Break		
10:45 am	300	Introducing the AWS Security Incident Response: Quickly and safely respond to security incidents	AWS Security Incident Response is a new service that helps organizations rapidly prepare for, respond to, and recover from security incidents. It enables teams to triage findings, automate responses, and access 24/7 expert support for managing events like account takeovers and ransomware attacks. The service integrates communication and collaboration tools while complementing AWS's Detection and Response portfolio to guide customers through the complete incident lifecycle.
11:30 am	300	AWS Security Hub: A unified cloud security solution	Join this session to learn about the new and improved AWS Security Hub. AWS Security Hub unifies visibility to detect, prioritize, and respond to critical security issues to help protect customer's cloud environment. It correlates and enriches security signals, delivering actionable insights and enabling streamlined response. Learn how the service helps unify security operations, provide enhanced risk context and prioritizes analysis. Leveraging the Open Cybersecurity Schema Framework, AWS Security Hub further streamlines response workflows and accelerates time to remediation of security issues by integrating with out of the box ticketing systems.
12:00 pm	Lunch		
1:00 pm	300	Vulnerability Management at scale with Amazon Inspector	Transform your security posture with Amazon Inspector's new and enhanced vulnerability management capabilities. This session shows how to gain complete visibility of security risks from code to cloud. Learn to track vulnerable container images in production, implement automated code scanning, and validate infrastructure as code. Discover how Inspector's new third-party repository integrations and security guardrails help ensure consistent secure coding practices. Walk away with practical knowledge to strengthen your organization's security at scale.
1:30 pm	300	GuardDuty Extended Threat Detection - Expansion coverage to EKS	Amazon GuardDuty Extended Threat Detection helps you identify sophisticated, multi-stage attacks targeting your AWS accounts, workloads, and data. Learn how this new capability uses AI/ML to automatically correlate security signals across AWS services, presenting attack sequences from compromised EKS clusters as single, critical-severity findings. See how attack sequence findings include incident summaries, detailed event timelines, and MITRE ATT&CK® mapping. Discover how this helps security teams spend less time on first-level analysis and more time responding to critical threats to minimize business impact.
2:00 pm	300	Threat Detection and Response Workshop	This workshop is designed to get you familiar with the AWS threat detection and response services, best practices, use cases, and then use what you learn to dive deeper into scenarios. All of this is designed to prepare you and help you operate more securely on AWS. This workshop goes though overviews, operationalization, and deployment of each of the services: Amazon GuardDuty, Amazon Inspector, AWS Security Hub, Amazon Macie, and Amazon Detective.
3:00 pm	Break		
3:15 pm	300	Top 10 Best Practices for Network Security with Network Firewall & DNS Firewall	This session covers real-world customer use cases and common issues to avoid when developing policies and rules. Practical tips, common scenarios, new feature releases, and troubleshooting strategies are also addressed to equip you with the skills needed to fortify your organization’s network defense on AWS. Explore practical guidelines for policy and rule creation with the Suricata engine in the AWS Network Firewall. Learn the top ten recommendations for getting started with Network Firewall and Amazon Route 53 Resolver DNS Firewall policy creation.
4:00 pm	200	Egress Deployments Made Easy	In this session, come learn about all latest launches to the AWS Network Firewall service designed to help customers prevent previous possible complexities in implementation. With the latest AWS Network Firewall and Route 53 Resolver DNS Firewall features, learn how to simplify your deployment and configuration process, dramatically reduce your exposure to a variety of threats, make specific recommendations for rules to support your use cases, and gain confidence your security policies are meeting intended needs.
4:45 pm	End of Day Survey		
5:00 – 6:00 pm	Welcome Reception (On-Site - Badge Required)		

Agenda

Wednesday, Aug 27:

Time (EDT)	Level (1-400)	Section Title	Abstract/Description
8:00 am	Breakfast		
9:00 am	300	Generative AI Security Grounding - What makes security different?	This session provides a grounding on what makes generative AI applications different from regular workloads. Security and safety are top of mind for customers deploying generative AI workloads, as they operate differently compared to traditional workloads. The expectation is generative AI applications provide similar security capabilities you would expect for data access and API access to workloads, which is not the case. This presentation covers a deep dive into four key expectations: structured outputs, data accuracy, deterministic, and authorization built-in.
10:00 am	300	AWS KMS Best Practices and the Post-Quantum Roadmap	In this session, we will take a deep dive into AWS Key Management Service (KMS), exploring best practices, real-world use cases, and common misconceptions. Additionally, we will discuss post-quantum cryptography at AWS, including its current state, challenges, and roadmap for the future. Join us to gain insights into securing your cryptographic assets today while preparing for the post-quantum era.
10:30 am	Break		
10:45 am	300	Understanding Generative AI Data Security and Data Authorization	In this session we will discuss the data security and authorization challenges involved in deploying generative AI applications. It highlights the need to expand data governance practices to properly manage data used for training and fine-tuning large language models. The session outlines techniques like using metadata filters and incorporating identity/authorization into agent-based workflows to address these challenges.
11:30 am	300	Automate Certificate Management at Scale with Exportable Public Certificates from AWS Certificate Manager	Learn how to automate TLS certificate management across hybrid and multi-cloud environments using AWS Certificate Manager's exportable certificates. We'll demonstrate building an end-to-end automation framework with AWS services including EventBridge, Lambda, and Step Functions to handle certificate lifecycle management. Through practical examples, you'll learn to implement automated certificate workflows and monitoring to eliminate manual tasks and reduce certificate-related outages.
12:00 pm	Lunch		
1:00 pm	300	Securing generative AI applications on AWS Workshop	In this workshop, we will focus on the security risks and vulnerabilities associated with building and deploying a generative AI application. As artificial intelligence continues to evolve, ensuring its security becomes more complex, and generative AI presents unique challenges. Over the course of this workshop, we will explore some of AWS security capabilities and best practices to address potential security vulnerabilities in generative AI applications built on Amazon Bedrock.
2:00 pm	200	AWS WAF got a makeover, and what else is new in Network & Application Protection	AWS security team presents key innovations and upcoming features for Network & Application Protection security services. Session highlights new tools and enhancements designed to strengthen your perimeter, gain network insights, simpify deployments, and layer defense-in-depth across AWS environments.
3:00 pm	Break		
3:15 pm	400	Bedrock Security Deep Dive	In this session, you will learn about how to securely use Amazon Bedrock. You will learn about Bedrock security features, such as model tenancy, access control, client connectivity, and data privacy.
4:45 pm	End of Day Survey		
5:30–10:00 pm	Networking Event (Off Site - Badge Required)		

Agenda

Thursday, Aug 28:

Time (EDT)	Level (1-400)	Section Title	Abstract/Description
8:00 am	Breakfast		
9:00 am	300	Architecting a Secrets Management Strategy that Scales	Explore centralized and decentralized approaches to secrets management in cloud-native applications. Learn how to leverage AWS Secrets Manager, KMS, and Config to implement a balanced strategy that serves both developer and security needs. We'll cover architectural trade-offs and best practices for compliance and auditing across different implementation patterns.
9:45 am	300	Building Secure Multi-Tenant SaaS: Best Practices with AWS Data Protection	SaaS providers must protect customer data while meeting security, compliance, and operational efficiency goals. In this session, we provide prescriptive guidance on implementing AWS data protection services - including AWS KMS, AWS Private CA, and Amazon Macie - to secure multi-tenant SaaS environments. Through real-world customer use cases, we explore how leading SaaS companies use encryption, certificate management, and data discovery to mitigate risks and meet compliance requirements. Attendees will leave with actionable best practices to enhance security while optimizing performance and cost.
10:30 am	Break		
10:45 am	100	Ask Experts Anything Panel	Ask the Expert Panel is an opportunity to connect with leaders from across AWS in a Q&A format.
11:15 am	300	IAM Access Analyzer for Security Pros	In this session, we'll go deep on IAM Access Analyzer, focusing on both the how and why behind key features like unused, external and internal access analysis, as well as policy validation and custom policy checks. We'll demystify our secret sauce — automated reasoning — and describe how we use it to generate provably correct security findings. Finally, we'll discuss our future roadmap and get your feedback on how we can better support customers on their journey to least privilege together.
12:00 pm	Lunch		
1:00 pm	400	Securing GenAI apps: Fine-grained access control for Bedrock Agents	Want to secure generative AI applications accessing your organizational data? Learn how to implement intelligent access controls for Amazon Bedrock-powered applications accessing your organizational data. In this builders' session, you'll build a defense-in-depth approach that combines authentication using Amazon Cognito and fine-grained authorization with Amazon Verified Permissions to secure access for Bedrock AI agents. Implement layered permissions that protect sensitive data without limiting your GenAI capabilities.
2:00 pm	300	Advanced Policy Evaluation	Dive into the world of policy evaluation, headfirst. We will examine several different types of policies (Service Control Policies, Resource Control Policies, Permissions Boundaries, Resource Policies, Identity Policies) and how they are evaluated. We will also examine the differences between the types, when to use which one, and explore the best practices behind their use cases.
3:00 pm	Break		
3:15 pm	300	IAM Architecture patterns, Getting builder into AWS (IAM role federation & IdC Permission sets)	So, you're designing an AWS multi-account structure, and looking for recommendations on how to control access for builders? In this talk we will discuss multiple ways of managing identities in AWS and provisioning access to AWS services and resources while highlighting some of the trade-offs that may be encountered. You will walk away with practical examples, best practices, and considerations on how to successfully manage access across AWS accounts.
4:15 pm	300	AWS Shield - Network Security Director	Get a deep dive into the AWS Shield- Network Security Director, a new service, now in preview, that allows you to discover network resources, analyze connectivity, understand misconfigurations, and get AI-assisted remediation recommendations with Amazon Q.
4:45 pm	End of Day Survey		