AWS re:Inforce

JUNE 13 - 14, 2023 | ANAHEIM, CA

本日のアジェンダ

時間	セッション	内容
10:00-10:40	AWS セキュリティ リーダーセッション	セキュリティリーダーに向けに実施されたセッションについて、その要点をまとめてお話します。組織においてセキュリティを統括しているCISO/CIO/CTO/事業部長の方や、セキュリティ計画実行の意思決定をされるセキュリティアーキテクト/ITアーキテクト/エンジニアリードの方を想定した内容となります
10:40-10:50	休憩	
10:50-11:30	AWS セキュリティ サービスアップデート	AWS re:Inforce 2023 にて発表されたセキュリティ関連の新サービス/新機能に関するまとめをお話します。業務においてAWSセキュリティに携わる方にとって効率的に必要な最新情報を学べるセッションです

AWS re:Inforce 2023 re:Cap Online Seminar
AWS セキュリティリーダーセッション

Hayato Kiriyama
Head of Security Sales
Amazon Web Services Japan

AWS re:Inforce 2023

AWS 専門家や業界リーダー顧客と
共に学ぶセキュリティ学習の場

カリフォルニア州アナハイム
2023 年 6 月 13 日~ 6 月 14 日

16 の新サービス新機能の発表

16 の新サービス新機能の発表

- AWS Verified Permissions
- Amazon Inspector code scanning
- Amazon Inspector SBOM
- Amazon CodeGuru Security
- Amazon Codewhisperer security scans
- Amazon Detective finding groups
- AWS Security Hub Automation Rules
- Amazon GuardDuty Summary View
- WAF Account Creation Fraud Prevention
- AWS Control Tower and AWS Security Hub Integration
- AWS Cyber Insurance Partners
- Amazon EC2 Instance Connect Endpoint
- AWS Private CA Connector for Active Directory (beta)
- AWS Payment Cryptography
- Temporary elevated access management (TEAM)
- AWS built-in

セキュリティリーダー向けセッションリスト

[AWS re:Inforce 2023 Watch on Demand]

https://reinforce.awsevents.com/on-demand/

[基調講演]

AWS re:Inforce 2023 - Keynote with CJ Moses

https://www.youtube.com/watch?v=_piUB5FrYVE

[リーダーシップセッション]

Achieving end-to-end security on AWS

https://www.youtube.com/watch?v=Khhni4Ce-Ow

How AWS can help navigate shifts in the global regulatory landscape

https://www.youtube.com/watch?v=2Yu3QpmqTMs

Journeys to Zero Trust on AWS

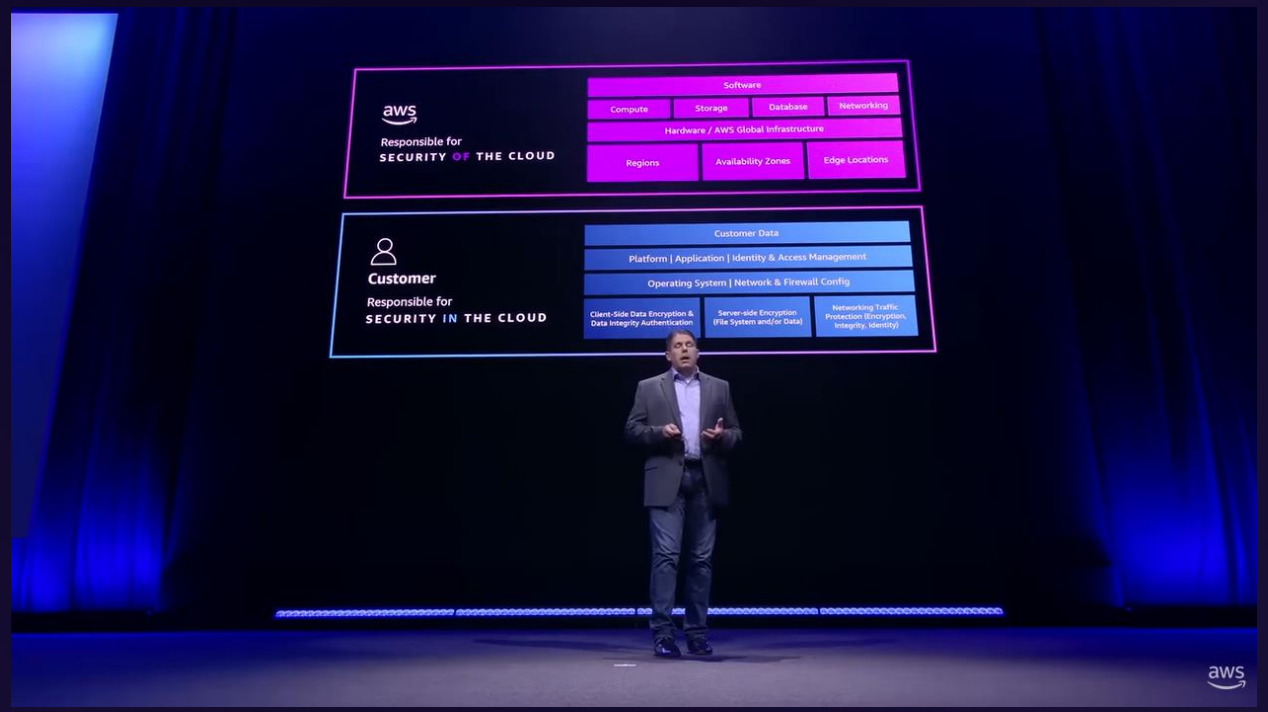
https://www.youtube.com/watch?v=Uke2CmFaVZ8

Security in the open: OSS and AWS

https://www.youtube.com/watch?v=kMY8gGmWfAI

セキュリティは AWS の最優先事項

セキュリティを担保する重要な概念が「責任共有モデル」



- 「アクセス権があるなら責任がある」
- データセンターなどのインフラは AWS がアクセスする
- お客様が設計・実装する範囲は、お客様がアクセスする

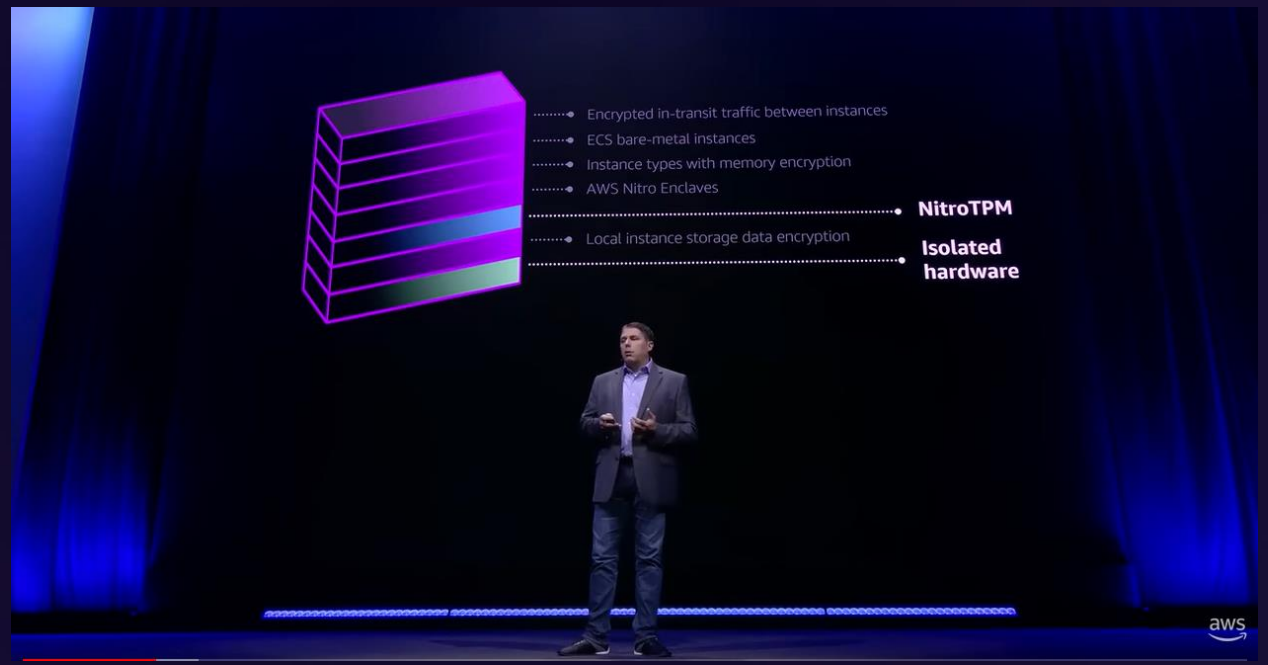
仮想環境のセキュリティ - AWS Nitro System

従来の仮想化の問題点は攻撃者がハイパーバイザーの脆弱性を悪用できること

- 5年の研究開発を経て、AWS Nitro システムをリリース
- 仮想化機能とセキュリティ機能を Amazon が設計した専用のハードウェアとソフトウェアにオフロード
- ベアメタルに近いパフォーマンスと強化されたセキュリティ

Nitro は機密性の高いワークロードのニーズに対応

不必要なデータアクセスを防止しデータを保護

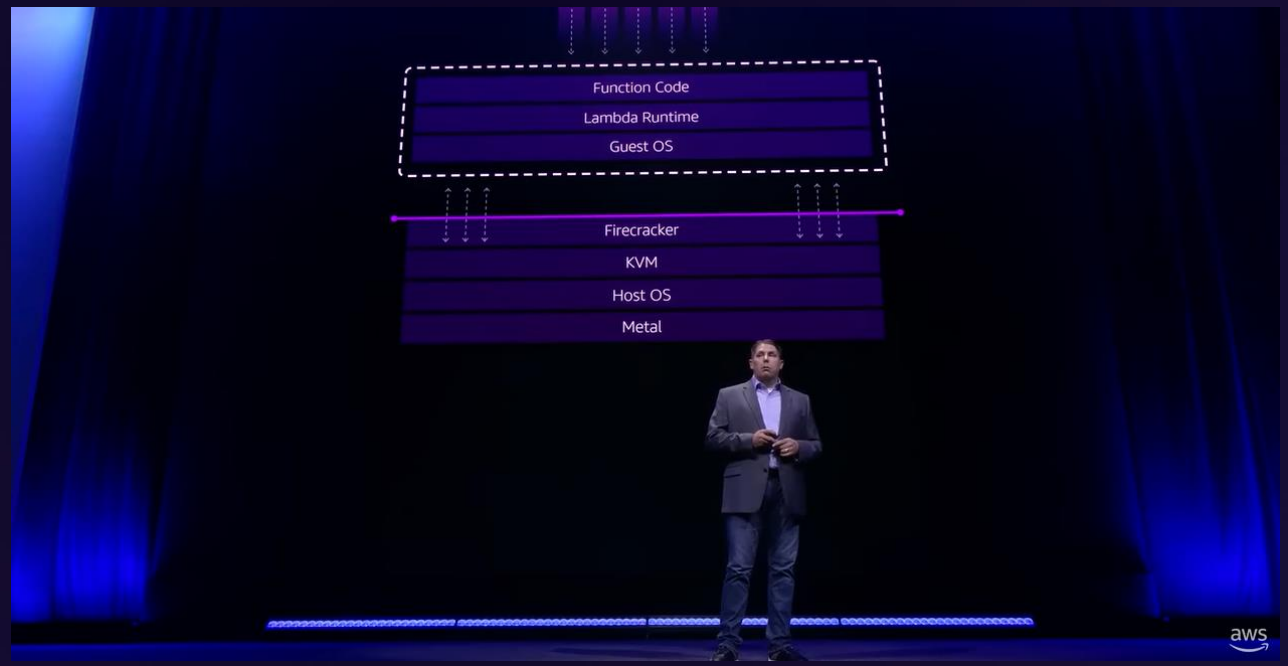


- Nitro で実行されるOSから不要なシステムコールを完全に削除
- AWS オペレータがお客様 EC2 Nitro ホストにアクセスするパスが存在しない
- NCC Group*が Nitro システムのセキュリティ保証をレビューし、確認した報告書を発行

* 英国大手サイバーセキュリティコンサルティング会社

マルチテナントなコンテナや関数サービスの保護

マイクロVMを実行する必要最小限の仮想化モデルFirecracker



- ビルド時に全ての依存関係ライブラリを静的リンク
- Firecracker プロセスがアクセスできるリソースを制限
- 小規模で厳重管理されたシステムコールのみアクセスを許可

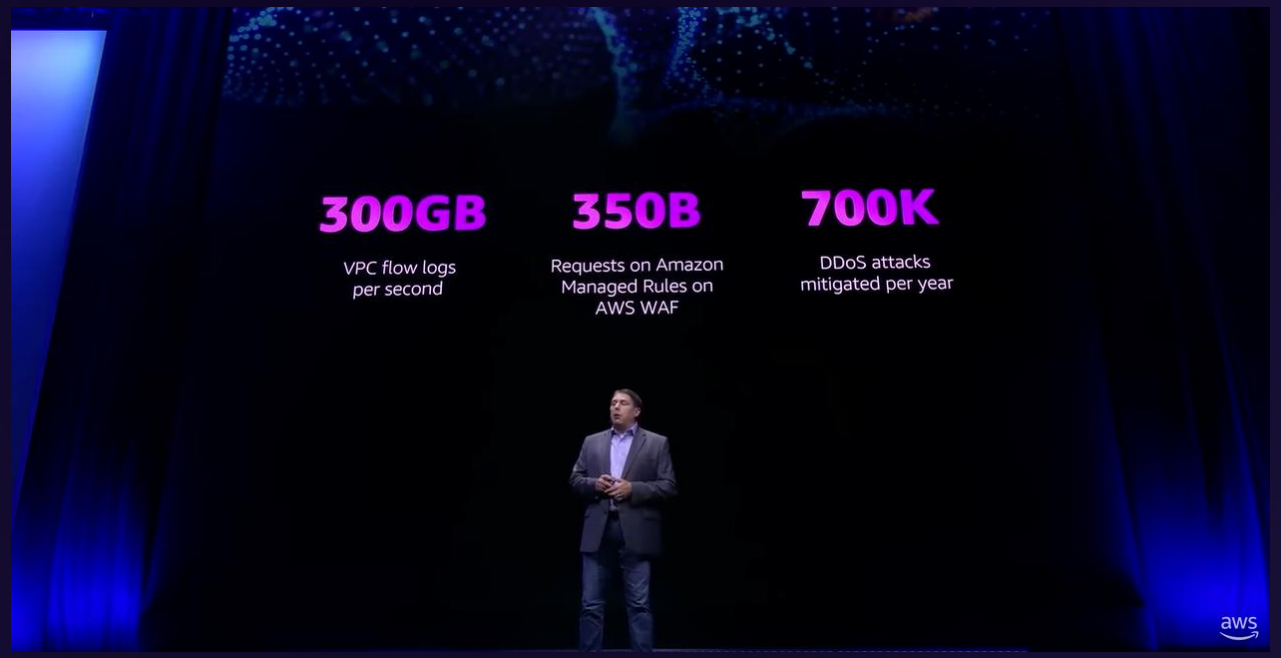
ソフトウェアコードはどのように保護するか？

ビルダー(開発者)がセキュリティのオーナーシップを持つ

- セキュリティチームは教育やツール提供を通じて、ビルダーが開発の早い段階で問題修正できるようにする
- セキュリティテスト結果をビルダーに自動的にフィードバック
- 問題やレビューから得られた知見を他チームとも共有

規模がインテリジェンスを生み出す

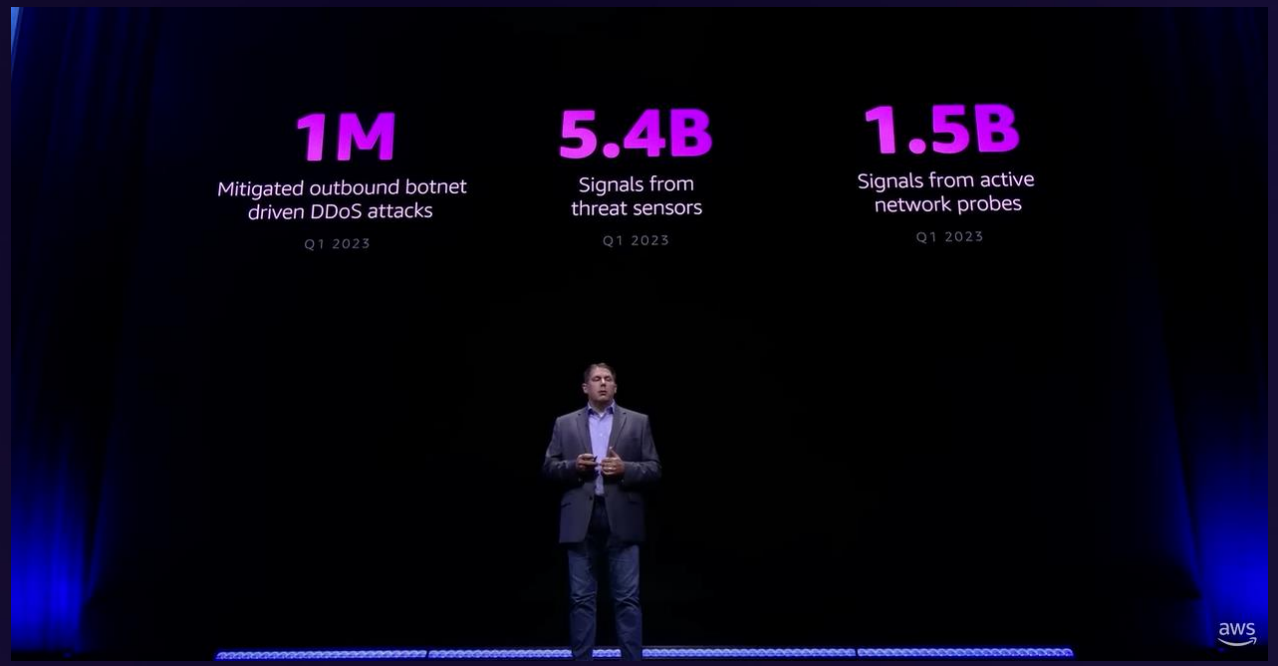
より多くの脅威インテリジェンスがセキュリティを向上させる



- 脅威インテリジェンスを AWS サービスに継続的統合
  - AWS Backup
  - Amazon GuardDuty
  - Amazon Route 53 Resolver DNS Firewall
  - AWS Shield

AWS では「Mean Time to Defense」を重視

どれだけ早く脅威インテリジェンスを収集し、AWS サービスに適応できるかを示す尺度



- 世界中に分散された脅威センサーのネットワークを使用
- 自動マルウェア分析、アクティブなネットワーク調査、ボットネット追跡ツール併用
- 脅威アクターのTTP(戦術・技術・手順)を理解する

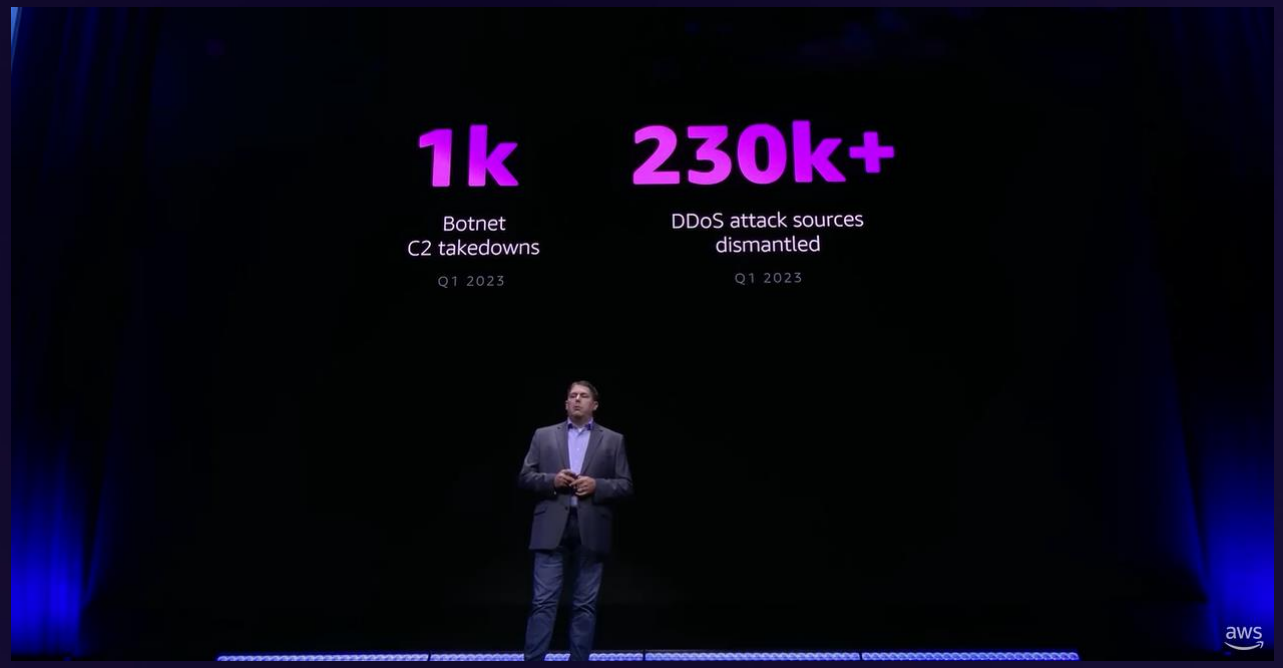
攻撃者の戦術の変化：ワイパーウェア

攻撃者の動機を理解することで、身を守る準備ができる

- 金銭目的でデータの暗号化を行うランサムウェア
- データ破壊や削除を目的としたワイパーウェア
- 一部の攻撃者の動機が次の日に変化することもある

インターネットをより安全な場所に

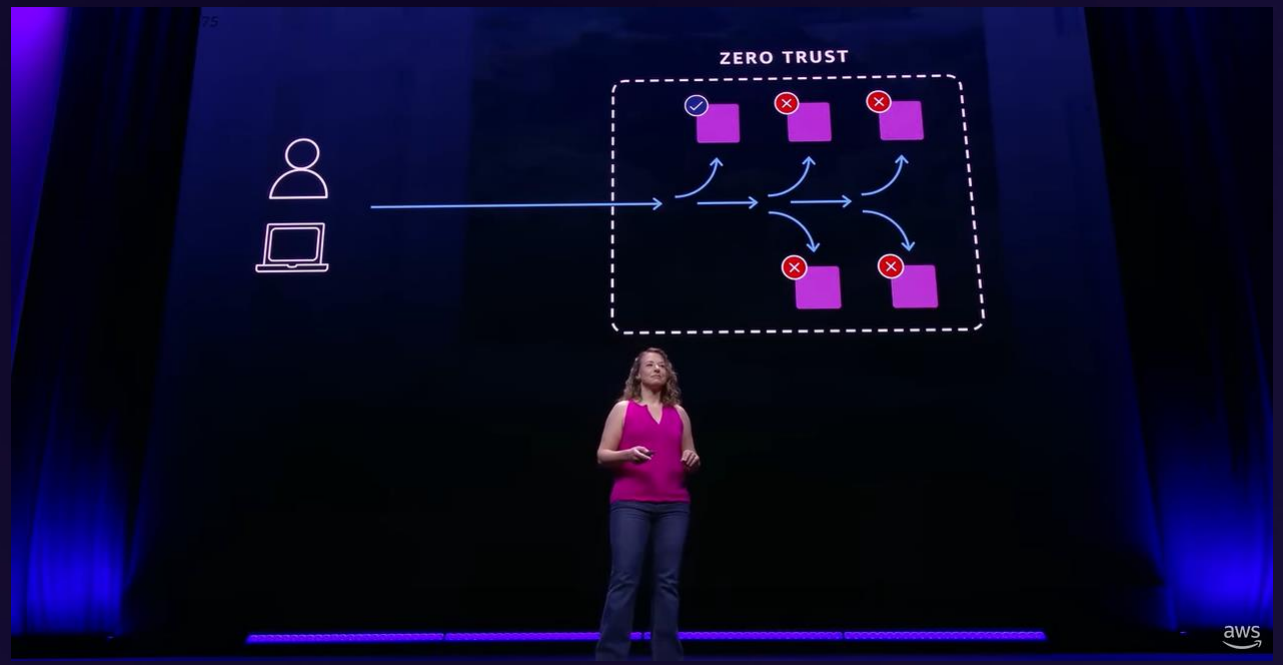
AWS は世界中のセキュリティコミュニティ/パートナーと連携



- インターネット上のC2サーバー停止、DDoS攻撃ソース解体などにも貢献
- Log4j脆弱性が公開された時、AWS はお客様環境含むAWS Lambdaに24時間以内にパッチ適用した
- 「最良のパッチ戦略はパッチ適用しなくて済むこと」

AWS 環境における Zero Trust の実現

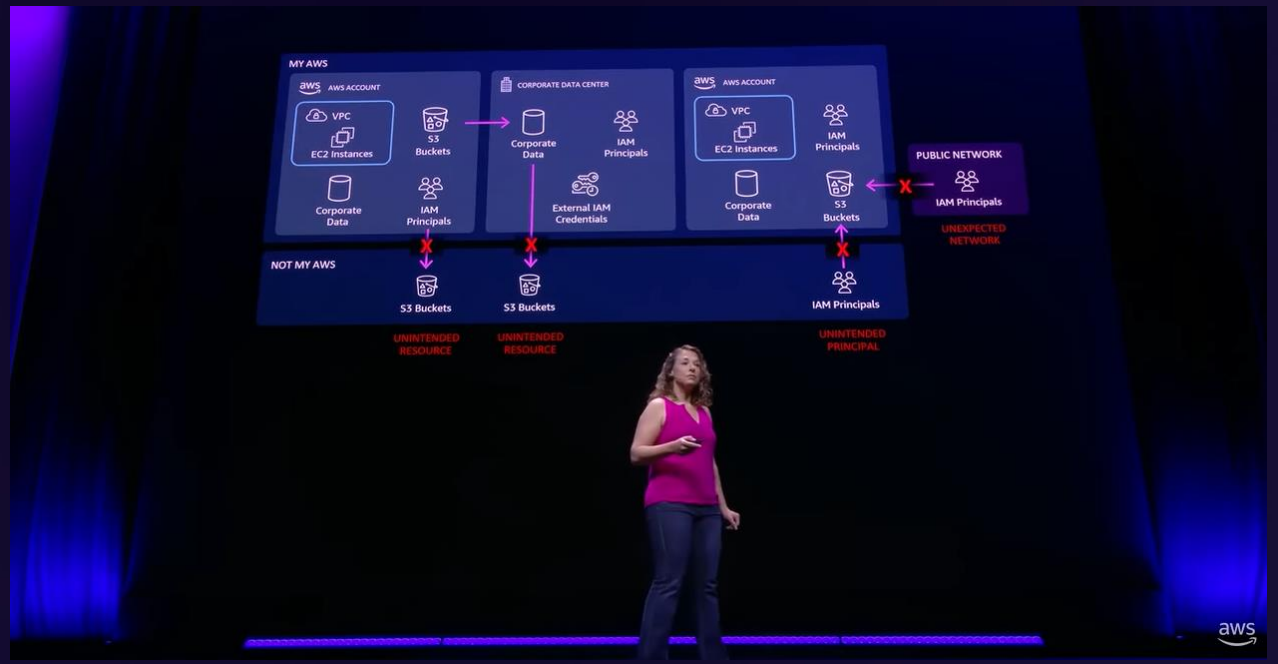
AWS サービスは従来からアイデンティティやネットワークで
アクセス評価するゼロトラストアプローチで設計されてきた



- AWS Verified Access で VPN 無しに社内アプリケーションへセキュアにアクセス
- Amazon Verified Permissions によるアプリケーション認可の一元管理と評価
- Amazon EC2 Instance Connect Endpoint による EC2 へのセキュアなアクセス

AWS 環境のデータを保護する概念：データ境界

自分達の組織が、自分たちのネットワーク環境で、自分達のリソースやデータにアクセスするための境界



- 複数ポリシーを組み合わせてデータ境界を実現(以下は例)
  - AWS Organizations Service Control Policy
  - VPC Endpoint Policy
  - Amazon S3 Bucket Policy
- AWS Management Console Private Access により自組織内の不正ユーザーの管理コンソールアクセスを制限可能に

AWS 環境における脅威検知

Amazon GuardDuty が提供する脅威検知の範囲が拡大

- データベース
  - Amazon Aurora
- コンテナワークロード
  - EKS実行環境
- サーバーレスアプリケーション
  - AWS Lambda 関数

AWS 環境における脆弱性管理

Amazon Inspector の2つの新機能で脆弱性管理をサポート

- Amazon Inspector Code Scans for Lambda でLambda 関数コード自体を脆弱性スキャン
- Amazon Inspector SBOM Export によりソフトウェア依存関係を自動的かつ一元的に管理可能に

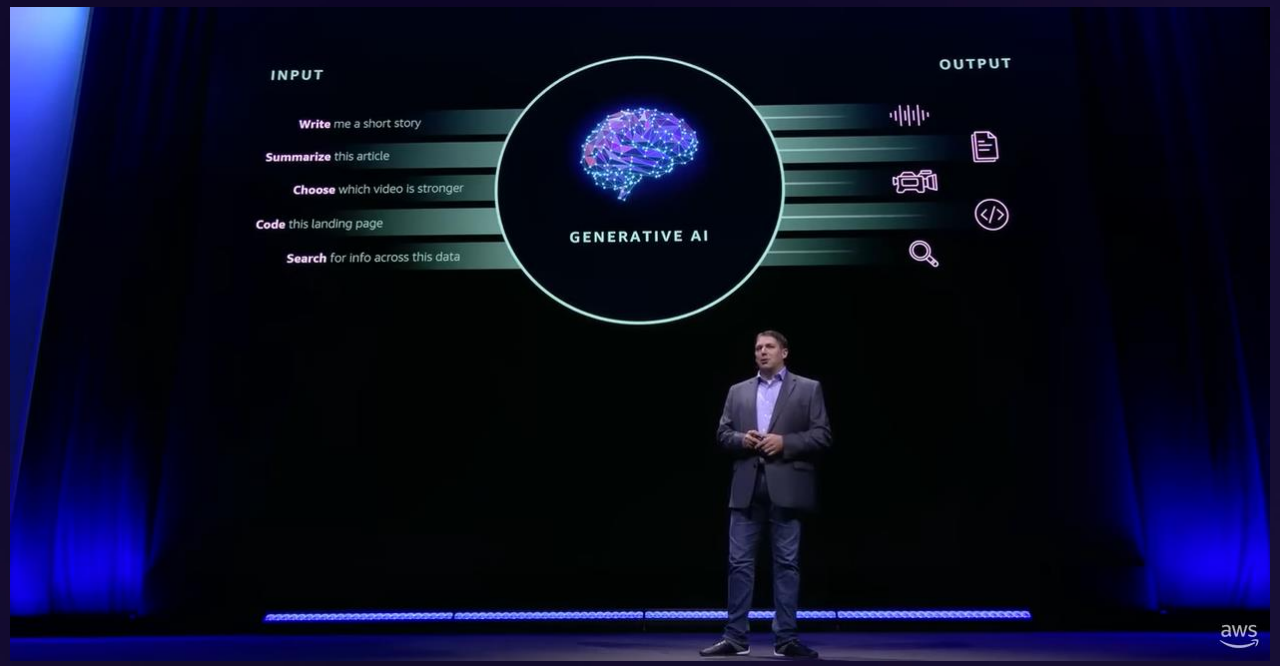
AWS パートナーとの連携

お客様セキュリティニーズに対応する広範なソリューション

- Amazon Security Lake はセキュリティログを業界標準形式で一元的に集約管理し、優れた可視性と洞察を得るためのデータレイクサービス
- AWS Built-in Partner Solutions (preview) は AWS パートナー製品が AWS サービスと統合できるよう設計されていることを保証し、価値実現を早める

機械学習と生成 AI でセキュリティを拡張する

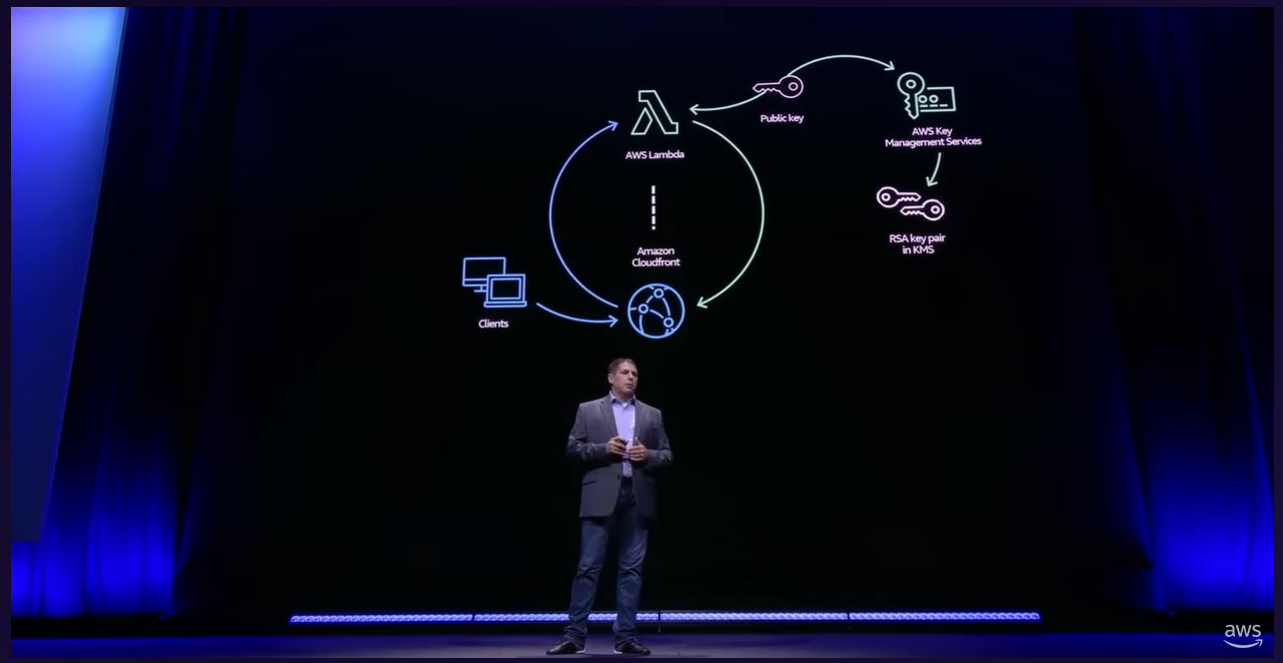
AWS では大規模言語モデルが脅威の予防、検知、対応のサイクル全体でセキュリティをどのように向上できるか検討中



- Amazon CodeWhisperer はリアルタイムにコード提案することで開発者の生産性を向上
- Amazon CodeGuru Security (preview) はCI/CDパイプラインと統合し、あらゆる段階でコード内の脆弱性を検出する
- Findings Groups for Amazon Detective は数千のセキュリティ検出結果からセキュリティイベントを抽出する

AWS のお客様の将来への投資：ポスト量子暗号

ポスト量子コンピューティング(PQC)は現在公開鍵暗号を使用しているすべての人に影響を与える可能性がある



- AWS は NIST (米国立標準技術研究所) とともに、ポスト量子暗号に関する標準化を支援
- ポスト量子ハイブリッド鍵交換に関する標準仕様案を s2n-tls ライブラリに実装して、AWS サービスにデプロイ

Let’s build trust and secure the future together.

Thank you