aws Canada

ARCTIC WOLF

Arctic Wolf + AWS

From Impossible to Unstoppable: Cracking the Code of Modern Security Operations

Wayne Feyer

Enterprise Account Executive
Arctic Wolf Canada

Bill Ohlson

Principle Executive Security Advisor
AWS

Two intertwined problems …

Tools

Sprawl/Noise

Staffing

Talent shortage

3200+ (Security tool vendors)

$215,000,000,000 (Spent on tools in 2024)

5200+ (Reported ransomware attacks in 2024)

The Arctic Wolf Security Operations Cloud

Arctic Wolf uses over 50 different AWS services

ARCTIC WOLF PLATFORM


Amazon Simple Storage Service


Amazon DynamoDB


Amazon Relational Database Service


Amazon Elastic Kubernetes Service


Amazon Elastic Container Service


Amazon Elastic Compute Cloud


AWS Lambda


Amazon GuardDuty


Amazon Simple Queue Service


Amazon CloudWatch


Amazon CloudFront


Amazon MSK Connect


Network Load Balancer

Ending Cyber Risk Together

ARCTIC WOLF | CANADA

Canadian-Born Co-Founder • HQ in Waterloo

1,000+ Canadians Employed

550+ Canadian Companies Secured

Global Canadian CSOC
LEADING GLOBAL DATA PRIVACY AND GDPR BENEFITS

Hosted in AWS Canada since March 2021

We make security work.

Canadian DNA

BlackBerry | CYLANCE
vxintel
RootSecure RISK · MANAGED

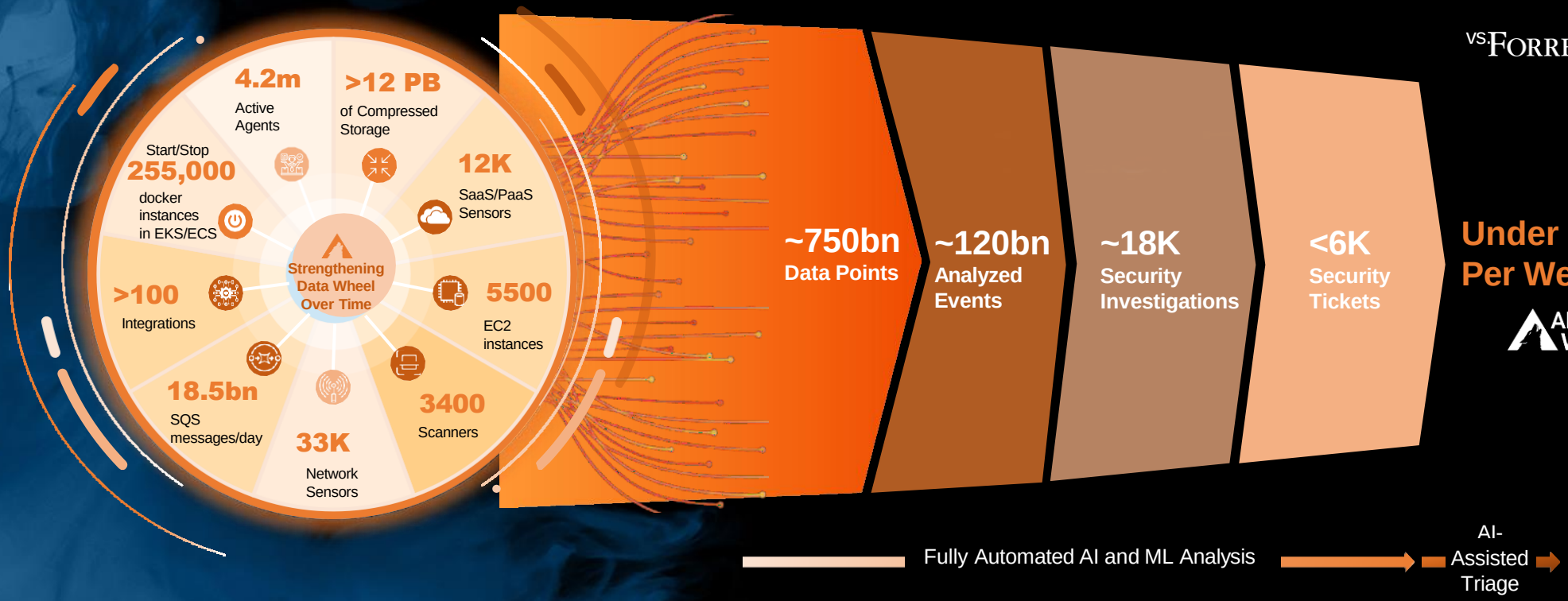
Investing for the Future

- **$150M** Invested in the past 12 months
- **1/3** Arctic Wolf Global Employees are Canadian
- Canada is home to **50%+ AW R&D**
- **~40%** of Global Security Services SOC in Canada

Partnering Together

- Canadian Cyber Community
- Rogers CyberSecure Catalyst
- WiCsys Ontario

Intelligent Correlation to Eliminate Alert Fatigue



Forrester Study: The 2020 State of Security Operations.

ARCTIC WOLF LABS

AI and Data Science

Threat Intelligence and Security Research

Detection & Response Engineering

Security Posture Engineering

Security Operations Platform Built on Open XDR

8+
Trillion events per week

500K+
New malware samples daily

>4.2M
AW active agents and 33,000+ sensors

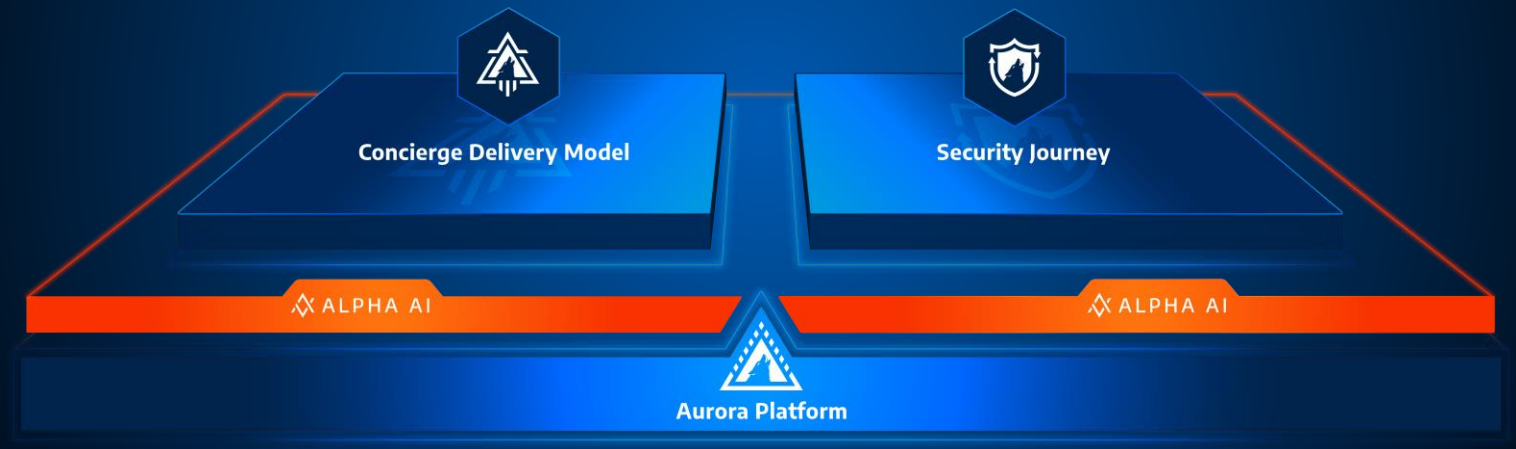
10+ YRS
Of development / SOC2 Type II and ISO 27001

80+
Security stack integrations

>700K
Tailored reports created for >7,000 customers

83%
Of tickets come from AW detections

UNMATCHED POWER



UNIQUE PRECISION

1 Ticket
Per day on average

99.9%
True positives

Single
View into your security stack

Unique culture of security

Four key components for a “culture of security”

Executive Support

Distributed Ownership

Psychological Safety

Communication Education

Shared Responsibility

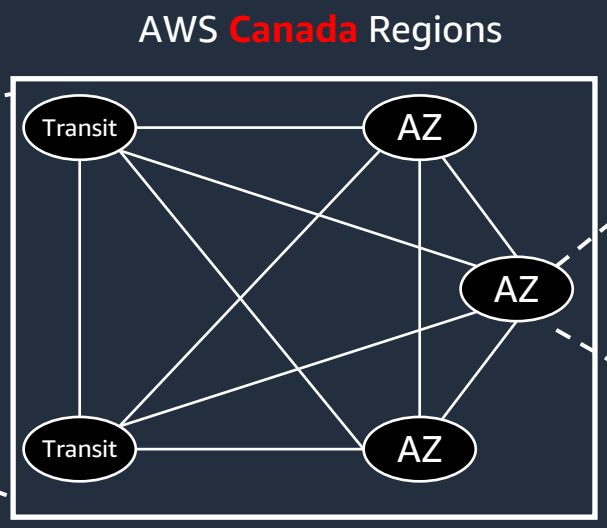
AWS Region design

AWS Regions are comprised of multiple Availability Zones (AZs) for high availability, high scalability, and high fault tolerance. Applications and data are replicated in real time and consistent in the different AZs.

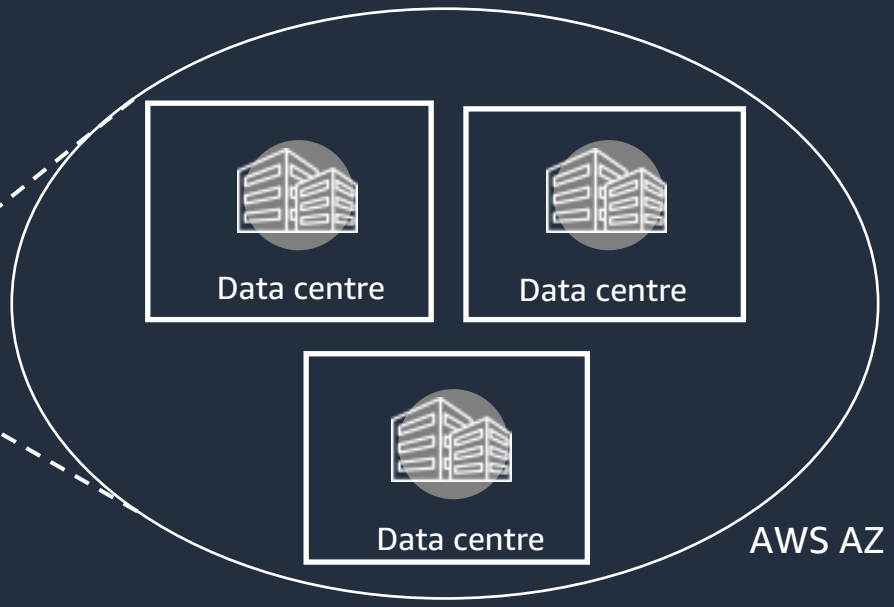
36 geographic Regions

114 Availability Zones

700+ points of presence



A **Region** is a physical location in the world where we have multiple **AZs.**

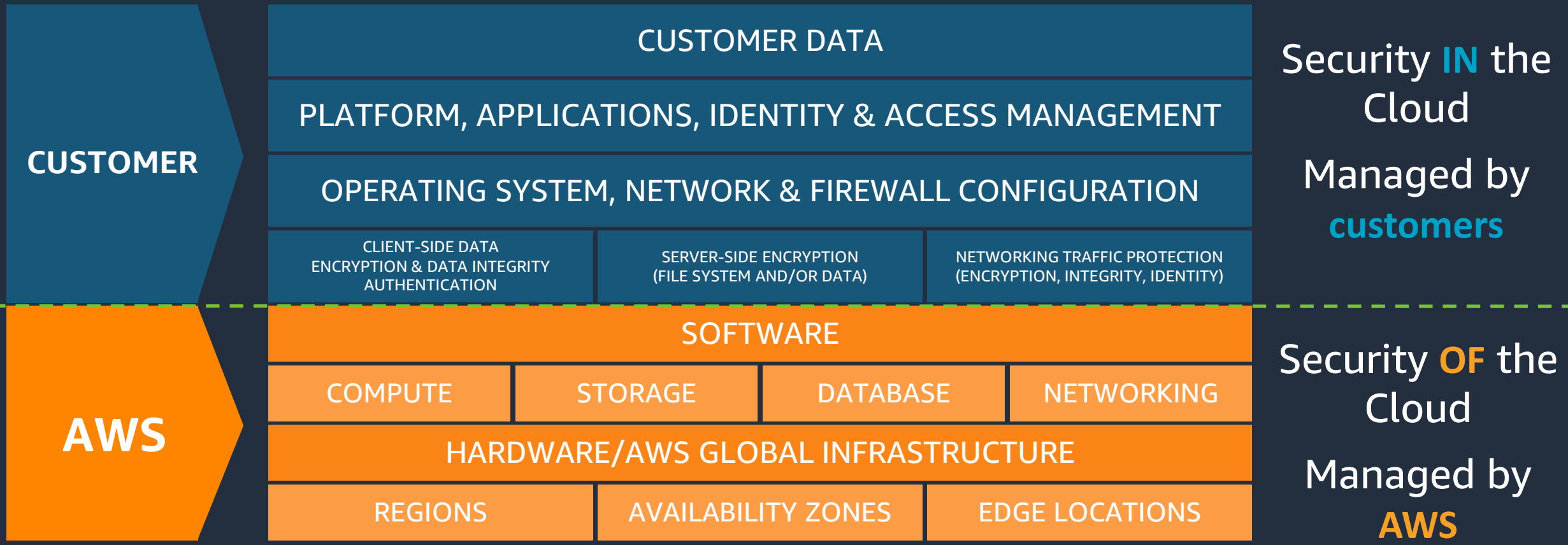


AZs consist of one or more discrete data centres, each with redundant power, networking, and connectivity, housed in separate facilities.

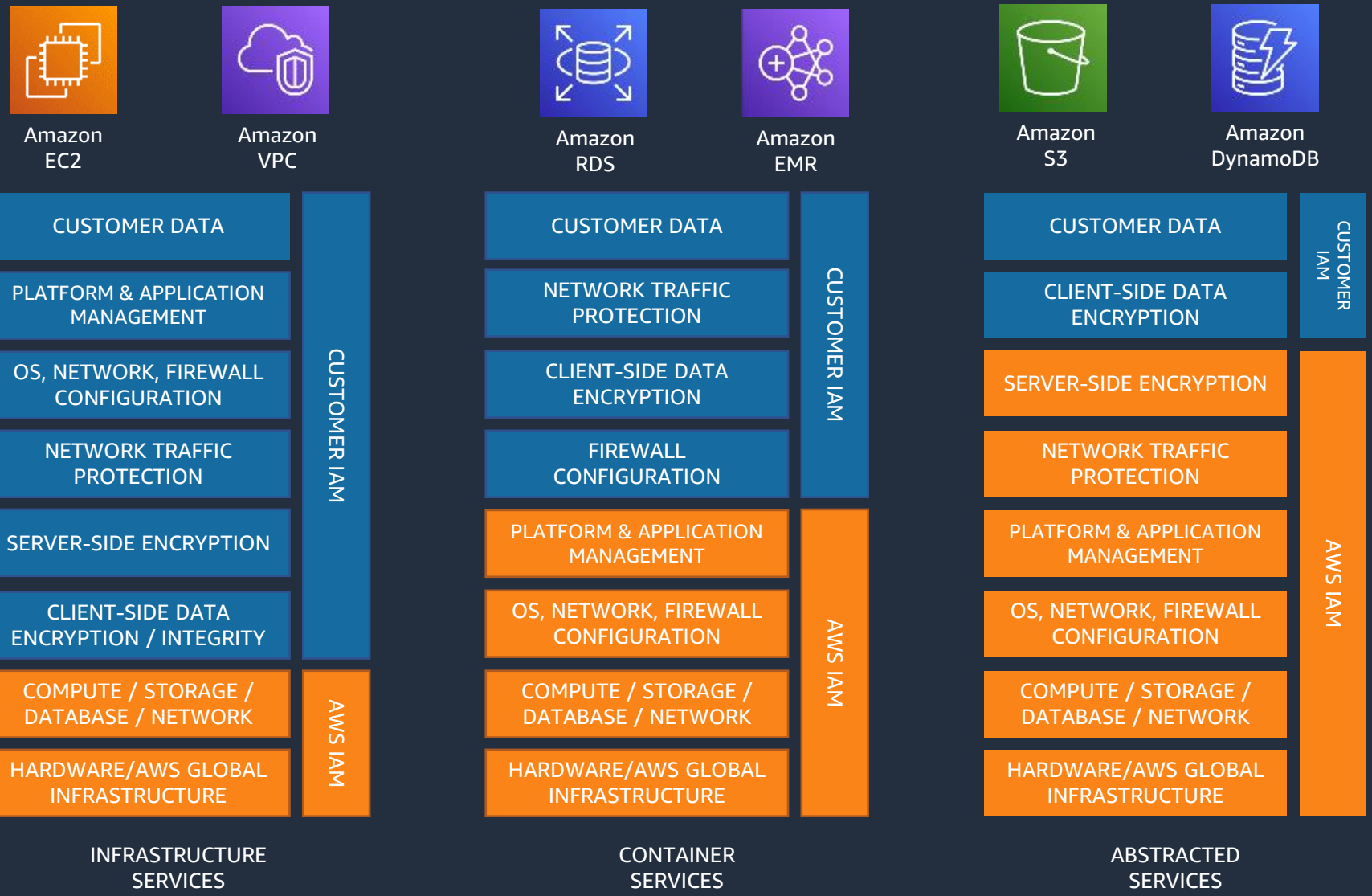
The Goldilocks zone for disaster recovery, business continuity planning, and disaster preparedness

aws Canada

AWS Shared Responsibility Model



Shared Responsibility Model is NOT static



More Customizable
+
More Customer Responsibility

Less Customizable
+
Less Customer Responsibility
+
More Best Practices built-in

aws Canada

How we design for security

Security is our highest priority

We start with our own internal operational processes. Application reliability is critical. Service interruptions result in a negative customer experience, thereby reducing customer trust and business value.

Develop a Correction Of Error (COE):

We don't ask why a human failed. We ask why the process failed to allow the human to perform the action. Then we fix the process.

The 5 Why's

An example of asking about an event X occurring:
#1 Why did X happen?
X happened because this action took place.
#2 Why did that action take place?
That action took place because there was a typo.
#3 Why was a typo allowed?
The typo was allowed because there was no validation.
#4 Why was there no validation of the code?
The current process does not validate code.
#5 Why doesn't the current process validate code?
The shell used to input the code does not have that feature.

Our processes are audited extensively

We eat our vegetables, we eat them often, and we can prove that we eat them!

- CSA cloud security alliance SM
- ISO 9001 International Organization for Standardization
- ISO 27001 International Organization for Standardization
- ISO 27017 International Organization for Standardization
- ISO 27018 International Organization for Standardization
- PCI Security Standards Council PARTICIPATING ORGANIZATION™
- AICPA SOC — SOC 1
- AICPA SOC — SOC 2
- AICPA SOC — SOC 3
- CJIS
- FIPS 140-2 CRYPTOGRAPHY
- FISMA FEDERAL INFORMATION SECURITY MANAGEMENT ACT
- DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA — DoD SRG
- FR FedRAMP
- DEPARTMENT OF EDUCATION UNITED STATES OF AMERICA — FERPA
- FFIEC Federal Financial Institutions Examination Council
- C5
- SEC Rule 17a-4(f)
- GxP
- HIPAA
- Cloud Medium (formerly PBMM) CANADA
- MPAA
- iDA SINGAPORE
- マイナンバー My Number Act
- VPAT Section 508
- FISC
- irap
- ISMS
- G-Cloud
- TISAX ENX ASSOCIATION
- ITAR Compliant International Traffic in Arms Regulations
- CYBER ESSENTIALS PLUS
- CERTIFICACIÓN DE CONFORMIDAD CON EL ens
- CGP CANADA

We keep humans way from things

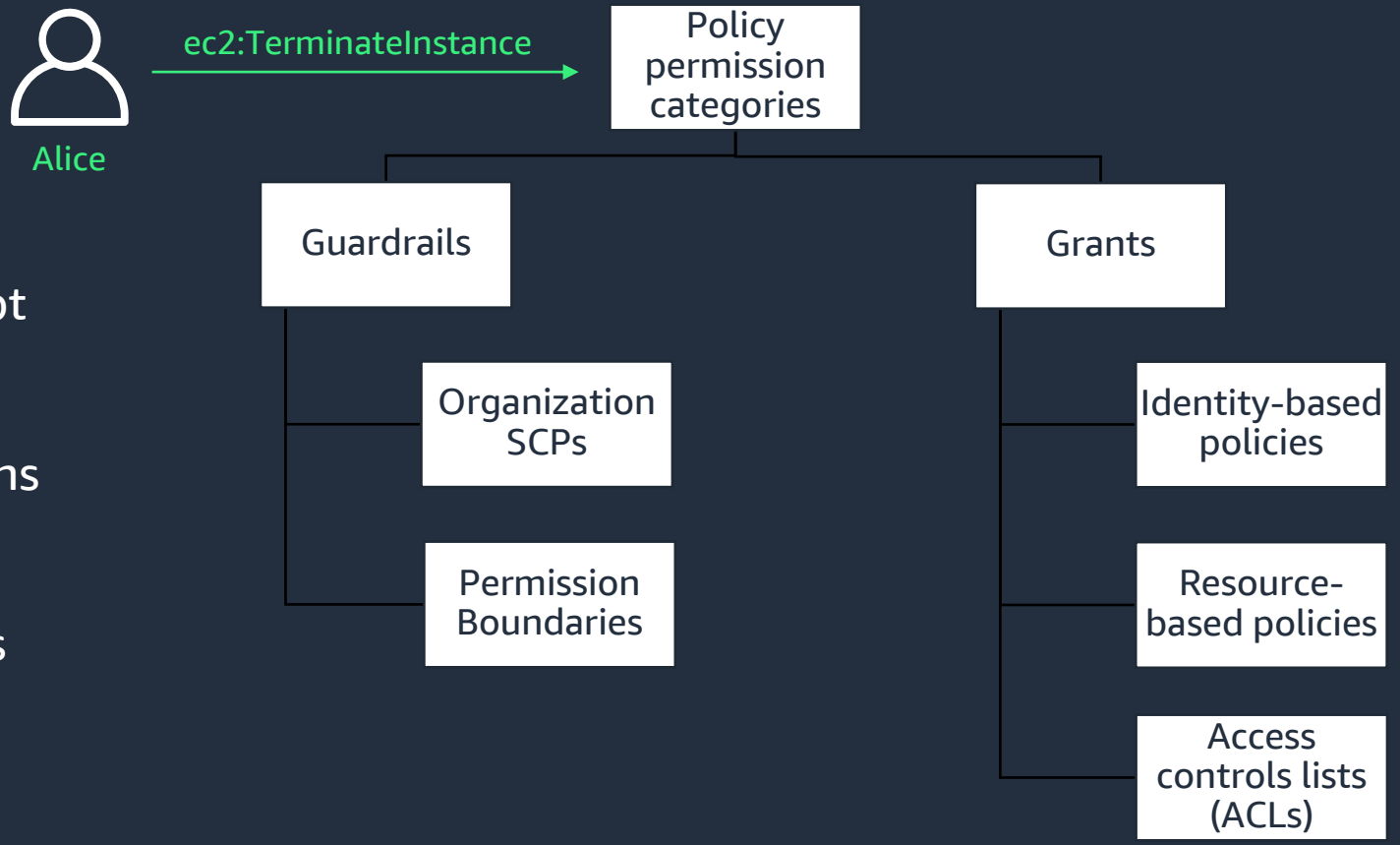
- Automate all the things! Code is predictable, repeatable, and auditable.

- There is no “Domain Admin” with god-like powers.
  - Access to physical systems requires multi factor awareness.
  - Access is extensively audited.
  - Access is granted on-demand as only as-needed

- We purposely lock ourselves out of your data.
  - We can’t access your account without your explicit permission.
  - Even then, we are limited to what can be done.

Authenticate and Authorize

Alice can only terminate an instance if everything agrees that she can.



No one is authorized in your account except who you let in

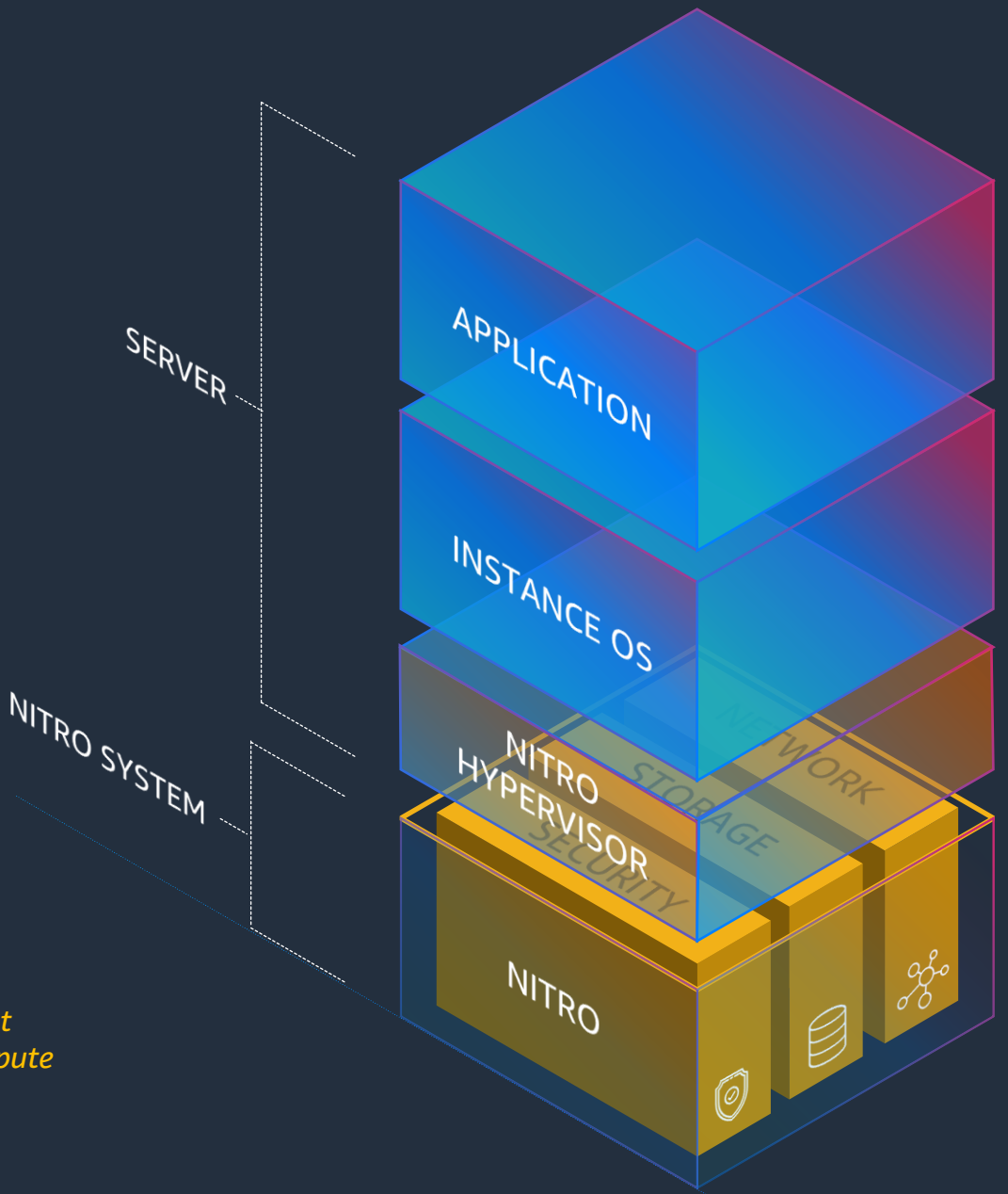
Authorization means evaluating permissions from multiple categories

Guardrails to create immutable boundaries

Grants to provide specific permissions to specific things

The AWS Nitro System architecture

OFFERING THE BEST SECURITY, PERFORMANCE, AND INNOVATION IN THE CLOUD



AWS Nitro System gets independent affirmation of its confidential compute capabilities

aws Canada

Active Defense

"AWS stirs the MadPot – busting bot baddies and eastern espionage"

aws Canada

Thank you!