

# AWS State, Local, and Education Learning Days

Philadelphia



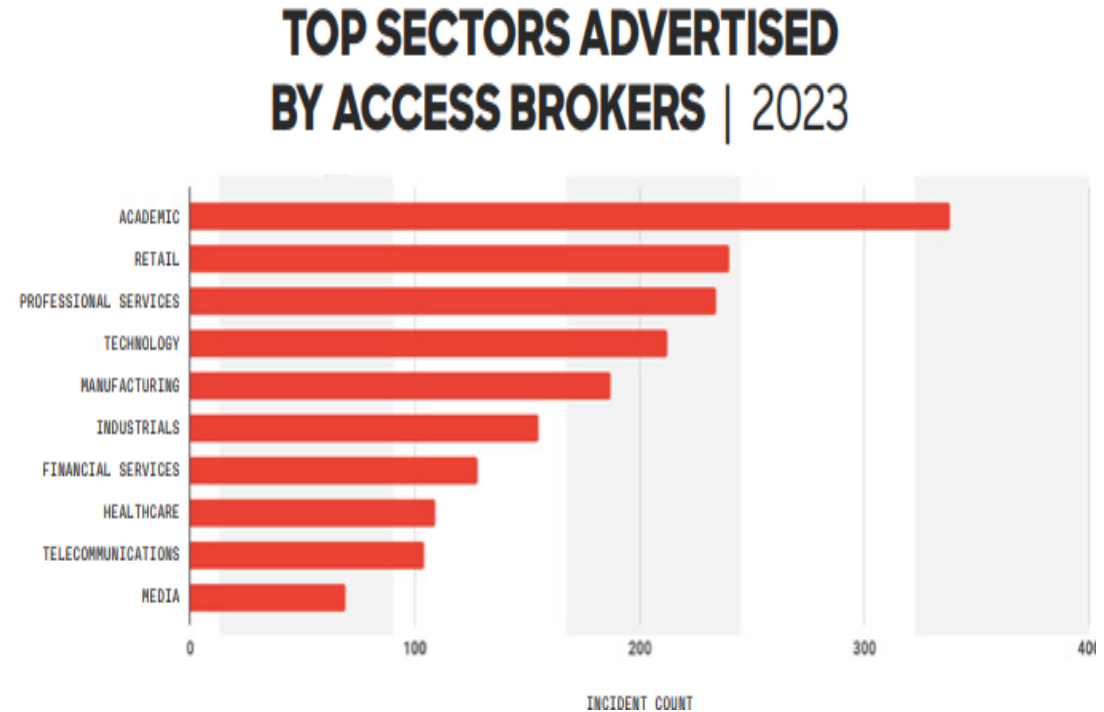
# Cyber trends and best practices

**Jesse Roberts (he/him)**

Principal Solutions Architect, Lead SA SLG/EDU US East  
Amazon Web Services  
[slgjesse@amazon.com](mailto:slgjesse@amazon.com)

# Cyber threat landscape

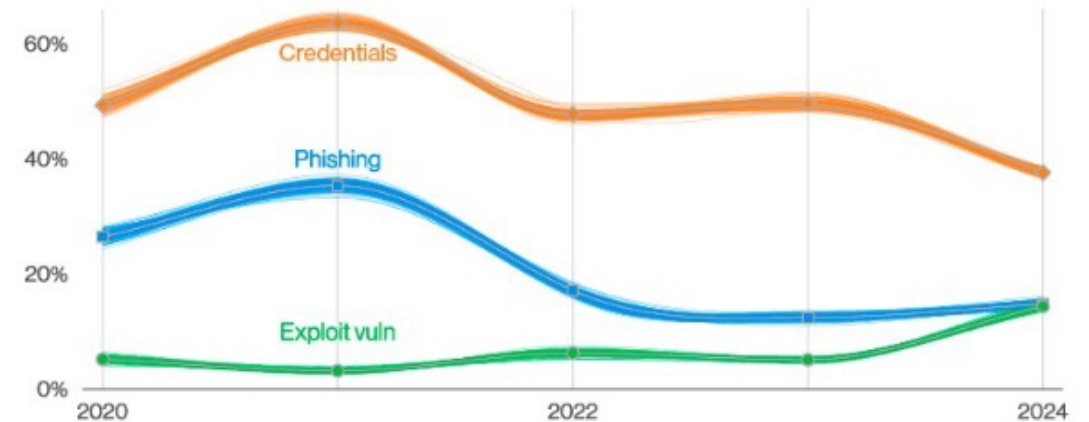
- Identity-based attacks on the rise
- 34 new threat actors
- 20 percent increase in access brokers
- Breakout time decreased from 84 minutes to **62 minutes in 2023**
- Fastest breakout time two minutes and seven seconds



Source: CrowdStrike 2024 Global Threat Report

# Cyber threat landscape

- 1/3 of all breaches involved ransomware
- Pure extortion on the rise and is a component of 9% all breaches
- Ransomware a top threat across 92% of all industries
- 68% of breaches involved “human element”
- 15% of breaches involved a third-party party



**Figure 6.** Select ways-in enumerations in non-Error, non-Misuse breaches over time

Source: Verizon 2024 Data Breach Investigations Report

# Challenges and threats facing public sector

- Compliance requirements
- Lack of data / IT strategy
- Workforce shortages
- Legacy infrastructure
- Increase in connected devices
- Insecure systems
- Lack of security as a culture mindset
- Third-party risks
- Emerging technologies & threats

TOP STORY

## FMU hit by widespread cyberattack

Miami Times Staff Report Apr 2, 2024 Updated Apr 3, 2024

Economy / Business / Health News Florida

## Up to \$30 million in revenue at risk at Miami's Jackson Health due to cyberattack

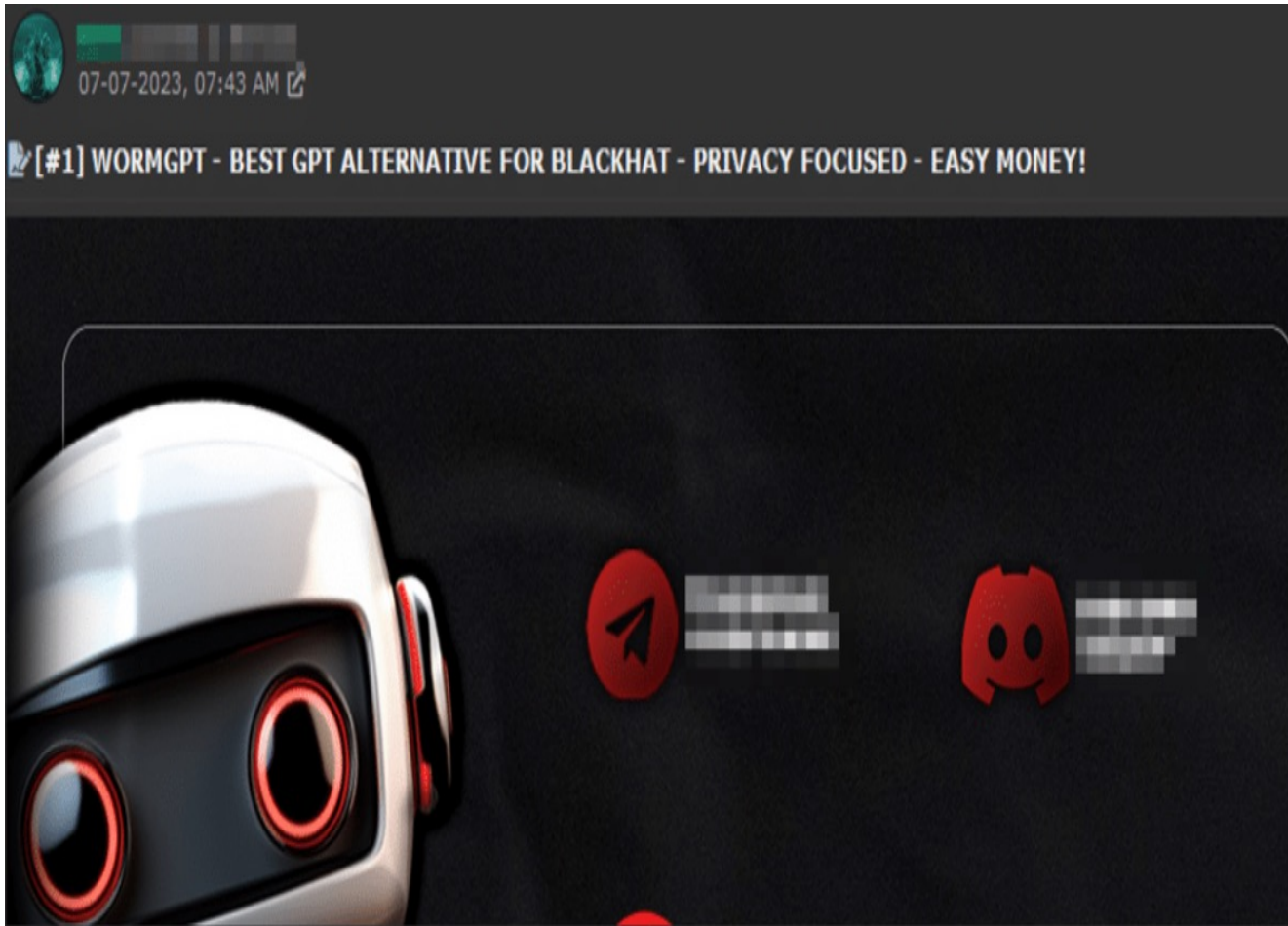
CYBERATTACK

**'We should all be concerned': Effects linger following Change Healthcare cyberattack**

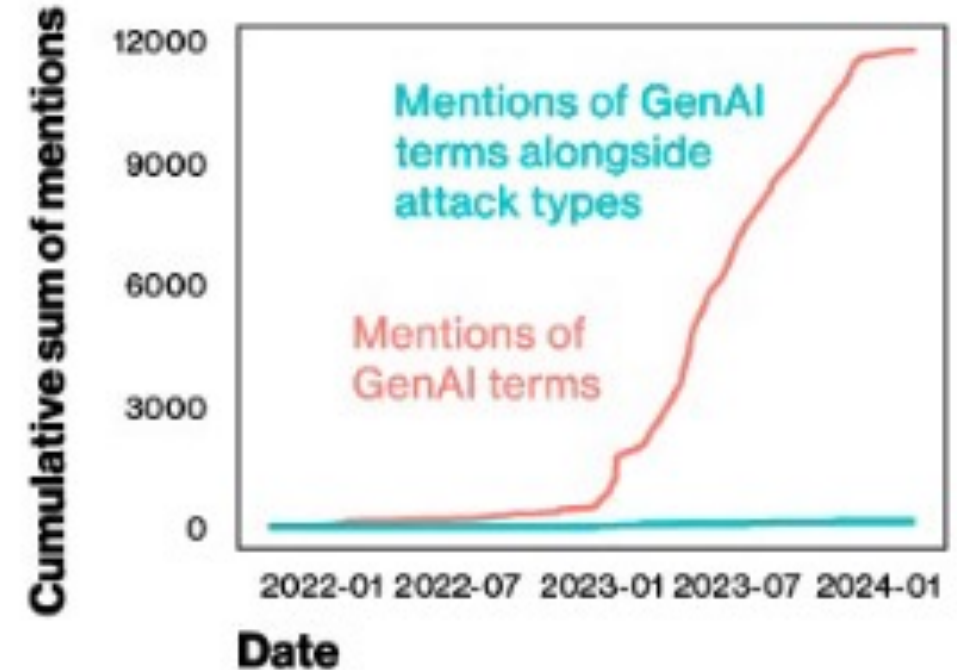
Jackson Health System in Miami was one of the hospitals affected by the attack

**St. Cloud most recent in string of Florida cities hit with ransomware**

# Prevalence of cyber attacks – WormGPT anyone?



Source: Krebs on Security: Meet the Brains Behind the Malware-Friendly AI Chat Service 'WormGPT'



**Figure 14.** Cumulative sum of GenAI in criminal forums

Source: Verizon 2024 Data Breach Investigations Report

# Risk mitigation strategies

# Recommendations for organizations



Invest in the most impactful security measures



Recognize and actively address resource constraints



Focus on collaboration and information sharing

Source: [Partnering to Safeguard K-12 Organizations from Cybersecurity Threats](#), CISA

# Cybersecurity strategies

- Whole of [insert AOR] cybersecurity
- Establishing governance models
- Developing cybersecurity strategic plans
- Collaborating across the sector lines
- Focusing on mission areas as priority
- Developing use cases to leverage AI/ML



Fig. 2. CSF Functions

# Cybersecurity legislation trends


## 2023 EDUCATION CYBERSECURITY BILLS & LAWS



# Cybersecurity legislation trends


- **Cyber risk insurance funds:** States created these funds for school districts to mitigate increasing insurance costs
- **Regional alliances and partnerships:** Momentum has grown behind partnerships to promote information sharing and collaborative responses to cybersecurity incidents
- **Cybersecurity workshop expansion:** Scholarship programs have been established to address the shortage of qualified cybersecurity experts
- **Governance enhancement:** Efforts have been made to bolster governance structures to consolidate responsibility and promote prevention and response mechanisms across agencies
- **Cybersecurity task forces:** Several task forces have been established to study and evaluate the cybersecurity landscape, including how artificial intelligence impacts the field


# Cyber insurance

 Lower/reduced coverage

 Higher rates

 Mandatory requirements

 Less cyber underwriters

 FTC suing non-compliant organizations

## Top Cybersecurity Controls

The key to insurability, mitigation, and resilience

### Preparation for the underwriting process:

1. Start early! Without positive responses in the top 5 control categories, coverage offered and insurability may be in question.
2. Evaluate your cybersecurity maturity by completing Marsh's Cyber Self-Assessment – where improvements are needed, leverage [Cyber Catalyst vendors](#).
3. Expect more rigorous underwriting and more detailed questions from underwriters.



Multifactor authentication for remote access and admin/privileged controls



Endpoint Detection and Response (EDR)



Secured, encrypted, and tested backups



Privileged Access Management (PAM)



Email filtering and web security



Patch management and vulnerability management



Cyber incident response planning and testing



Cybersecurity awareness training and phishing testing



Hardening techniques, including Remote Desktop Protocol (RDP) mitigation



Logging and monitoring/network protections



End-of-life systems replaced or protected

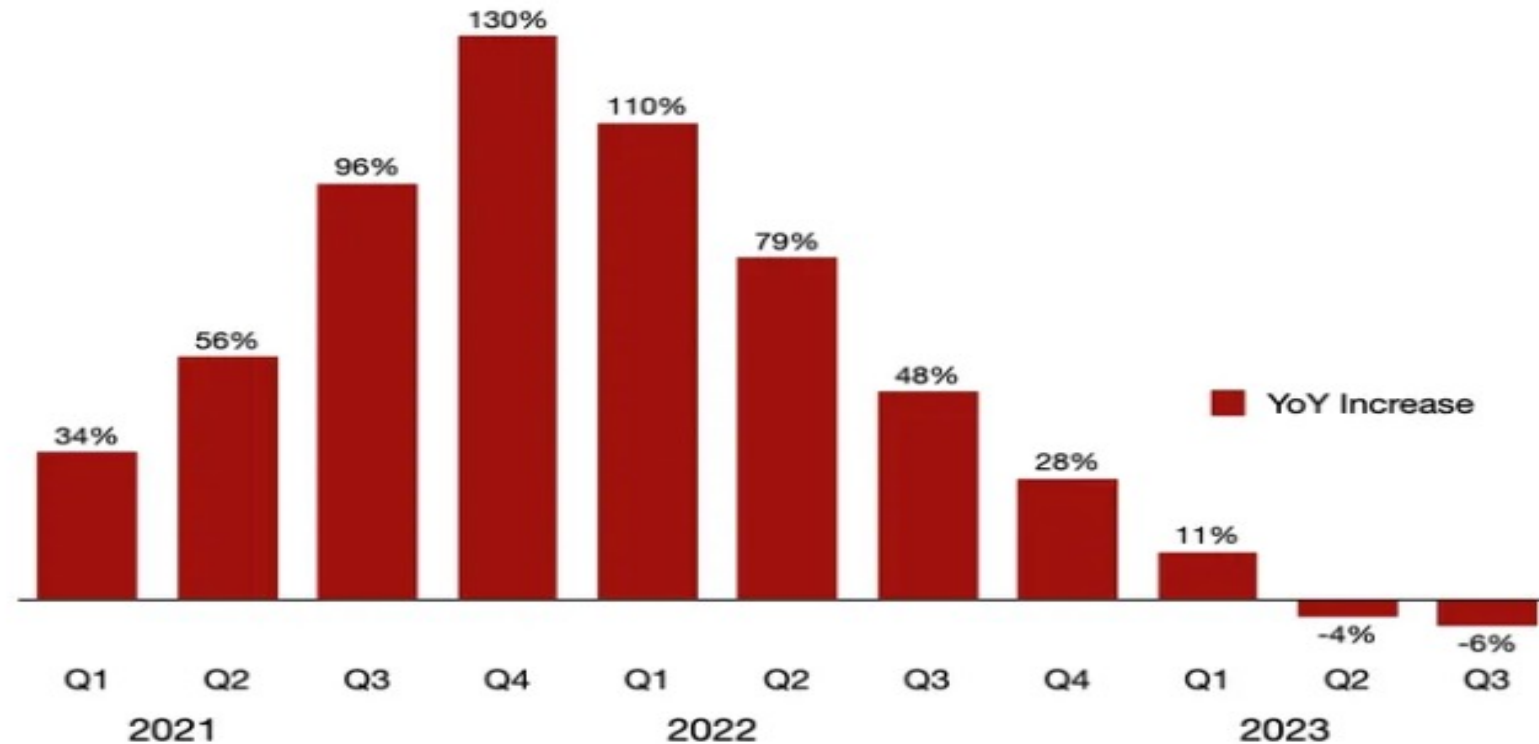


Vendor/digital supply chain risk management



Note: Each insurance carrier has their own specific control requirements that may differ by company revenue size & industry class. For more on the Cyber hygiene controls critical as cyber threats intensify ([marsh.com](#))

# Cyber insurance market



## Global insurance markets: Rates continue to stabilize entering 2024

Global commercial insurance rates rose 2% in the fourth quarter of 2023, compared to 3% in the prior two quarters, according to the *Marsh Global Insurance Market Index*. This was the twenty-fifth consecutive quarter in which composite rates rose, continuing the longest run of increases since the inception of the index in 2012.

# AWS Cyber Insurance Partner

Cyber Insurance Partners have committed to generating a quote for AWS customers within two business days of the request. Customers will use external SaaS insurance platforms that provide:

- Direct, easy-quote systems that run an audit of their AWS environments and security posture to provide a cyber insurance quote, including recommended actions that can result in lower rates
- Ongoing subscription-based cyber insurance that moves with the customer based on their assessed security posture and size, allowing customers' coverage to match and grow with them

[AWS Cyber Insurance Partners - Amazon Web Services \(AWS\)](#)

# Think differently – Smart procurement considerations

- Streamline cybersecurity solution procurement to standardize operations and reduce costs
- Find ready-made solutions in a digital catalog to support cybersecurity governance and more
- Prioritize resilience for your infrastructure
- Skill your organization with no-cost cybersecurity training
- Think long-term with a modernization strategy

Source: [5 things to consider while applying to the State and Local Cybersecurity Grant Program \(SLCGP\) | AWS Public Sector Blog \(amazon.com\)](#)



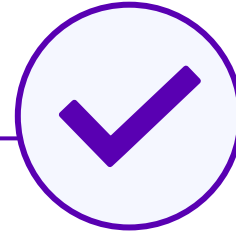
# Imagine if there was a service that...



**Allows for  
State entities  
to procure  
security  
capabilities  
based specific  
cyber gaps**



**Centralizes  
and allows  
Enterprise  
visibility of  
contracts for  
mandatory  
reporting**



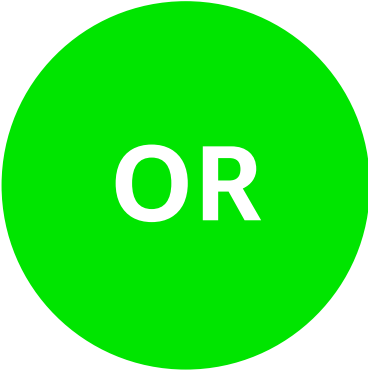
**Allows for  
volume  
discounts and  
cost  
optimization**



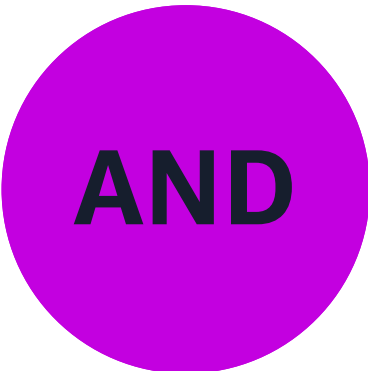
**Enables  
centralized  
enterprise  
security  
visibility into  
threats across  
the state**

# Why the cloud?

Before...

Move fast  Stay secure

Now...

Move fast  AND Stay secure

# Why the cloud - Highest standards for privacy and data security



**Meet data  
residency  
requirements**



**Encryption at scale**



**Comply with local  
data privacy laws**



Access services and  
tools that enable you  
to  
**build compliant  
infrastructure**

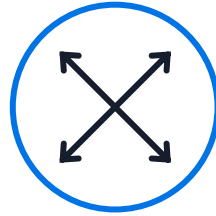
# Why the cloud - Inherit global security and compliance controls



# Why the cloud - Infrastructure and services to elevate your security



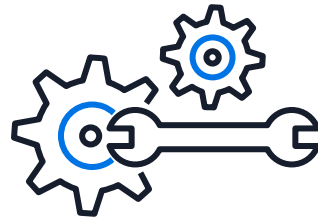
Inherit global security and compliance controls



Scale with superior visibility and control



Highest standards for privacy and data security

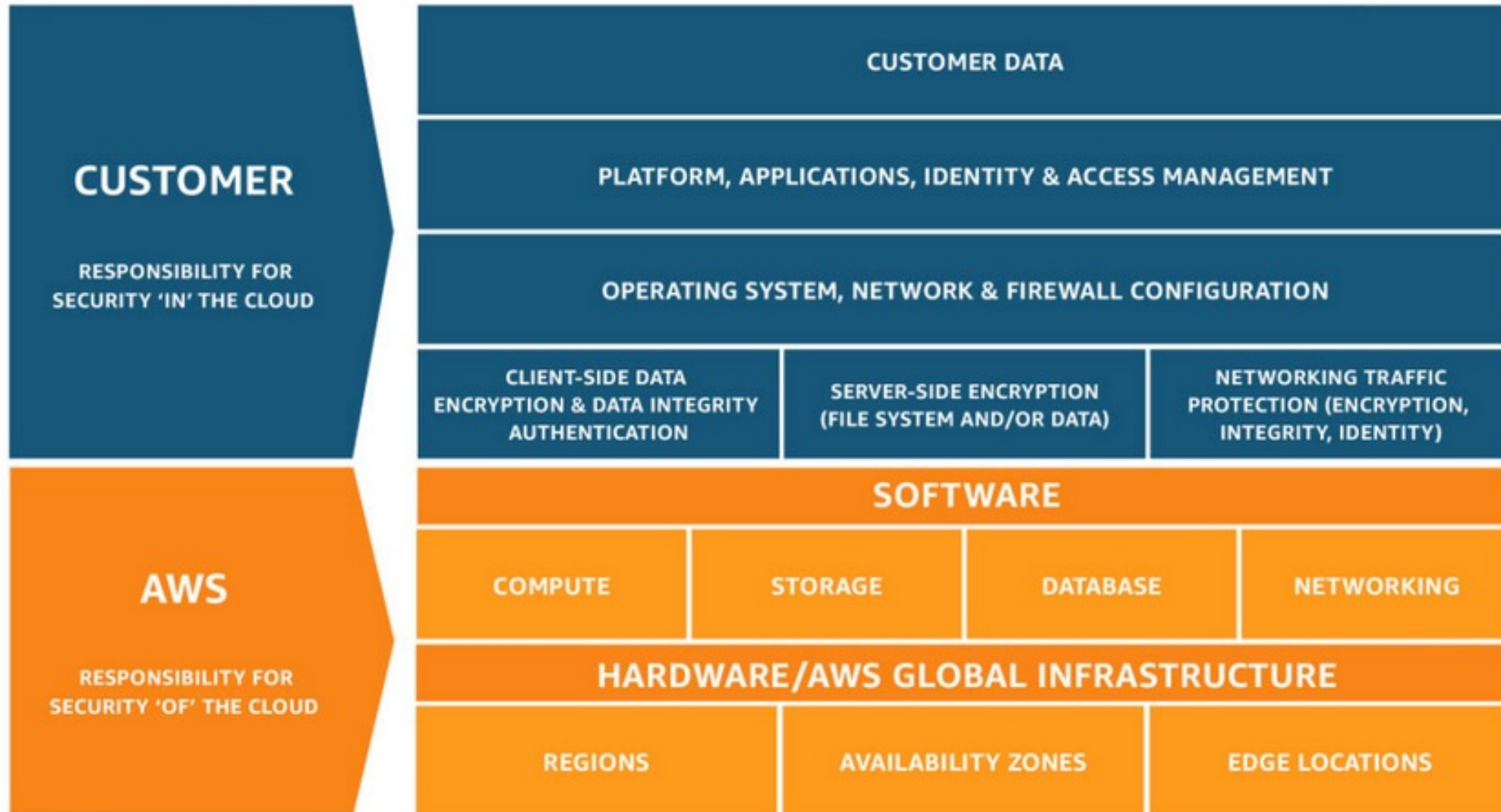


Automate and reduce risk with deeply integrated services



Largest ecosystem of security partners and solutions

# Shared Responsibility Model






# What about generative AI?

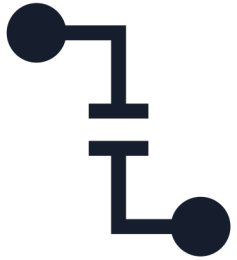
- ✓ Ease of use – Reduce friction to deployment
- ✓ Security and privacy – Top of mind for customers
- ✓ Choice – Multiple models to meet your needs
- ✓ Availability – Scale to meet customers' needs

# Core AWS security services

- Deploy a defense in depth strategy
- Activate and operationalize across accounts

		
<b>Security monitoring &amp; threat detection</b>	<b>Edge / perimeter protection</b>	<b>Data protection</b>
<div><b>AWS Security Hub</b> <b>Amazon GuardDuty</b></div> <div>Amazon Detective Amazon Inspector Amazon Security Lake</div>	<div><b>AWS Shield Advanced</b></div> <div>AWS Firewall Manager AWS WAF – Web application firewall  AWS Network Firewall  Route53 Resolver DNS Firewall</div>	<div><b>AWS Key Management Service (KMS)</b></div> <div>Amazon Macie AWS CloudHSM  AWS Certificate Manager  AWS Secrets Manager  Server-Side Encryption</div>

# Enterprise-wide security data analysis is challenging



## Inconsistent and incomplete data

Logs and alerts in varying formats scattered across the organization in tough to find data silos



## Growing volumes of security data

Explosion of security and log data means more time wrangling data than actual analysis



## Inefficient use of data across use cases

Need for specialized tools can result in data duplication and reprocessing for each use case



## Lack of direct control over processed data

Certain tools store processed data in their own system. This reduces your flexibility in using that data.

# Security Lake

AUTOMATICALLY CENTRALIZE SECURITY DATA INTO A PURPOSE-BUILT DATA LAKE IN A FEW CLICKS



**Centralize** data automatically from cloud, on-premises, and custom security sources across regions

**Optimize** and manage security data for more efficient storage and query performance

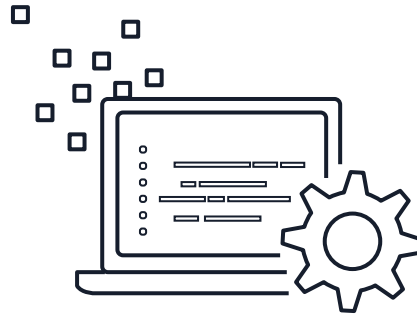
**Normalize** data to an industry standard to easily share and use with multiple analytics tools

**Analyze** using your preferred analytics tools while retaining control and ownership of your security data

# Cloud is only part of the recipe for success



Organization



Process



Culture

# Opportunities for success - Reassess, reinforce and reconnect

- ✓ Develop a continuous monitoring plan
- ✓ Prioritize data resilience and modernization
- ✓ Leverage cloud for resiliency and immutable backup capabilities
- ✓ Implement information sharing for collective defense – use “persistent collaboration”
- ✓ Reassess/review security architecture periodically
- ✓ Use integrated solutions w/automation
- ✓ Leverage federal funding opportunities
- ✓ TEST, TEST and...TEST
- ✓ Revamp procurement processes - create digital catalogs for approved services
- ✓ Apply responsible AI principles to all AI/ML projects



## How do we improve?

CIO/CTO/ CFO/Head of Security, IT Manager, Director of IT Security, Security Operations Manager, Head of Security Architecture

### TOP 3 WAYS

- › Trained and skilled workforce leads to innovation, cultural and behavioral changes
- › Drive growth and reduce risks through IT modernization efforts
- › Take a data centric approach to security and adopting an industry framework for continuous assessment

# Parting advice: BE SAFE

B – be collaborative

E – educate and upskill your teams

S – secure your data

A – apply cyber hygiene practices

F – fund your cyber projects as a lifecycle

E – everybody is part of the cyber ecosystem



# Thank you!

**Jesse Roberts (he/him)**

Principal Solutions Architect, Lead SA SLG/EDU US East  
Amazon Web Services

[slgjesse@amazon.com](mailto:slgjesse@amazon.com)

**Please complete the survey  
for this session**



**Track Name: Executive Track**

Session Name: Cyber trends and best practices