

David Brown

Vice President, Amazon Elastic Compute Cloud (Amazon EC2)

David Brown joined AWS in 2007 as a software developer based in Cape Town, South Africa, working on the early development of Amazon EC2—a web service that provides secure, resizable compute and networking capacity in the cloud. Over the last 15 years, he's held several roles within the Amazon EC2 organization, shaping the service into what it is today. Prior to joining AWS, David worked as a software developer within a financial industry startup.

The power of cloud network innovation

From the very beginning, the AWS network has been the foundation for how AWS delivers on the promise of cloud computing. In this talk, join Dave Brown, VP of Amazon EC2 Networking and Compute Services, as he looks at the history of AWS networking and how its growth and innovation continues to this day—helping unleash your creativity and make leaps forward in what's possible. With a combination of real-world examples and looks behind the scenes, Dave dives into the latest innovations in AWS core networking infrastructure, VPC networking, data center networking for AI/ML, security, and global connectivity.

Networking Matters

1440 Germany Gutenberg printing press

Ada Palmer "You printed 200 copies of the Bible, there are three people in town who can read."

Venice was a better market, shipping and distribution network carried the books around the world.

Without connectivity it's hard to succeed.

Connectivity drives collaboration, and collaboration drives innovation.

AWS Backbone, 5,000,000km of fiberoptic backbone

74 Zettabytes per year

Total network **capacity**

2005

2019

2023



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

2006–2011
8 new Regions

2012–2017
10 new Regions

2018–2023
14 new Regions

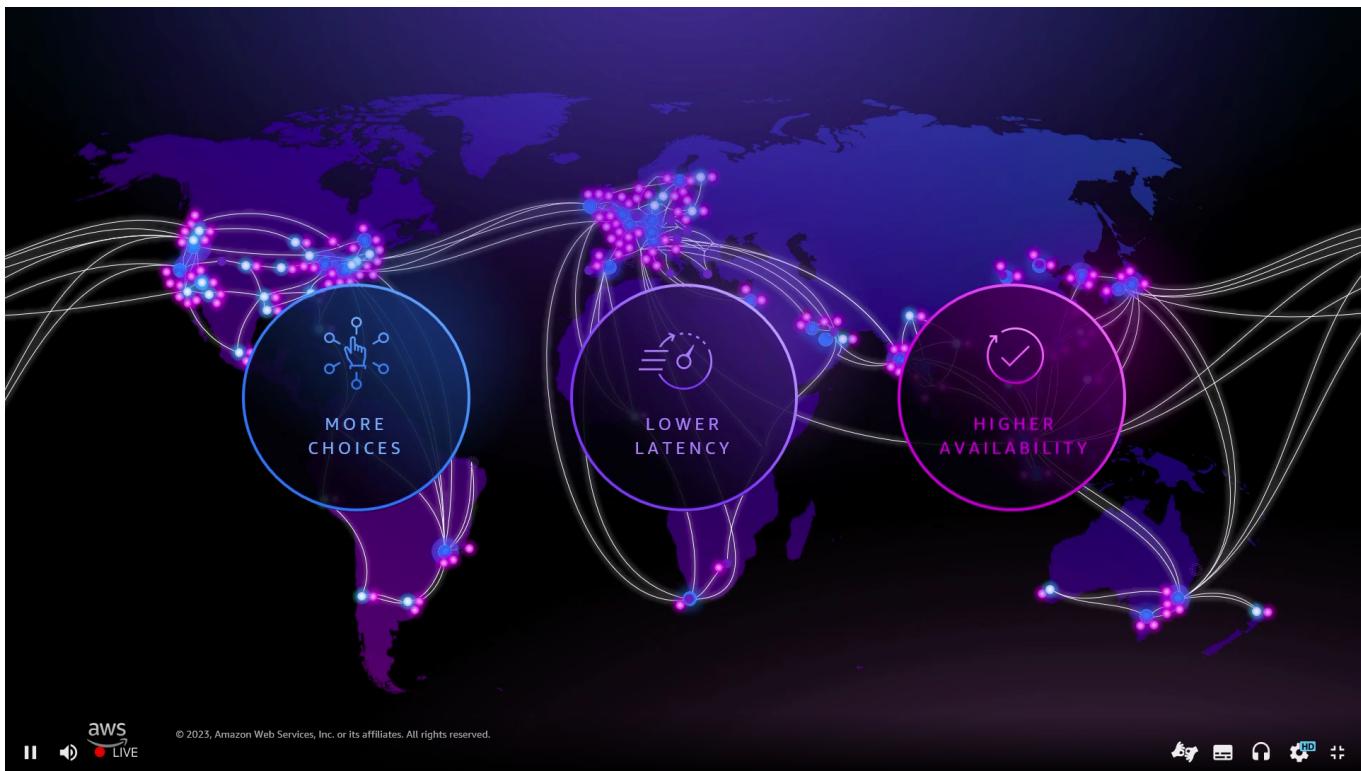
COMING SOON
4 new Regions



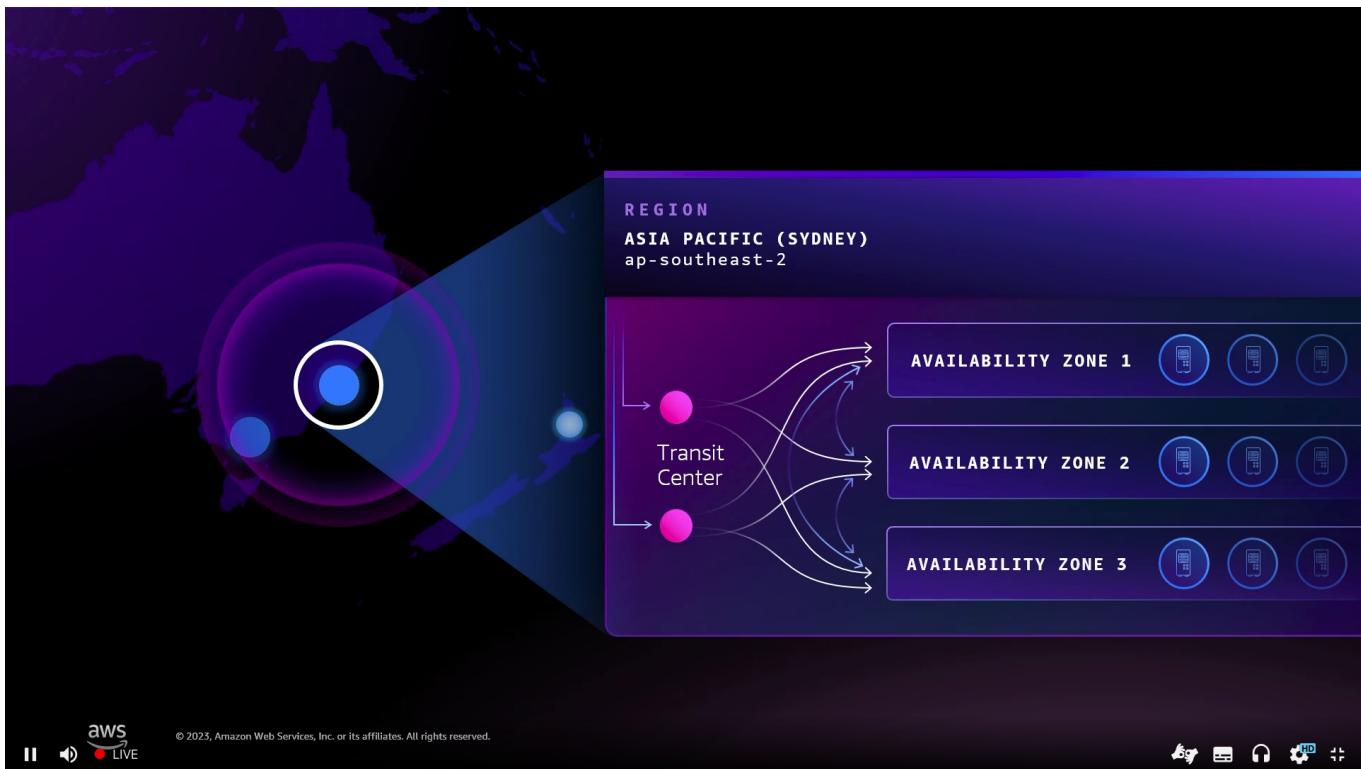
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Region expansion benefits



How AWS regions are different



Local Zones



They make "movie shows" - using Local Zone GPUs on AWS

LA Local Zone 1-2ms latency

Direct Connect colocation sites now over 130, globally.
(100Gbps)

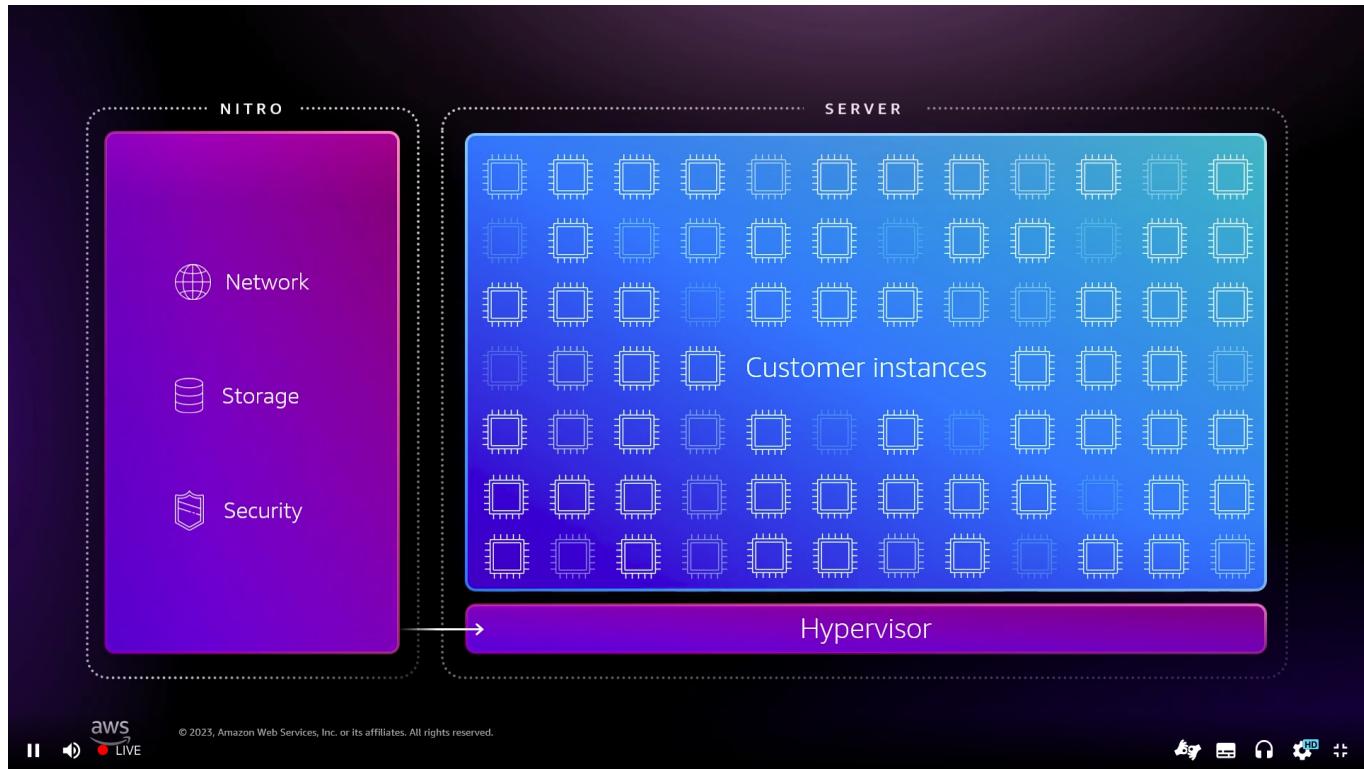
Cloudfront is 15 years old

- 600 points of presence
- 3 trillion requests per day

120Tbps peak during the NotFL SuperbOwl

Telegraph was the first computer network

AWS Nitro architecture behind EC2



Uses no part of central machine resources for their internal workloads.

This is hardware-based hypervisor virtualization.

400Gbps 2020 with C7GN instances.

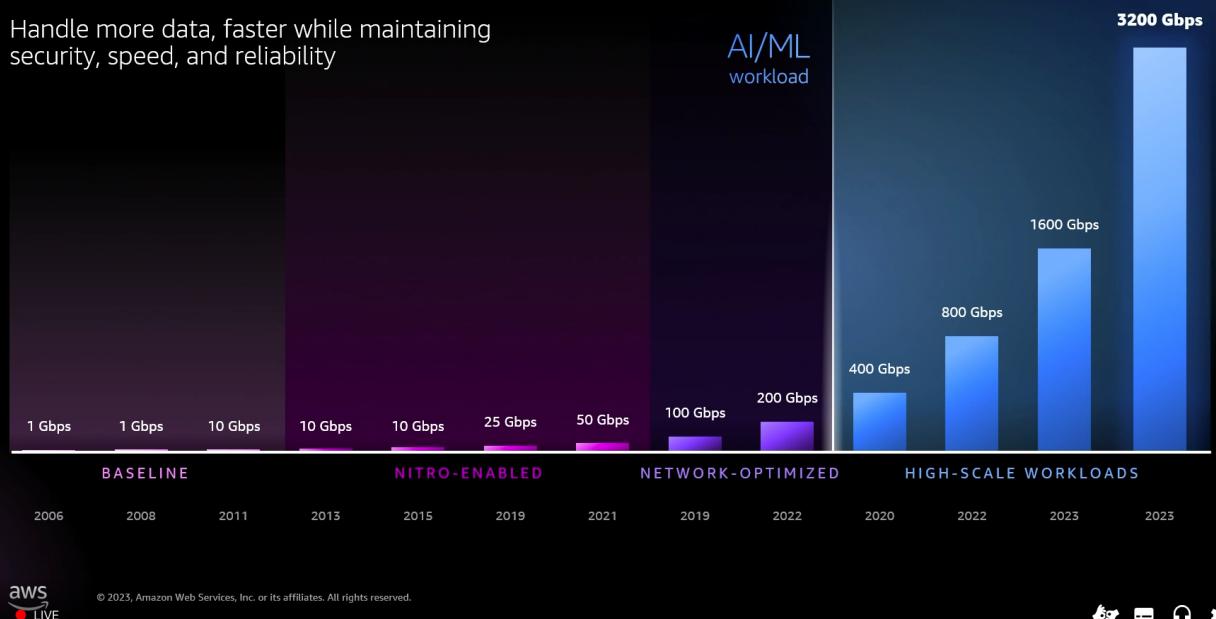
All enabled by Nitro

AI/ML workloads P4d, A100 GPU 400Gbps

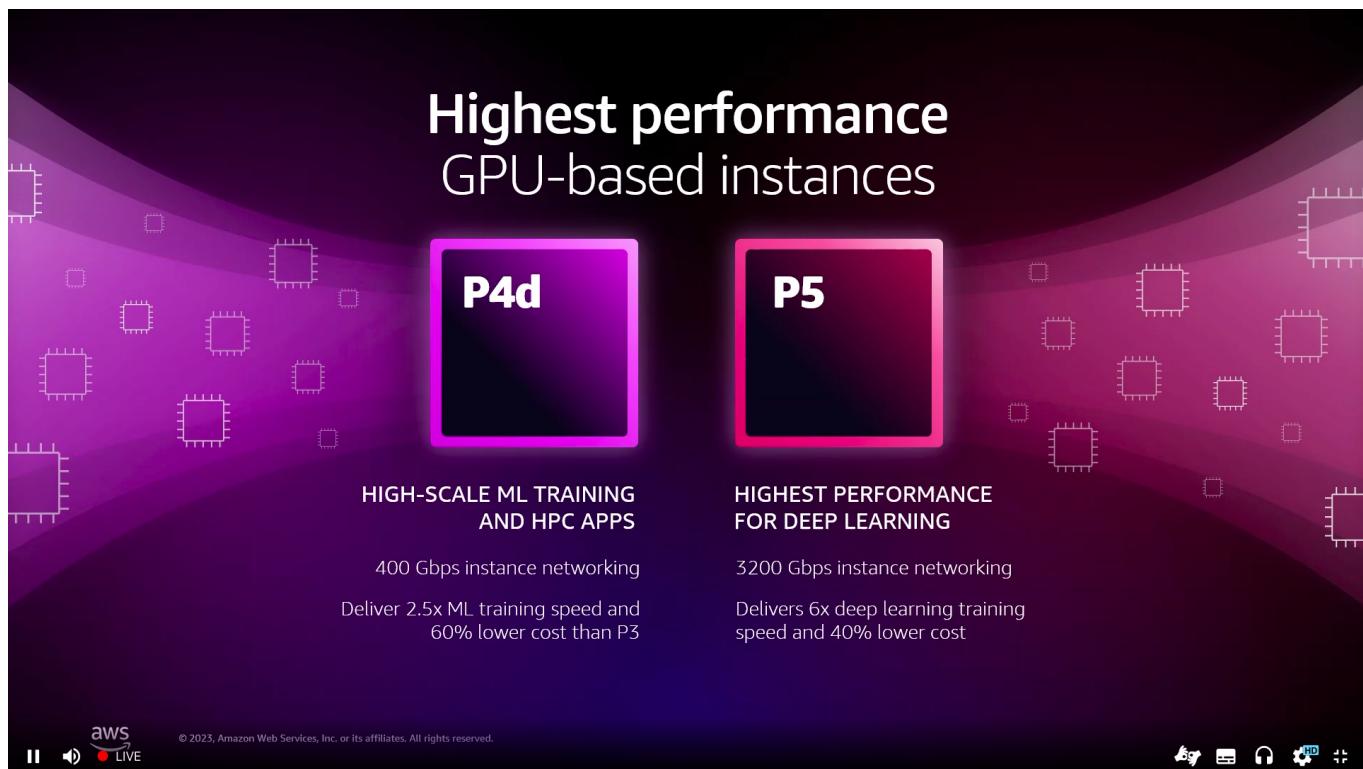
Now line go up....

Network bandwidth

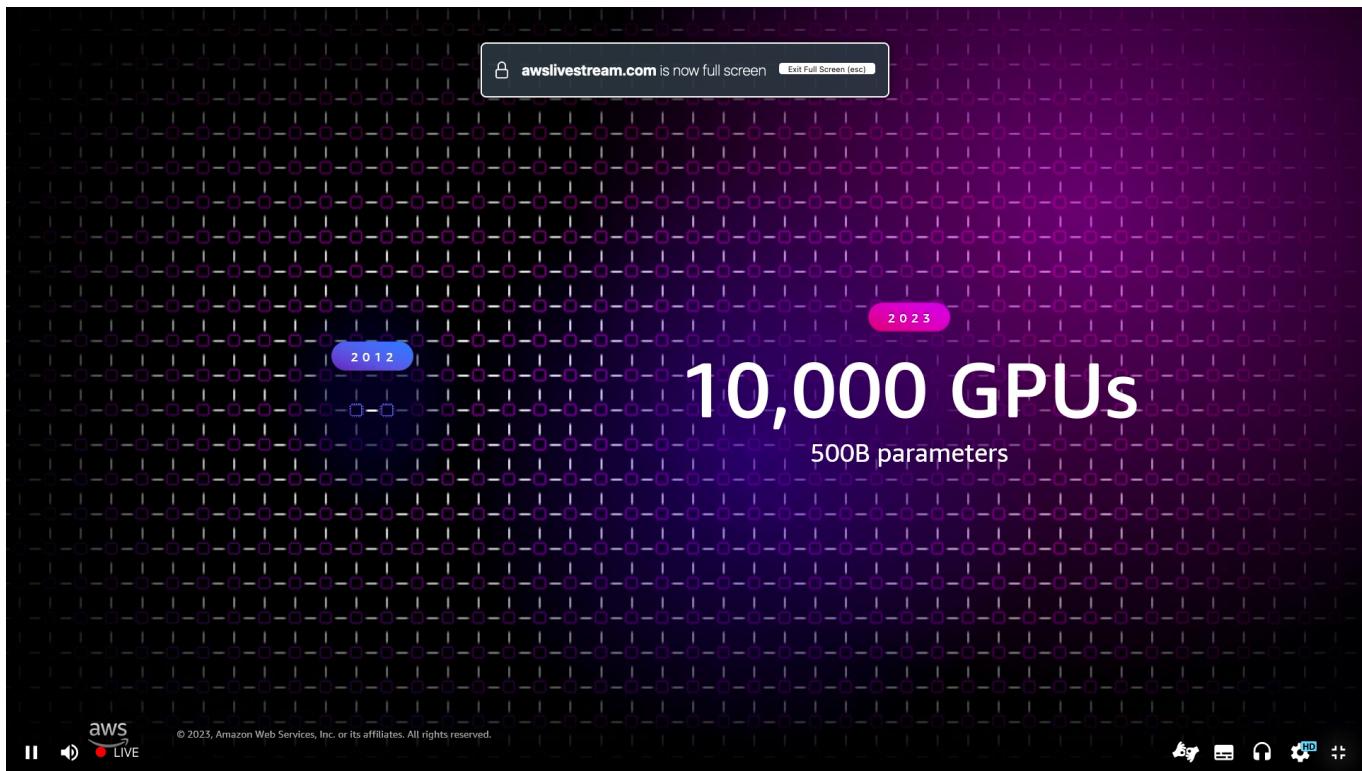
Handle more data, faster while maintaining security, speed, and reliability



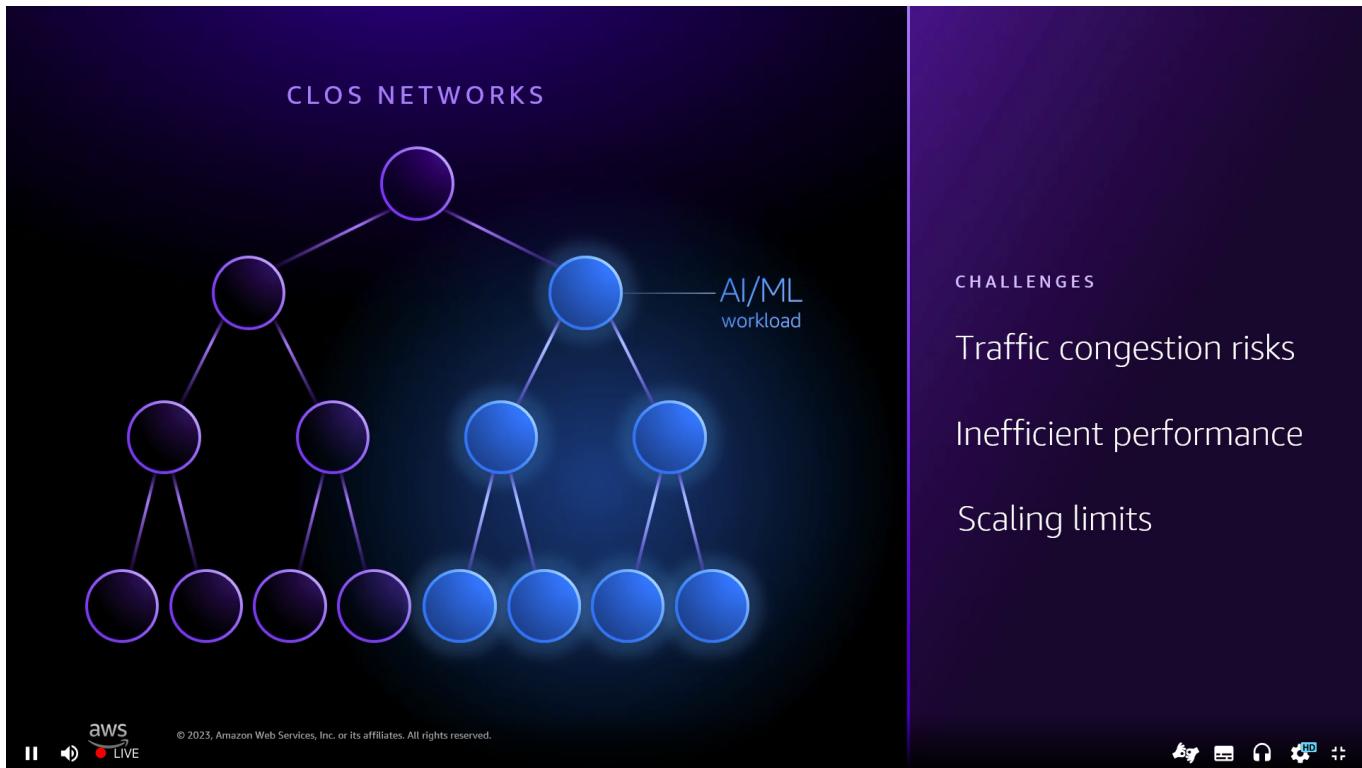
AMD H100GPU 32000Gbps on a single EC2 instance



It's a lot

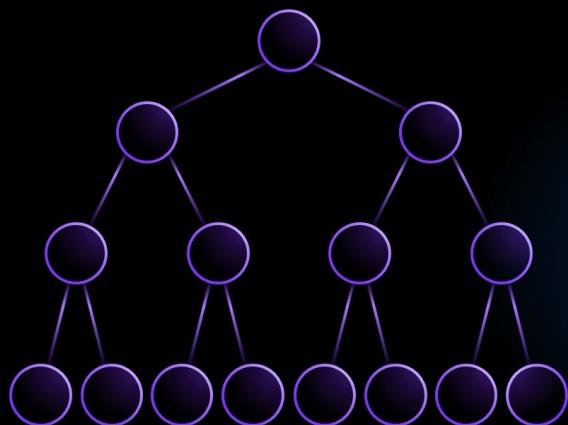


Up to 50 Petabits per second?



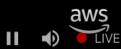
AI/ML scale is pushing network topology design

CLOS NETWORKS



AMAZON EC2 ULTRACLUSTER 1.0

Dedicated network for AI/ML



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



AMAZON EC2 ULTRACLUSTER 1.0

Dedicated network for AI/ML



CHALLENGES

Scale

From portions of buildings to multiple buildings in a campus

Performance

From 400 Gbps instances to 3.2 Tbps instances

Availability

Higher convergence time with traditional protocols (BGP/OSPF)



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



AMAZON EC2 ULTRACLUSTER 2.0



SOLUTIONS

New network design

Flatter and wider network fabric,
optimized specifically for the P5
and future ML accelerators



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

64,000 GPUs per cluster? what? eeeeeeee!

NEW

Amazon EC2 Instance Topology API

Optimized instance placement for
ML and HPC workloads

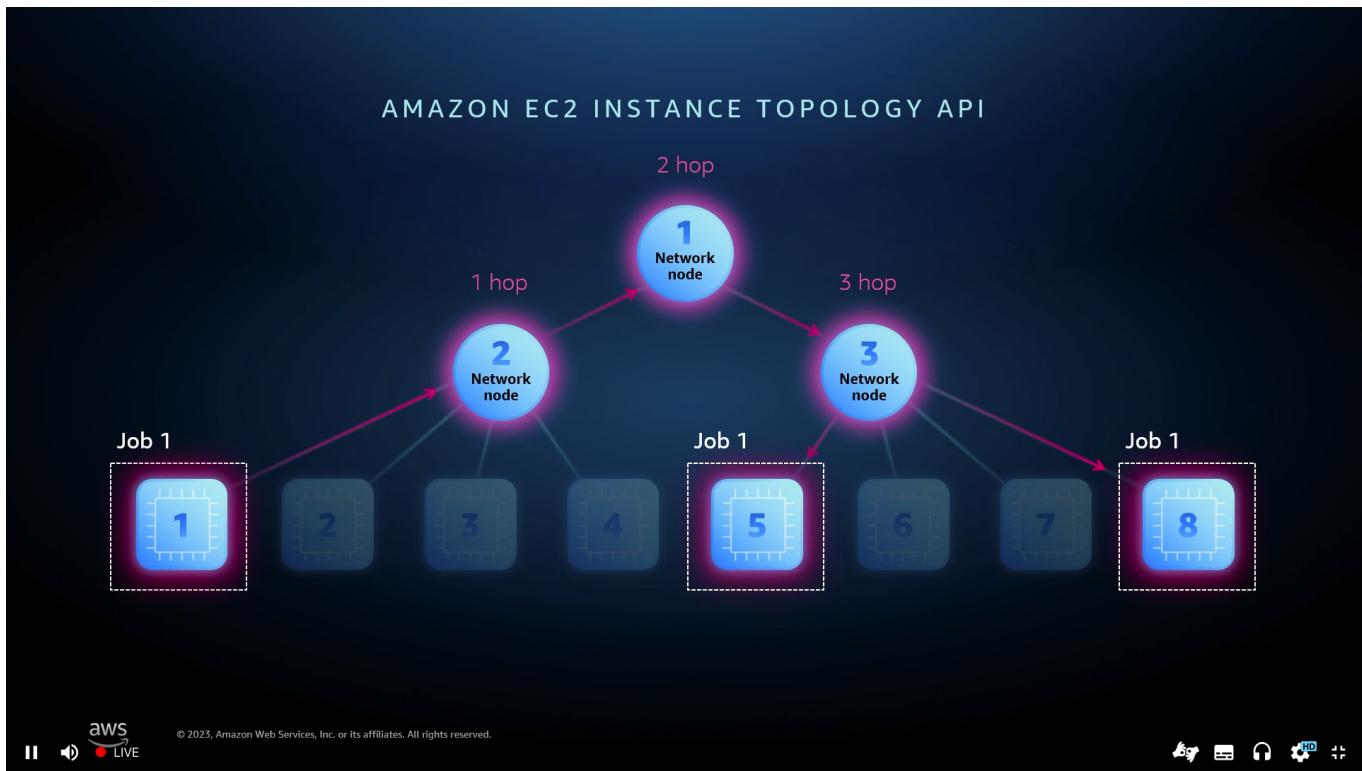
GENERALLY AVAILABLE



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

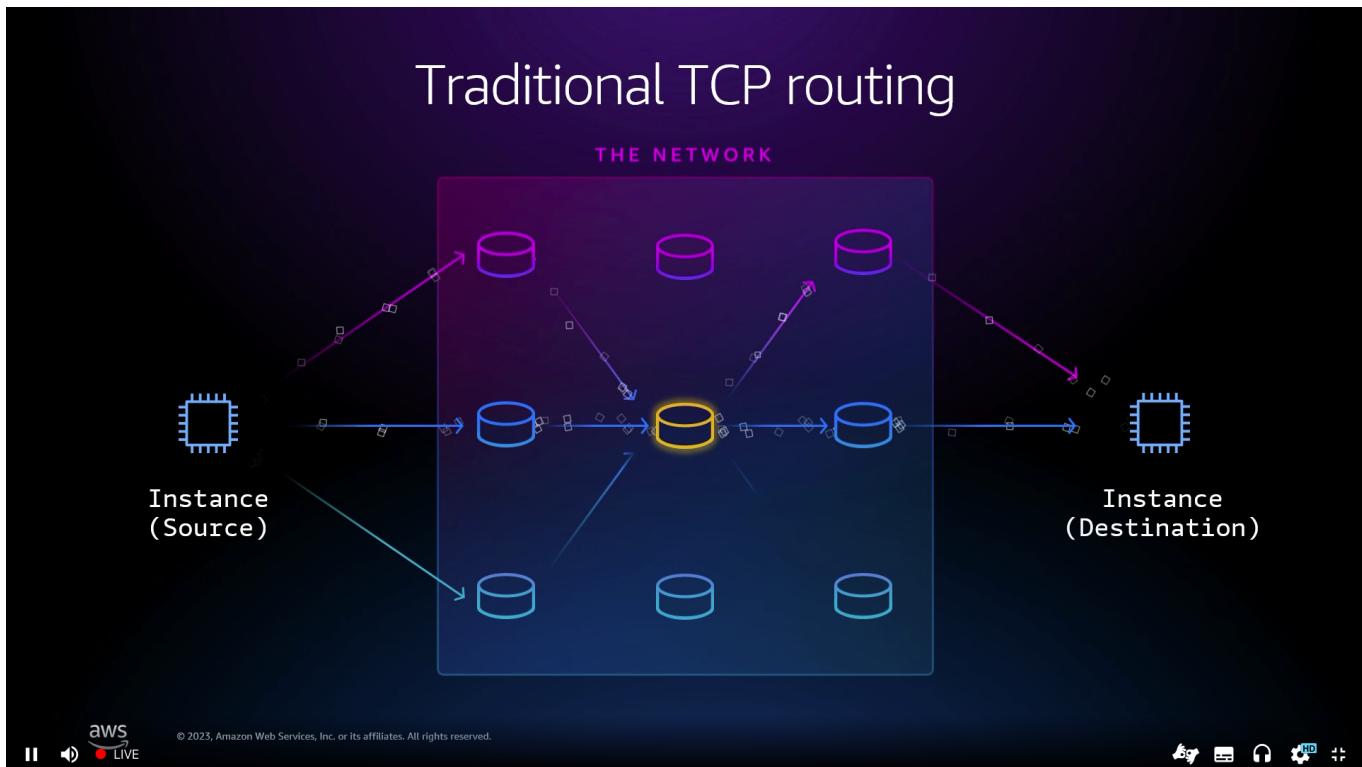


Very important to count hops for latency prediction



Topology API gives information on relative network fabric topology

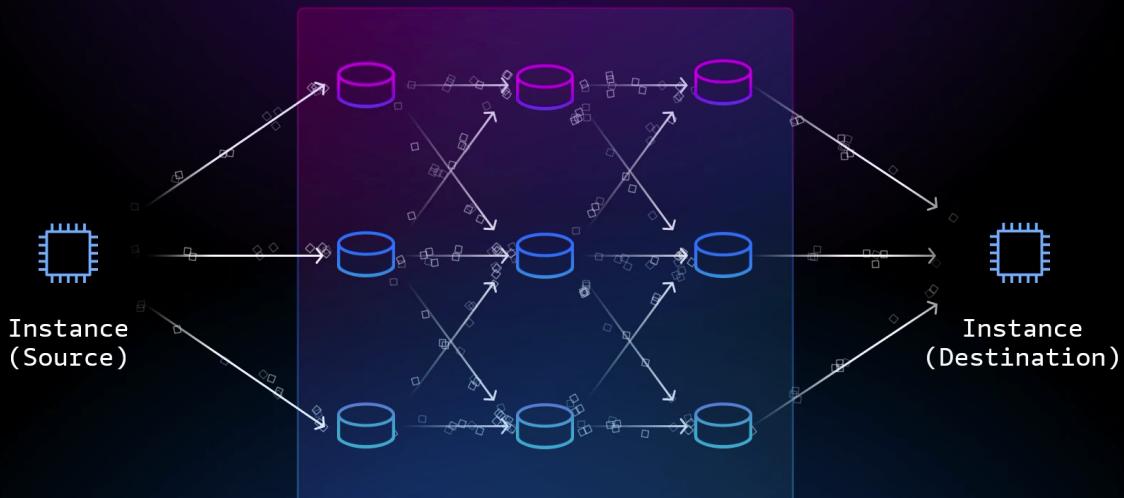
Trad TCP routing



New AWS sauce (a few years old now)

Scalable Reliable Datagram (SRD) routing

THE NETWORK



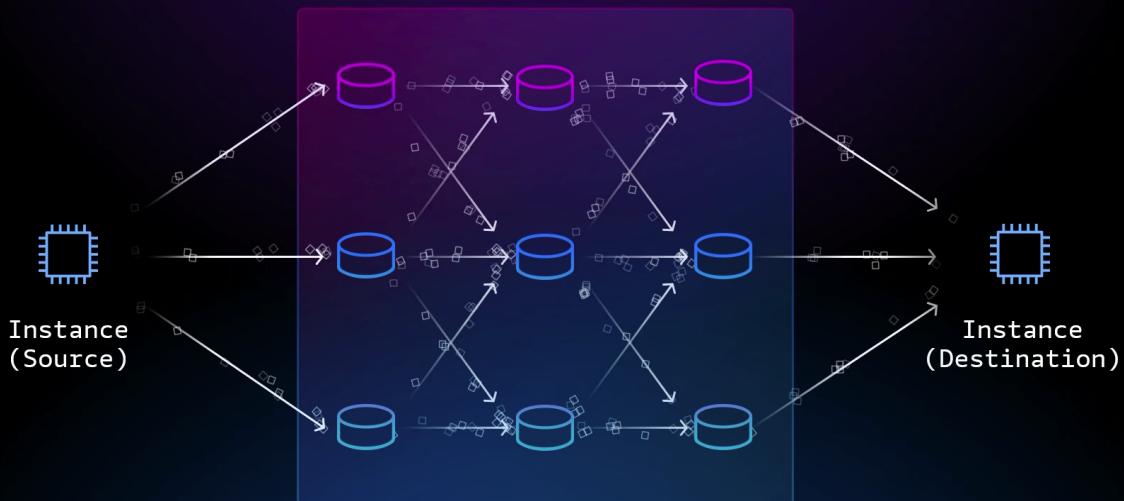
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



ENI Express SSD big data flow instance types

Scalable Reliable Datagram (SRD) routing

THE NETWORK



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Reduced P99 routing latencies by up to some big percentage...50%+?

David is AWS VPC OG dev

When the VPC feature launched AWS was one big flat network, basically, he says.

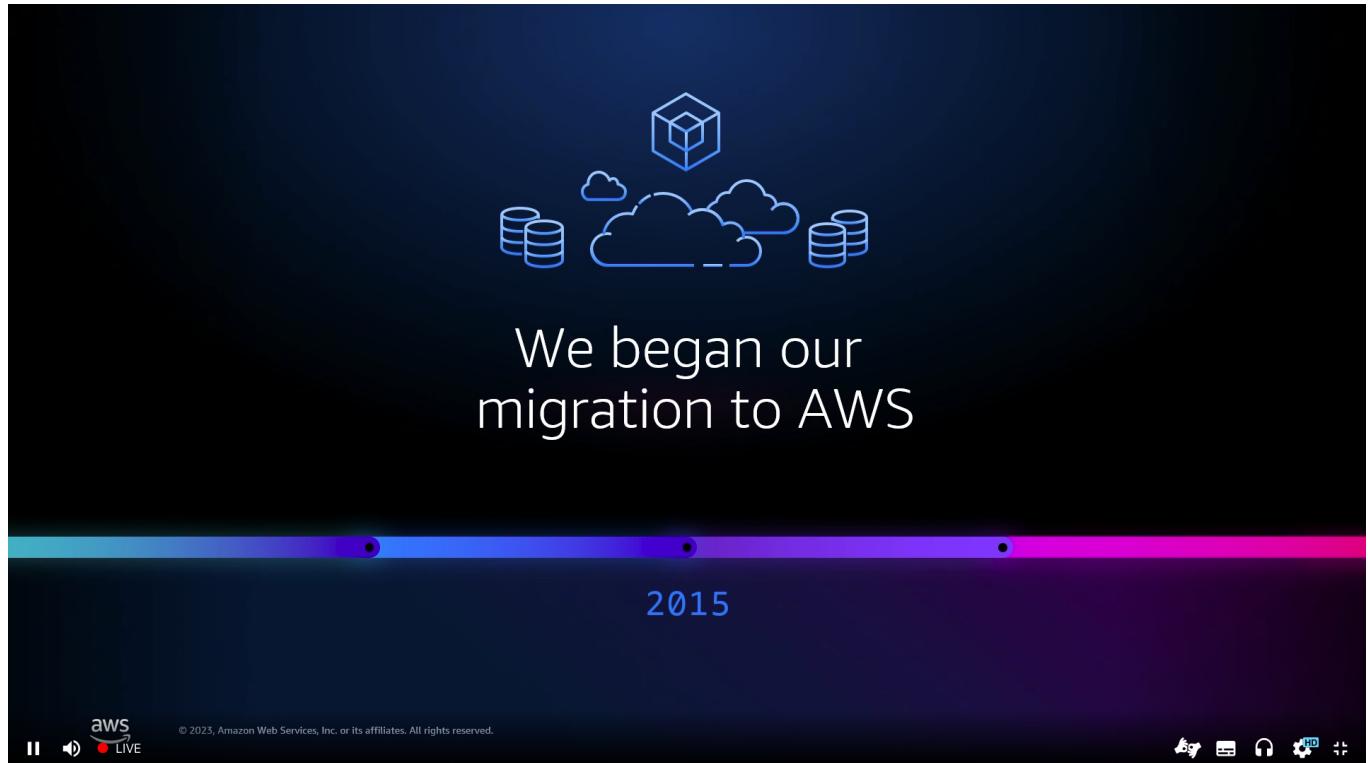
2013 VPC peering was released

Continuing need to scale pushed Transit Gateway development

CapitalOne SVP Cloud and Networking

Will "something" from CapitalOne talking about how they live on public cloud juice

2015





We're maturing on AWS

FinOps | Serverless | Network expansion

TODAY



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



100k EC2 instances

200k Lambdas, maybe more

"Any sufficiently advanced
technology is indistinguishable
from magic."

ARTHUR C. CLARKE
Author and futurist

Arthur C. Clarke - "Profiles of the Future: An Inquiry into the Limits of the Possible," 1962



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.





Large-scale distributed systems made simple



Resilience and operational integrity baked in



Automation of infrastructure as a massive enabler



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



One common set of deployment and build tools across the enterprise, not for the faint of heart, but worth it.

Serverless is the way to go, long run.

Half of their applications are running on Fargate or other Serverless-ish things

VPC peering complexity at scale



AWS Transit Gateway



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



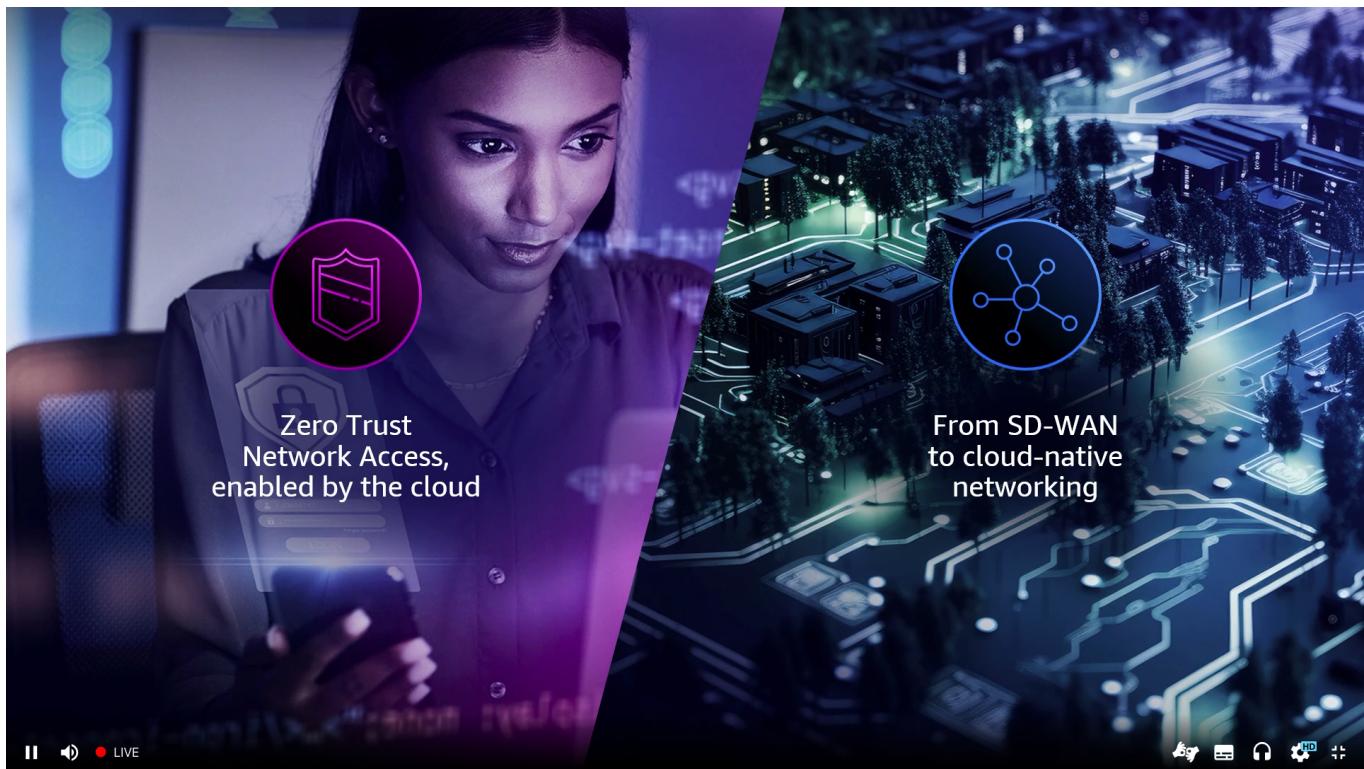
Continuing to expand



They test network segmentation



Network address IP space is still a challenge. CIDR allocation still matters.
Private NAT gateways are the good answer.



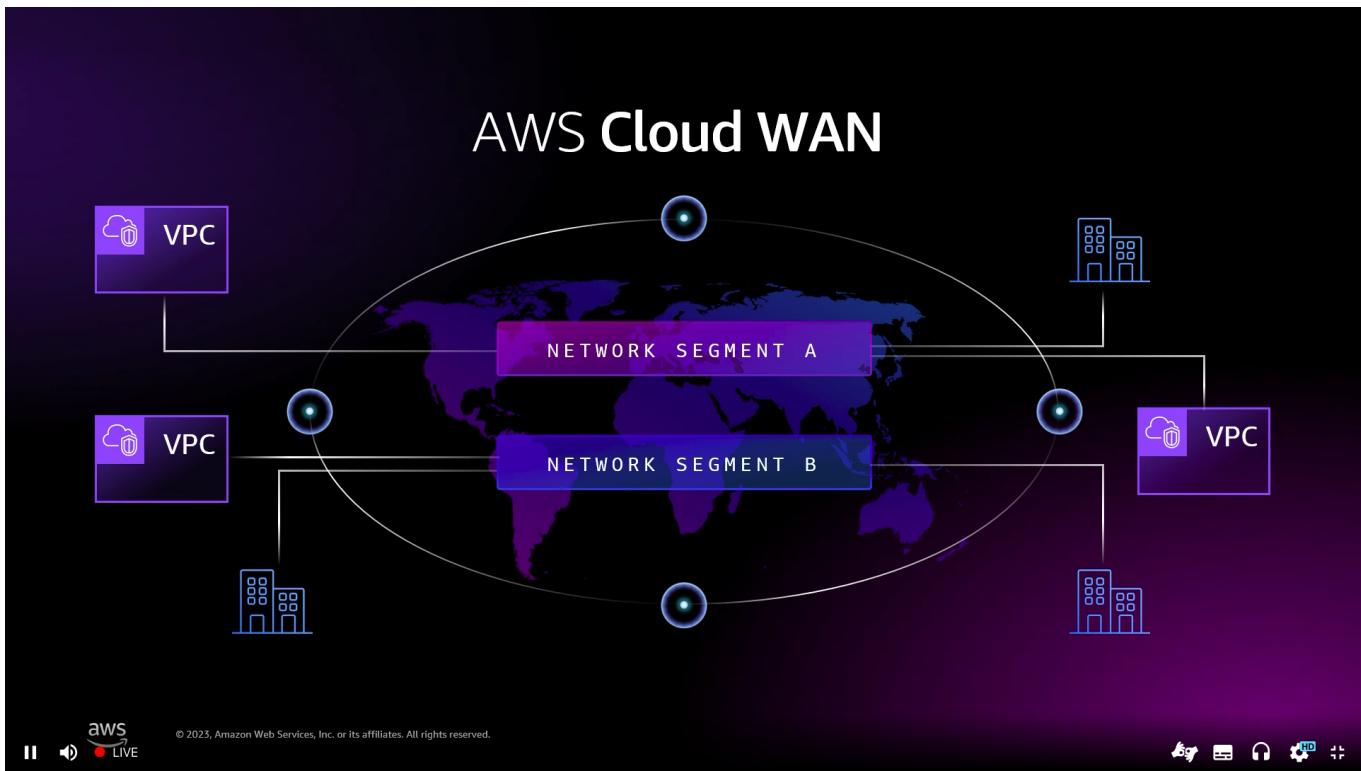
Design for the "primarily distributed world that we now live in."

Back to you Dave.

Best customer testimonial so far, less pump piece and more practical value based content.

Transit gateways Inter-region peering, but no....

AWS cloud WAN



Maybe talk more about Terraform and CloudFormation

AWS Cloud WAN tunnel-less Connect

Umm, lots of words, no GRE overhead

Native BGP support, cool cool

More interoperability is good, clap clap clap from me.

Back to IP address management

CIDR samurai, Tina Morris

This person has to be a badass, by definition.

Amazon VPC IPAM Enhancements

NEW

Amazon VPC IP Address Manager Enhancements

Automate IP assignments based on your unique networking and security needs

GENERALLY AVAILABLE



Automate subnet IP address assignment



Bring your own ASN (Autonomous System Number)



Get visibility into Public IP usage with Free Tier



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Autonomous System Number import!

Free tier for IPAM

Cool, groovy, useful.

IPV6 - The Future, obvi

IPV4 exhaustion

NEW

IPv6 Contiguous blocks and IPv6 Tiered VPCs and Subnets

NEW

Gateway Load Balancer and GWLB Endpoint support IPv6 traffic

NEW

AWS Global Accelerator IPv6 extends IPv6 support to Amazon EC2 endpoints

NEW

Amazon EBS direct APIs and IPv6

NEW

Primary IPv6 address

NEW

AWS Network Firewall and IPv6 only subnet support

NEW

Amazon Route 53 Resolver Endpoints now supports IPv6

 © 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IPV6 contiguous blocks, makes sense

Gateway Load Balancer Support

BYO Firewall

Tina Morris is probably a genius engineer

I've been saying IP address management was a problem for....yeah, they just spent 20 minutes on that.

Anyway, let's go v6! It's been a long wait.

ARPANet history lesson, Load Balancer history, yada yada

2007 is when David joined AWS, Elastic Load Balancing team in 2013.

The slide features a dark blue background with three circular icons on the left: a clock icon labeled 'AVAILABILITY', a shield icon, and a hand icon. To the right are two callout boxes. The top box is titled 'ZONE ISOLATION AND REDUNDANCY' and describes maintaining zonal isolation while providing redundancy across multiple Availability Zones. The bottom box is titled 'ANOMALY DETECTION AND MITIGATION' and describes gracefully handling target grey failures to improve application up time. The AWS logo and a 'LIVE' indicator are at the bottom left, and a set of control icons are at the bottom right.

AVAILABILITY

ZONE ISOLATION AND REDUNDANCY

Maintain zonal isolation of their application stacks while still providing redundancy across multiple Availability Zones

ANOMALY DETECTION AND MITIGATION

Gracefully handle target grey failures to improve application up time

The slide has a dark blue background with a 'NEW' badge. It features a large purple network graph on the right. The main text reads 'Anomaly detection with automatic target weight'. Below it, a subtitle says 'Detect and mitigate grey failures for Application Load Balancer Targets'. A 'GENERALLY AVAILABLE' badge is at the bottom left. The AWS logo and a 'LIVE' indicator are at the bottom left, and a set of control icons are at the bottom right.

NEW

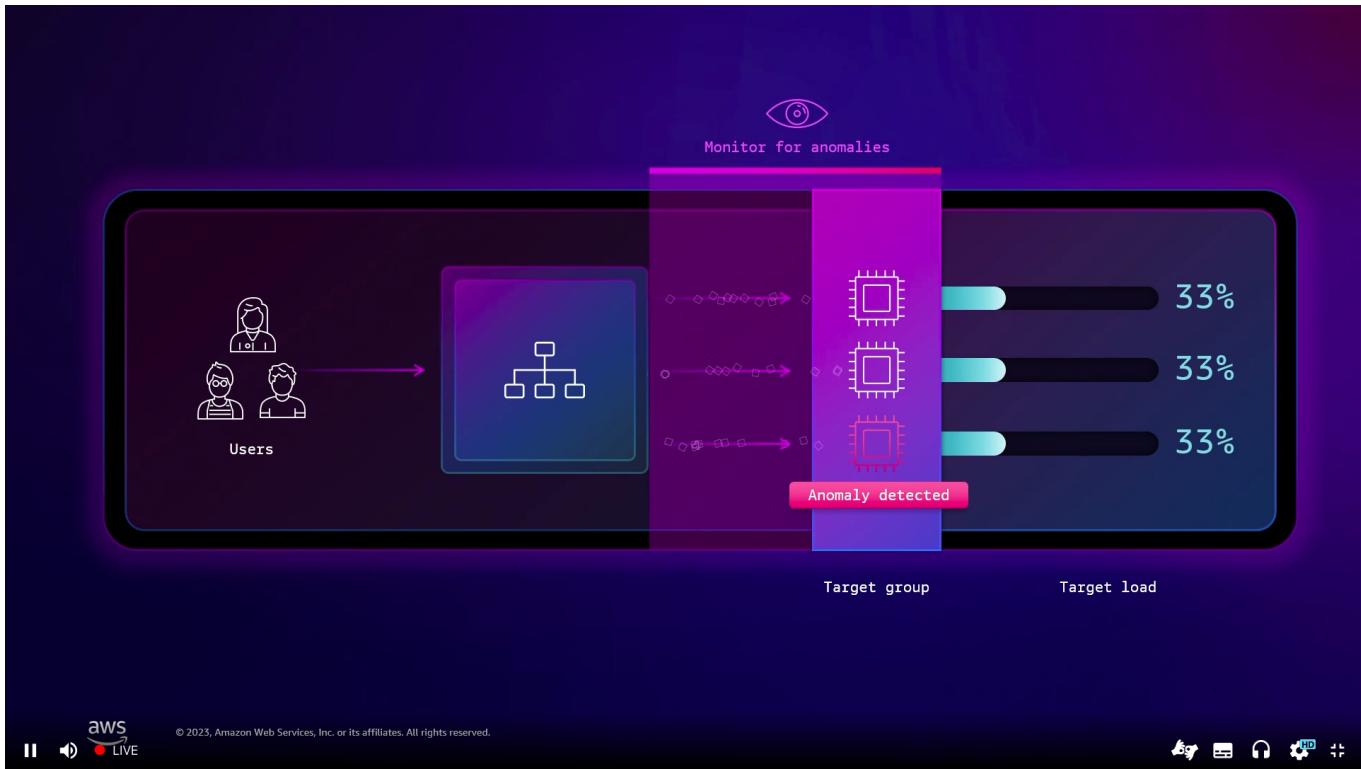
Anomaly detection with automatic target weight

Detect and mitigate grey failures for Application Load Balancer Targets

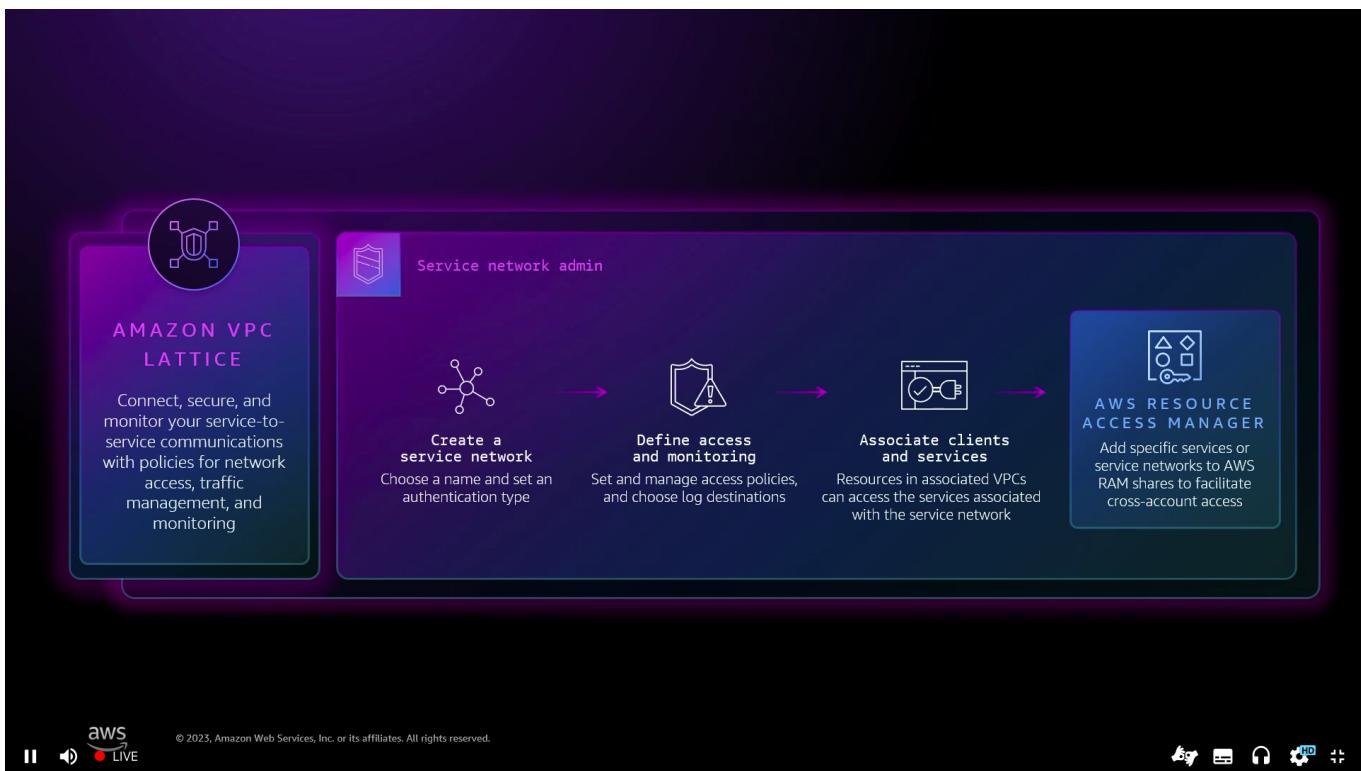
GENERALLY AVAILABLE

Anomaly detection with automatic target weight for grey failures in ALB Targets.

Generally available



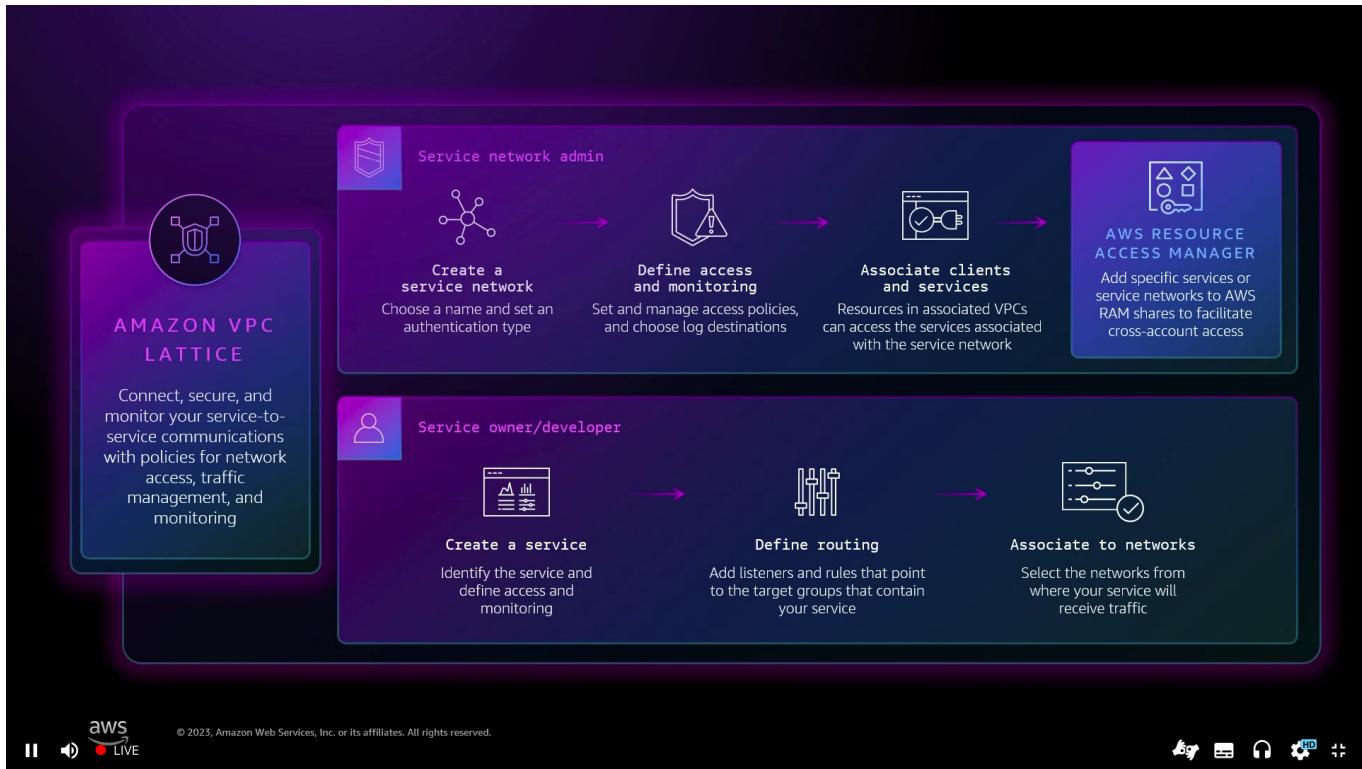
Automatically weights out the failed node.



What if we could abstract away the networking? See above. Mesh networking to the next level,

AWS VPC Lattice is generally available

Service network



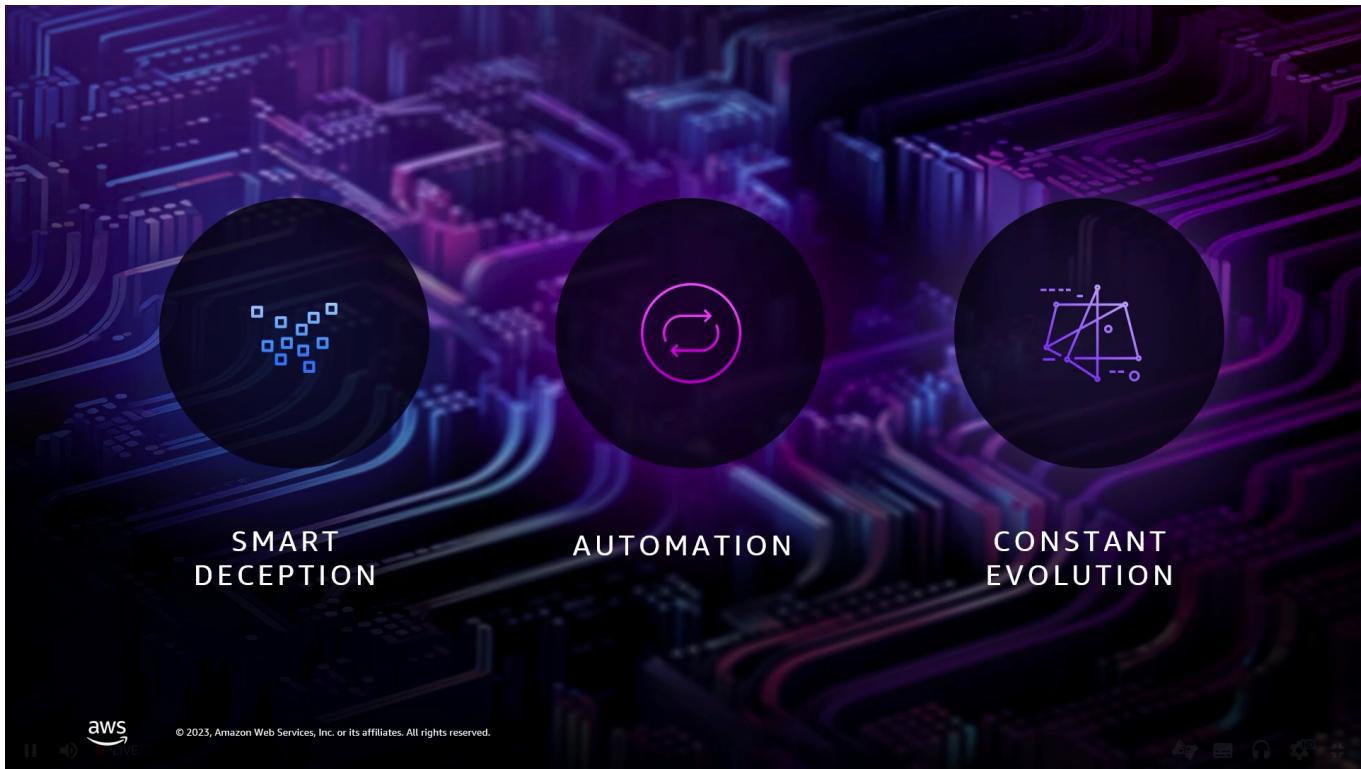
AWS Lattice is probably a sane way to do networking in a microservice-discovery environment. I like it.

Centuries of history including skytales

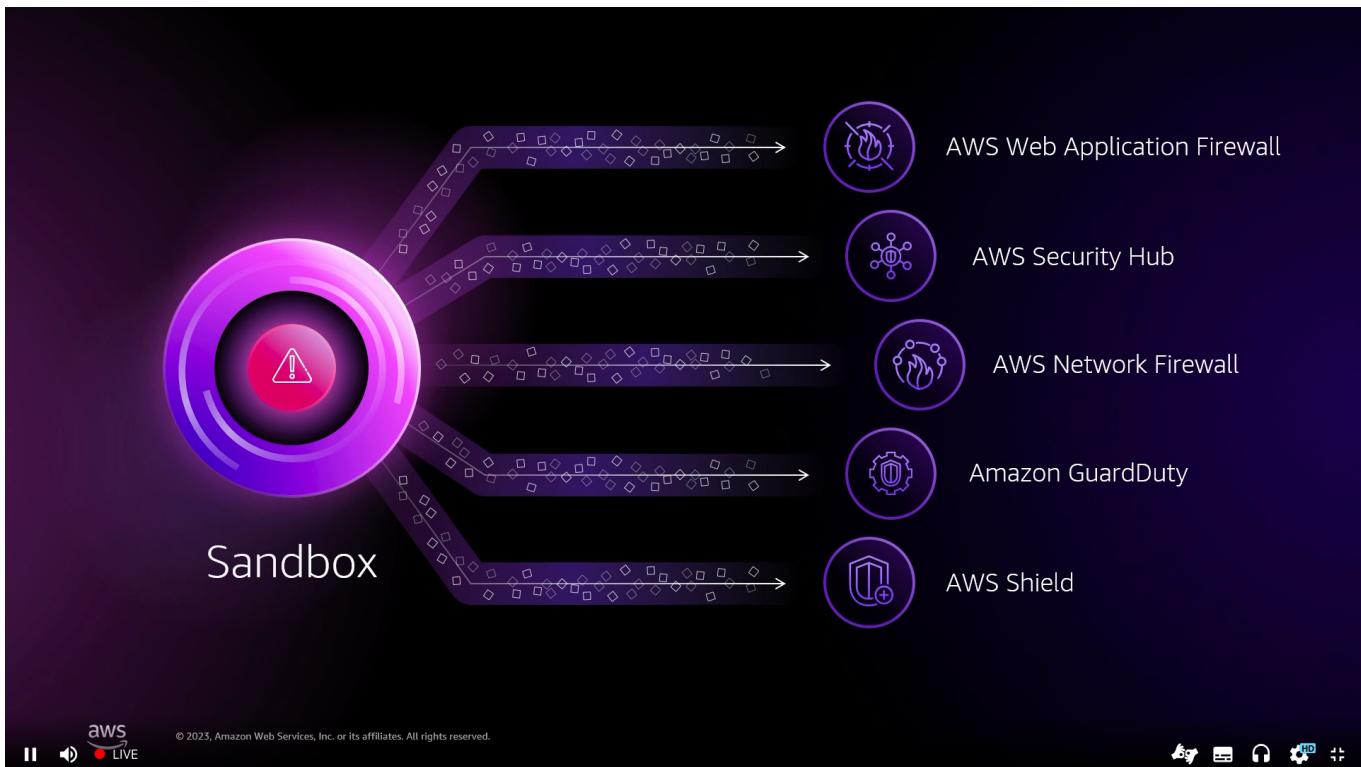
okay crypto, okay...yada yada crypto but pretending not to talk about crypto...skip skippity over this section into security....

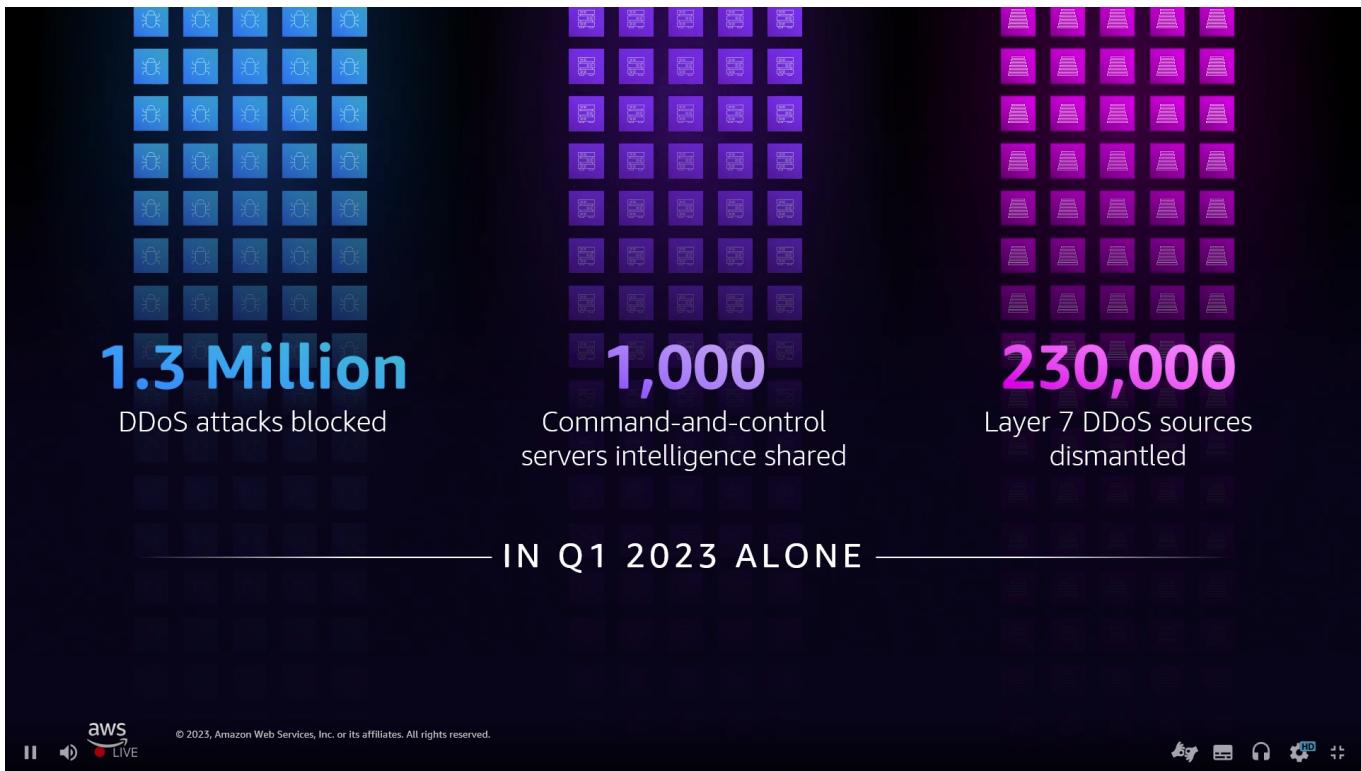
Cryptocurrencies are embarrassing, face it.

Oh, cyber-crime Project Mad Pot



How to get banned by AI, if you have bad luck.





MadPot is realtime threat disruption at scale.

Perimeter threat detection vs internal threat detection

NEW

New Features for AWS Network Firewall

Fully managed cloud-native firewall

GENERALLY AVAILABLE

- Decrypt and inspect TLS Connections
- Integrated with resource tagging
- Easy policy management via multiple administrators

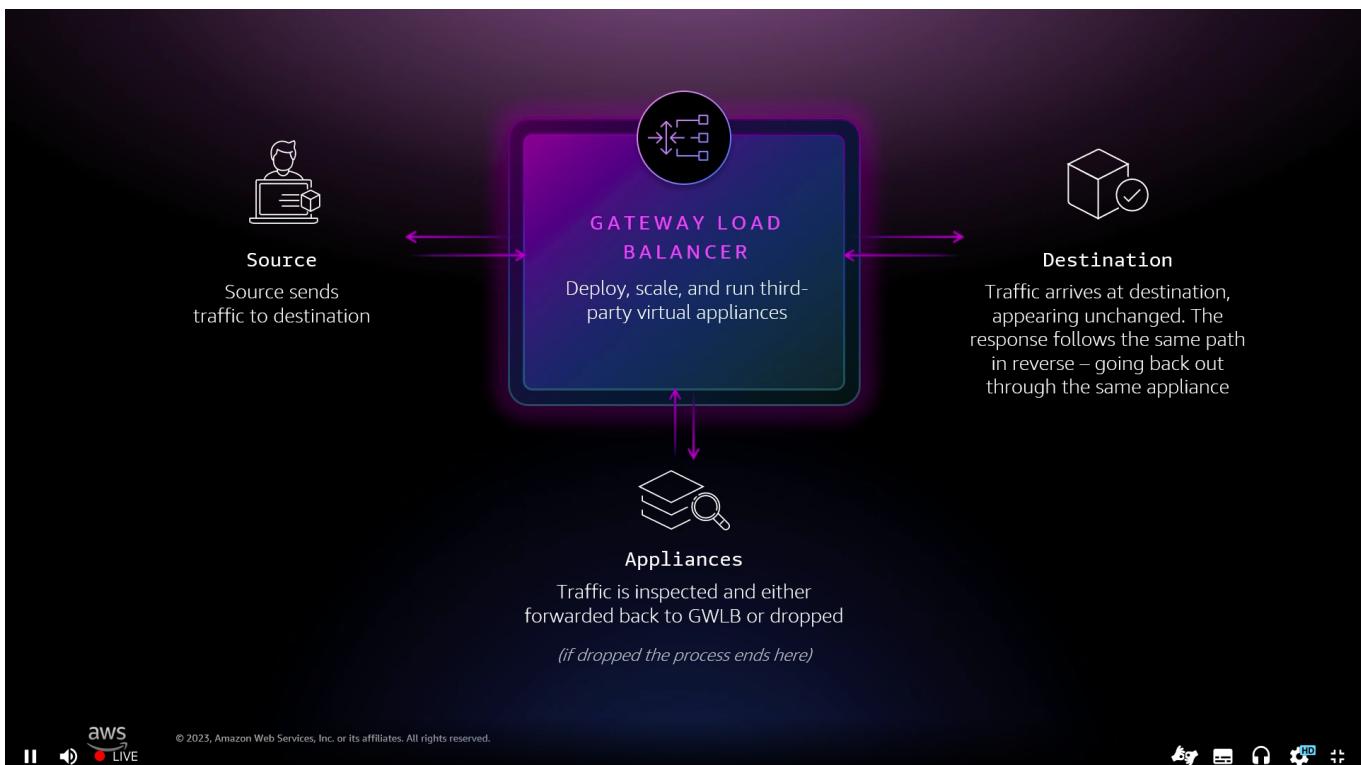
aws © 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Rules based firewall at the network level

Blast radius control

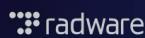


BYOF



Third-party security appliances

BROAD SET OF SECURITY APPLIANCES IN THE AWS MARKETPLACE



This is not a complete list. To view all AWS Partners for this category, visit [AWS Partner Solutions Finder](#).



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Zero Trust Computing



Users can securely access applications from anywhere



AWS VERIFIED ACCESS

Access to corporate applications without a VPN



Connect to trusted providers

Use your existing corporate identity and device management service



Express access policies

Create per application granular policies



Protect your applications using granular access policies

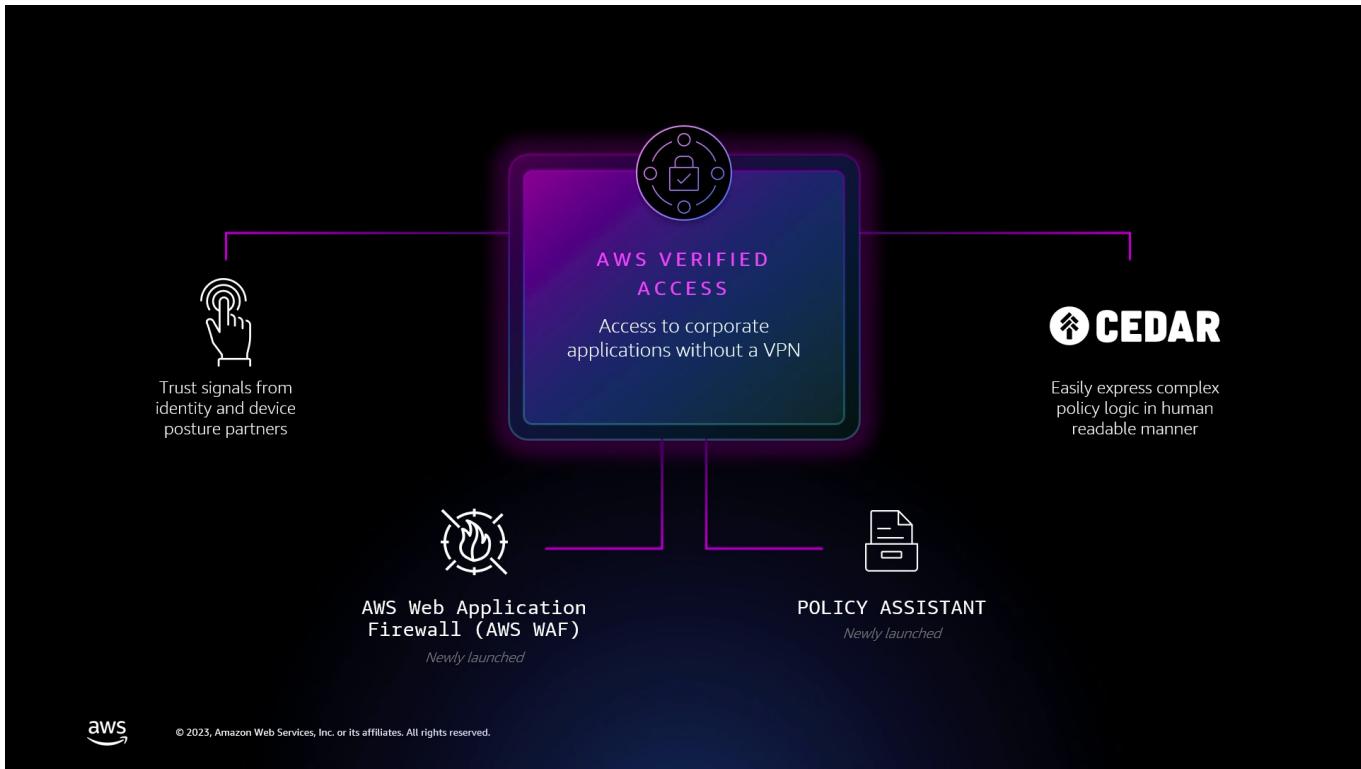


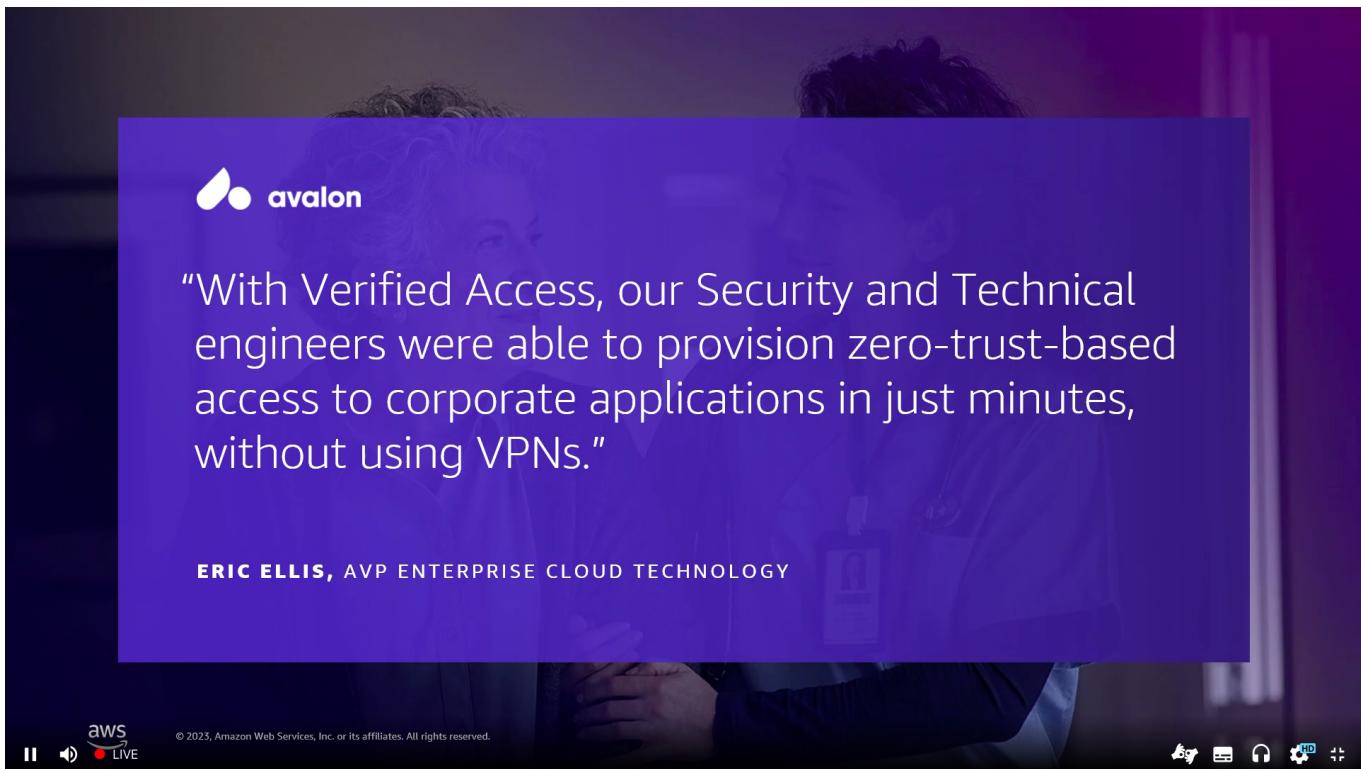
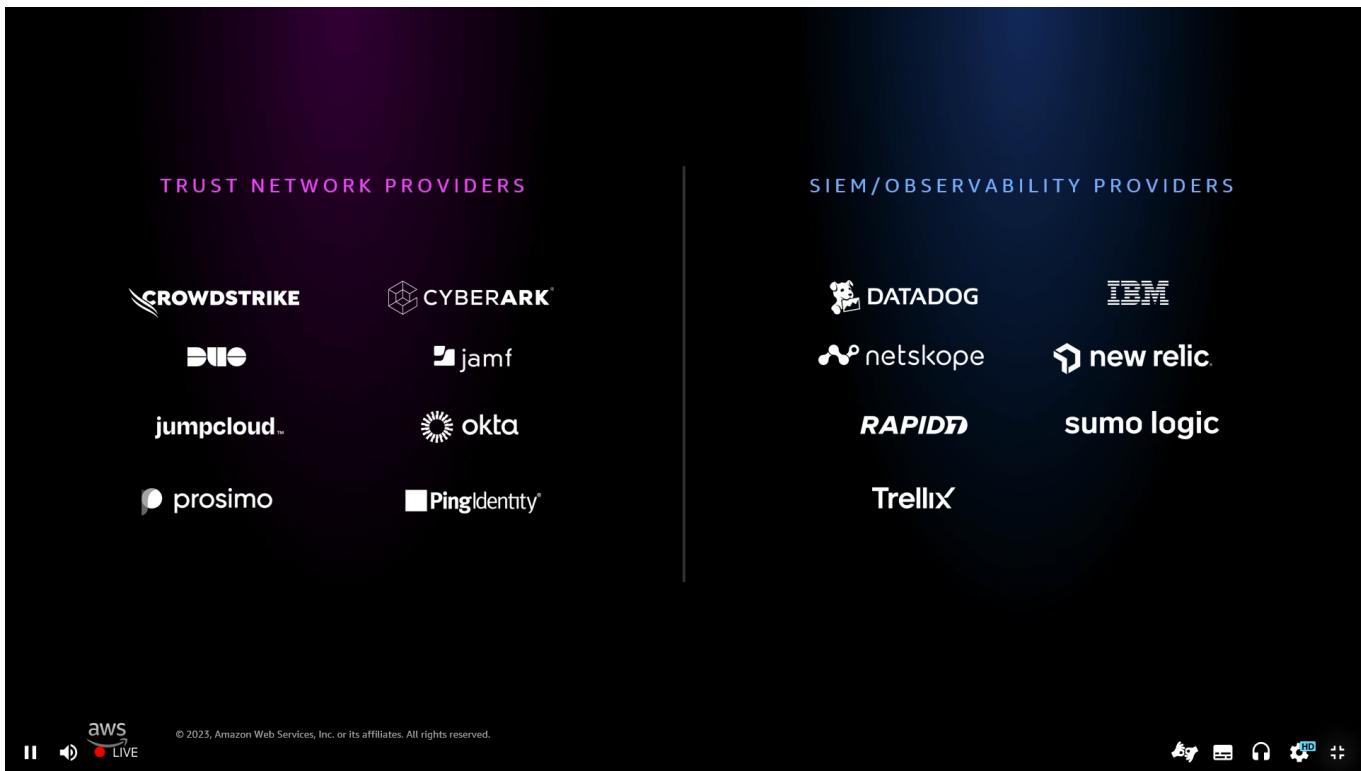
Analyze and audit security events using Verified Access logs



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Verified Access ^





recap

Printing press, load balancing, crypto, not sure what the through-thread is, but this was an information rich presentation that did not suck much, given how dry the material was.