AWS re:Invent

SEC329-S

# Zoom scales security capabilities with Splunk and AWS

**Richard Farley**
Chief Information Security Officer
Zoom

**Jordan Harris**
Regional Sales Manager
Splunk

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Agenda

The Data-to-Everything Platform

What Zoom needed

How Splunk helped

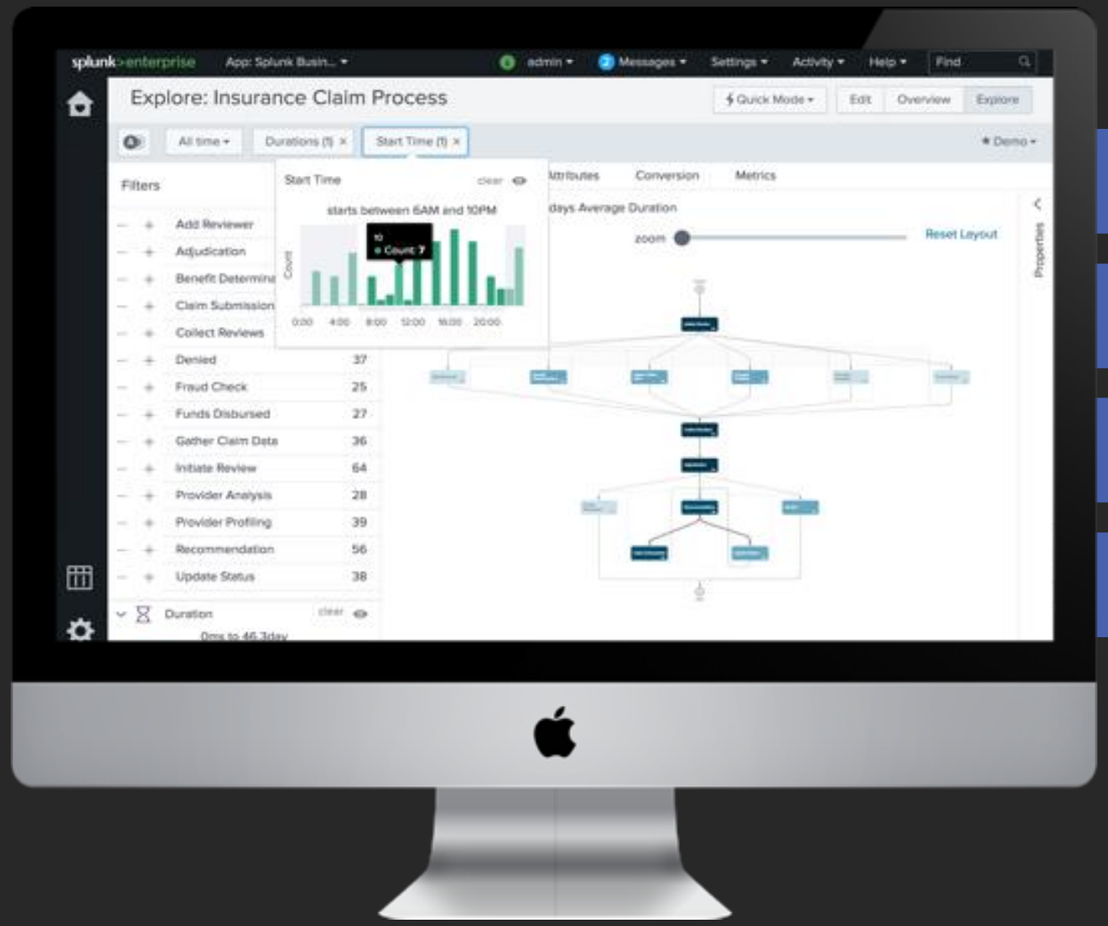
Securing the AWS environment

Scaling for the future

Key takeaways

splunk>

# TURN DATA INTO DOING




- Reduced downtime
- Continuous threat remediation
- Smarter production insight
- Application uptime

APP Custom applications

Web services

APM

Call detail records

Networks

Messaging

RFID

Firewall

Databases

Web clickstreams

Social media

GPS location

Servers

Smartphones and devices

Energy meters

Online shopping cart

Storage

Containers

Tracing

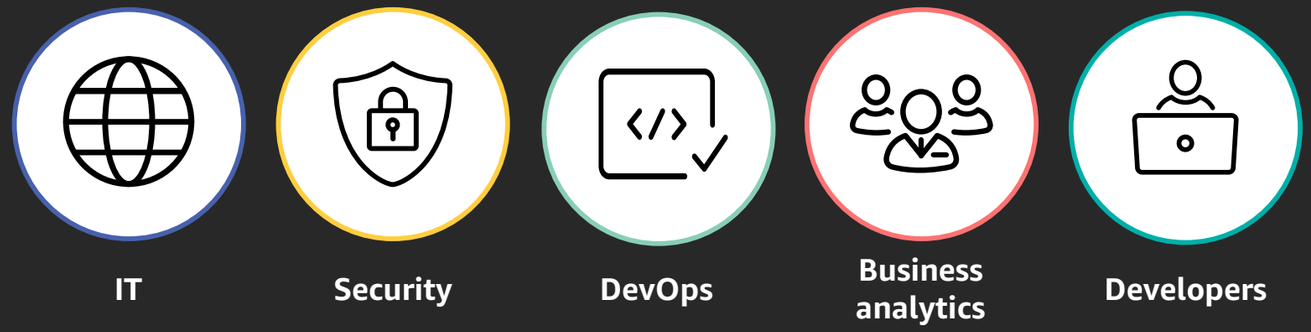
Online services

Security

Telecoms

splunk>

# Splunk delivers a holistic approach to turning data into business outcomes




Analyze with differentiated AI and ML

**Splunk Data-to-Everything Platform**

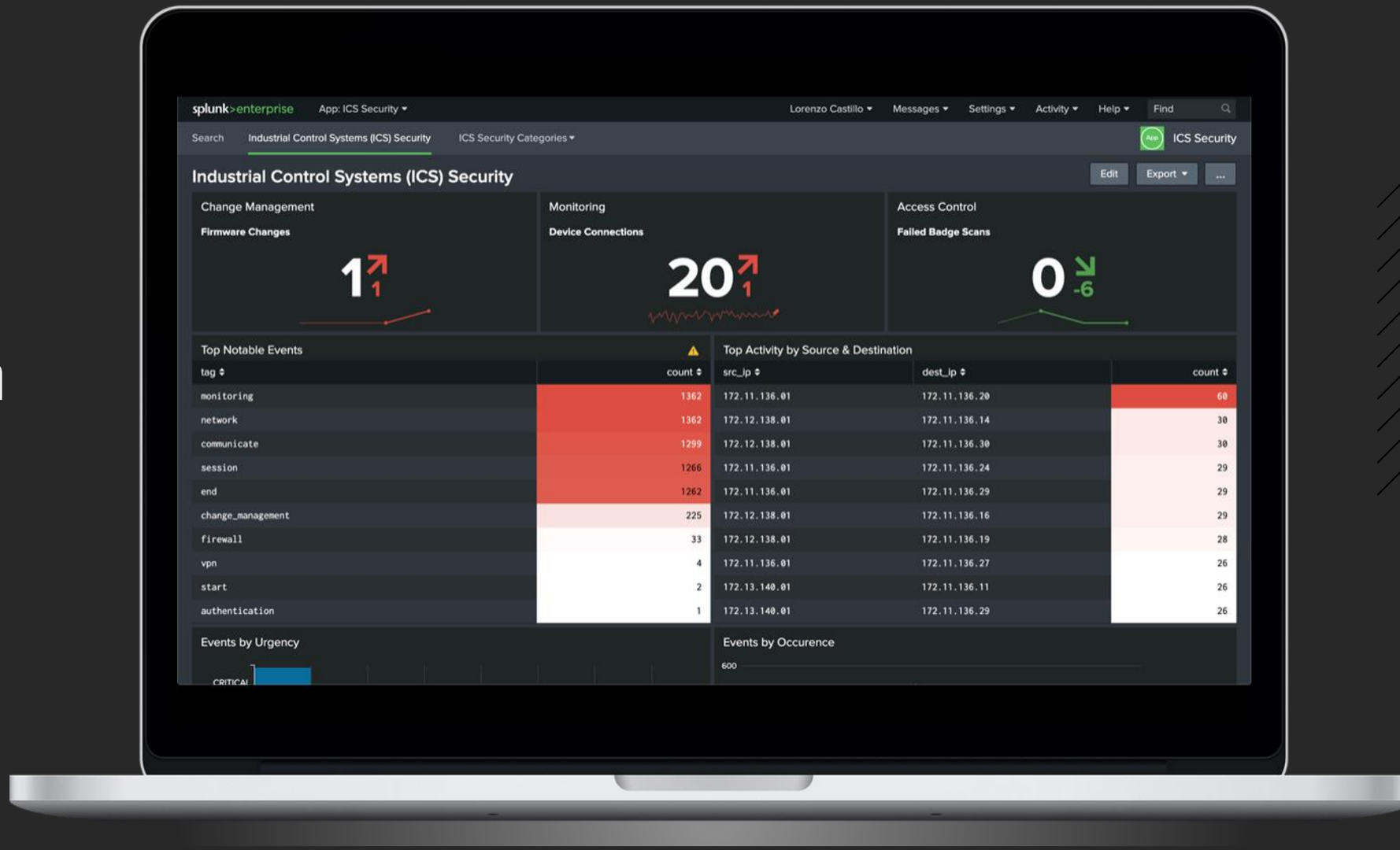
Investigate the expanding data universe

On premises

Cloud

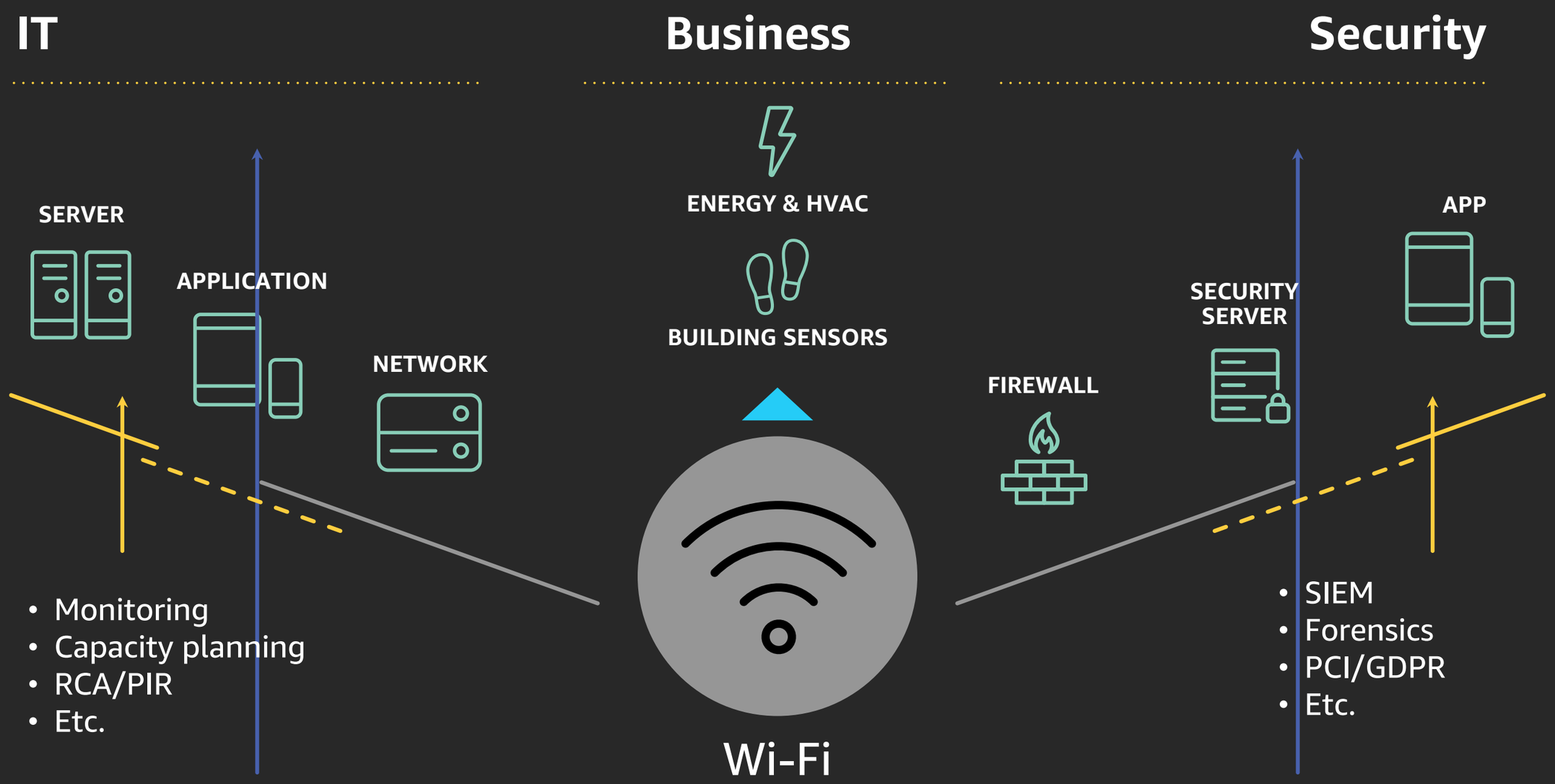
**Deployment options**

- Do you know what's happening?
- Can you turn data into action?
- How do you build for the future?



AMPLIFY

# YOUR DATA'S IMPACT




splunk>

# Splunk Enterprise and Splunk Cloud

## Deliver management at scale for a fully observable enterprise

### Expansive data access

Search,
Metrics and Events

### Faster, easier, more intuitive analytics

Analytics Workspace,
Connected Experience,
Natural Language Platform,
New Dashboards and Visualizations,
Machine Learning Toolkit

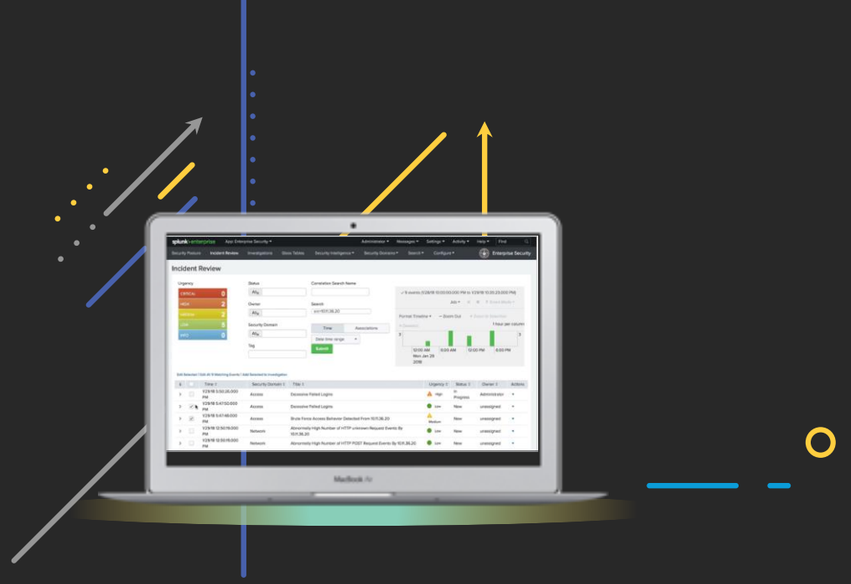
### Manageability at scale

Monitoring,
SmartStore,
Workload Management,
Security Access & Control,
Operator for Kubernetes,
Python 3.7 Migration

### Fast time to value with cloud

Features Immediately
Available on Splunk Cloud

splunk>




# Splunk at the Heart of Security

- Enhance threat visibility
- Accelerate incident response
- Scale your resources

# Security Use Cases

Security monitoring

Incident response & SOC automation

Advanced & insider threat detection

Compliance & data privacy

Fraud analytics & detection

Incident investigation & forensics

# DATA CHALLENGES OF THE FUTURE

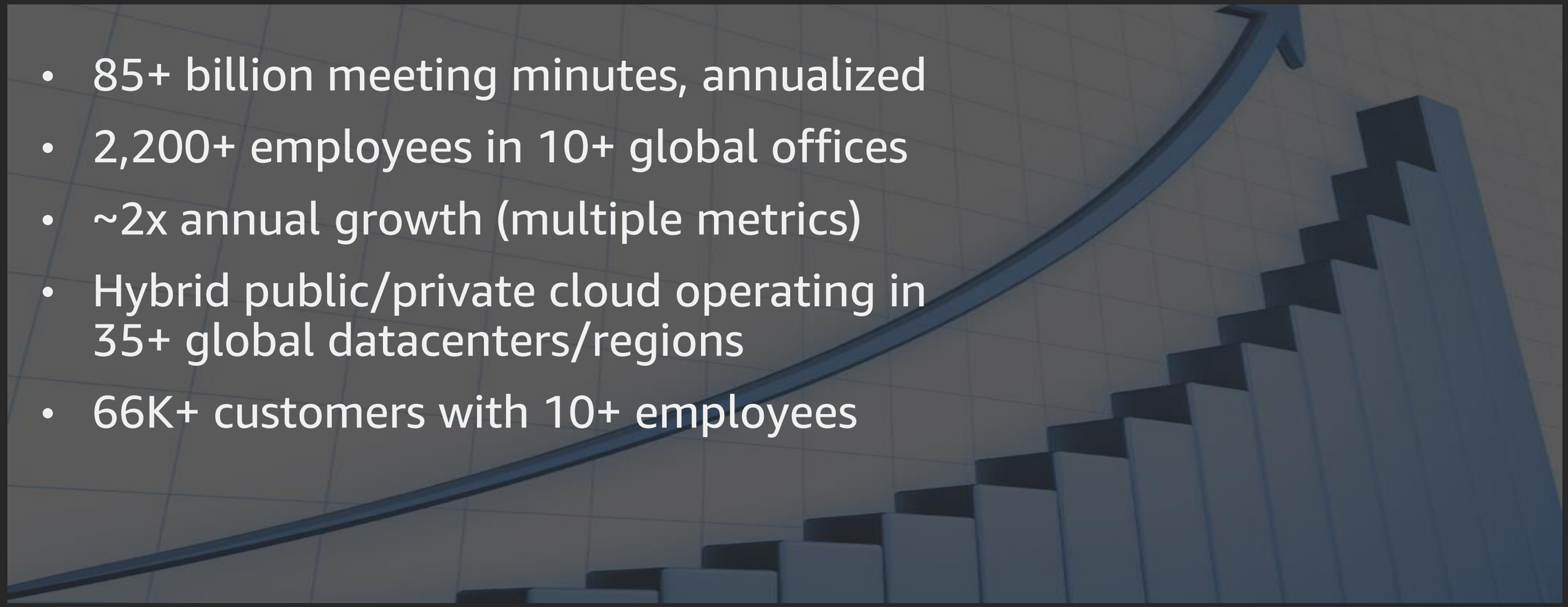
EMPOWERING
**DATA ACCESS**

ENABLING
**FASTER DECISIONS**

EMBRACING
**DATA WHERE IT LIVES**

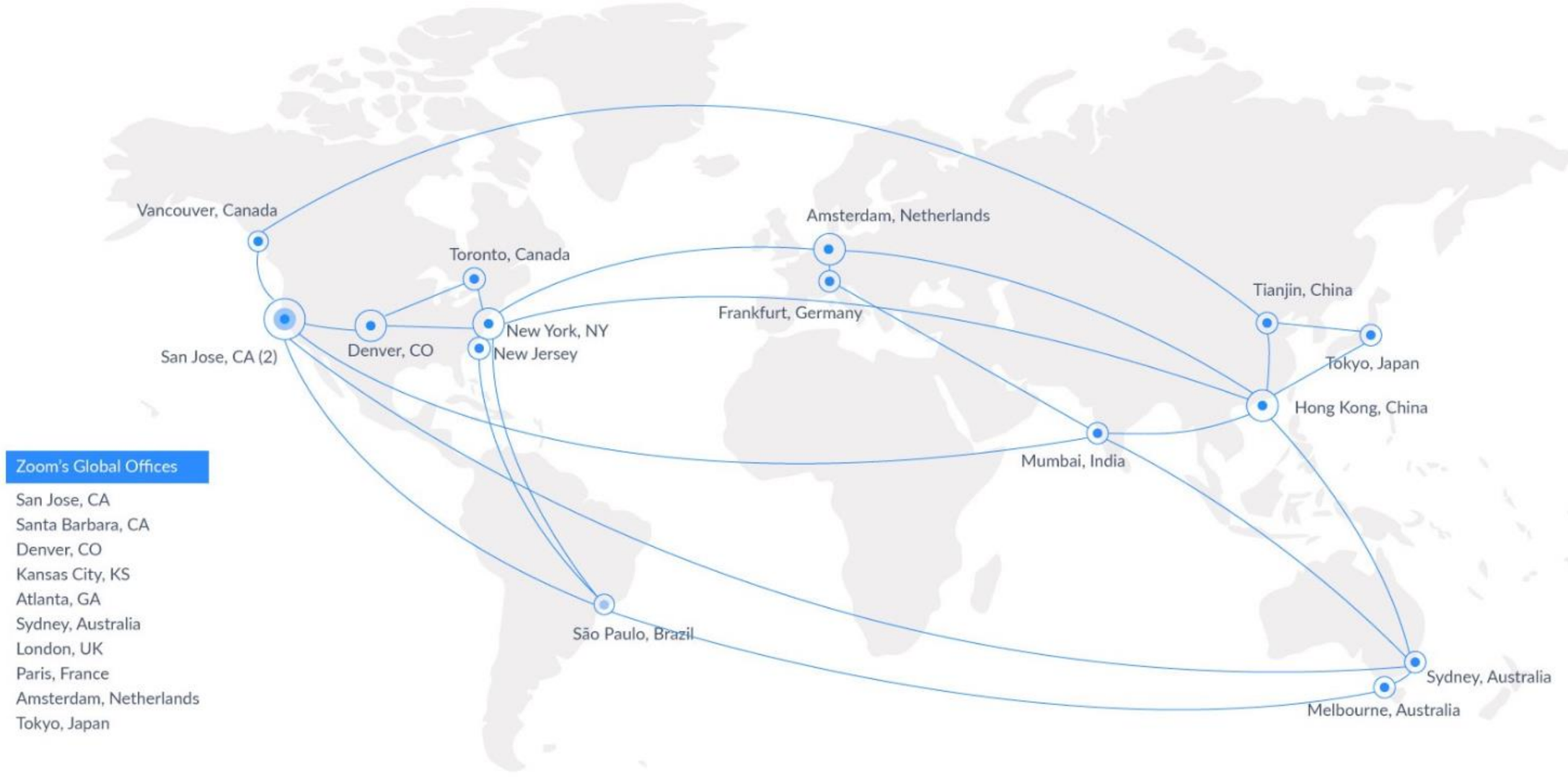
zoom

# Scale and growth



- 85+ billion meeting minutes, annualized
- 2,200+ employees in 10+ global offices
- ~2x annual growth (multiple metrics)
- Hybrid public/private cloud operating in 35+ global datacenters/regions
- 66K+ customers with 10+ employees

# Global datacenters & POPs – Performance and reliability



# 300+ products & significant features shipped in 12 months

## Zoom Phone

- Introduced Zoom Phone
- Upgrade Zoom Phone call to a meeting
- Suppress incoming calls while in a meeting
- Transfer to voicemail
- Automatic call recording
- Call delegation and shared lines
- Support 50+ phones
- Contact center and Salesforce integrations
- BYOC
- E911
- O365/Gmail contact integration
- VDI and Linux apps
- Dashboard reports on usage

## Zoom Rooms

- View in-meeting public chat
- Support for waiting room
- 1080p support for video sharing
- One-click to join third-party meetings
- Scheduling display: Reserve other rooms and view floor map
- Zoom Device Management (ZDM)
- Digital signage: Split screen and widgets
- People count
- Zoom Room use based on checked-in and released

## Meetings

- Virtual background without green screen
- Recording consent
- Video preview
- Capacity increase
- Default password for meeting
- Breakout rooms: Closed captioning and preassign rooms
- Audio watermarks
- Support for multiple pages on whiteboard
- Select a secondary audio device for ringer
- Audio coverage expansion (20+ dial-in countries, 16+ call-out countries)
- Sip connected audio
- Intelligent mute detection

## Chat

- Client UI redesign
- Star individual messages, contacts, and chat channels
- Alert when available
- Bot infrastructure

## Video Webinar

- Native HubSpot & Marketo integrations
- Post webinar survey
- Dial-in (phone-only) attendees can raise hand/allow to talk

## App Marketplace /Integrations

- Introduced App Marketplace
- 150+ apps & bots
- Google calendar add-on
- MS teams
- Slack
- OneDrive
- Dropbox
- Salesforce
- Atlassian
- Cornerstone
- Calendly
- New APIs and SDKs

# Security & compliance

SOC 2
(Type II)
Trust Services Principles

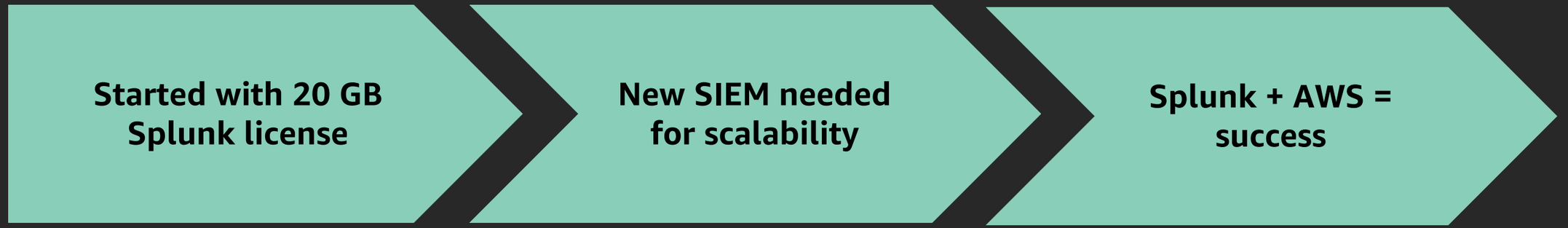
FedRAMP
(Moderate)

Federal Risk and Authorization Management Program View Certificate

EU/US Privacy Shield
Swiss/US Privacy Shield
Data Privacy Practices

Certified Privacy Practices and Statements

# What did Zoom need?




Zoom needed a tool that could help scale with the demands of the business while protecting the SOC

Migrating to AWS for the SOC allowed better scalability and monitoring

# Scaling with AWS

**Flexibility**

- Going to the cloud scales, flexibility
- Saw value in having ability to run Splunk in a separate VPC on AWS outside physical datacenters
- Large portion of logs run on AWS, so scaling to AWS made sense

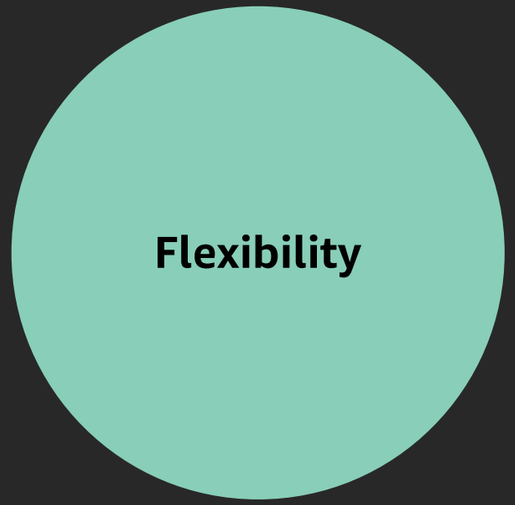
**Global data consumption**

- Co-located datacenters (15–16) to connect anywhere – mobile, desktop, etc.
- Datacenters all over the world, need to get data from the datacenters quickly, so AWS made the most sense
- Amazon CloudWatch Logs and all AWS service logs and application logs
- Amazon S3 buckets for video

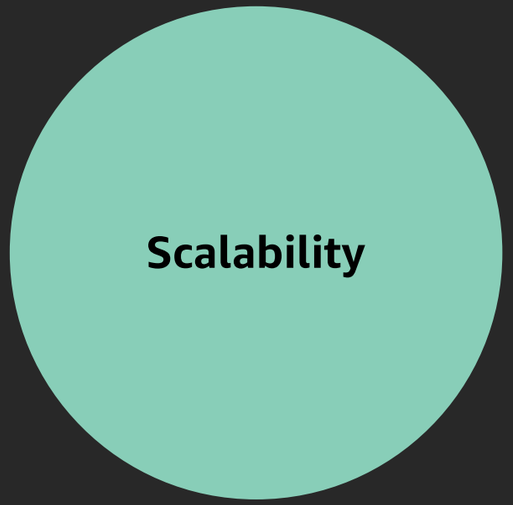
**Secure environment**

- Separating security infrastructure from the rest of the infrastructure, which works for some companies that are higher potential targets for compromised activities

# Securing environment with Splunk




- Scalability and flexible deployment model
- Capabilities with integrating with existing systems: Ticketing, CMBB




- Splunk implementation is for SOC processes, gathering point for all security instrumentation to correlate events from various points of infrastructure

- Splunk is a leader in security
- Detect threats before they happen
- Visibility into all applications ingesting data into Splunk

# By the numbers

## 100%

- Zoom is 100% cloud for IT – don’t run IT applications in datacenters
- Firewall and IDS and antivirus monitoring; endpoint protection, SSO data

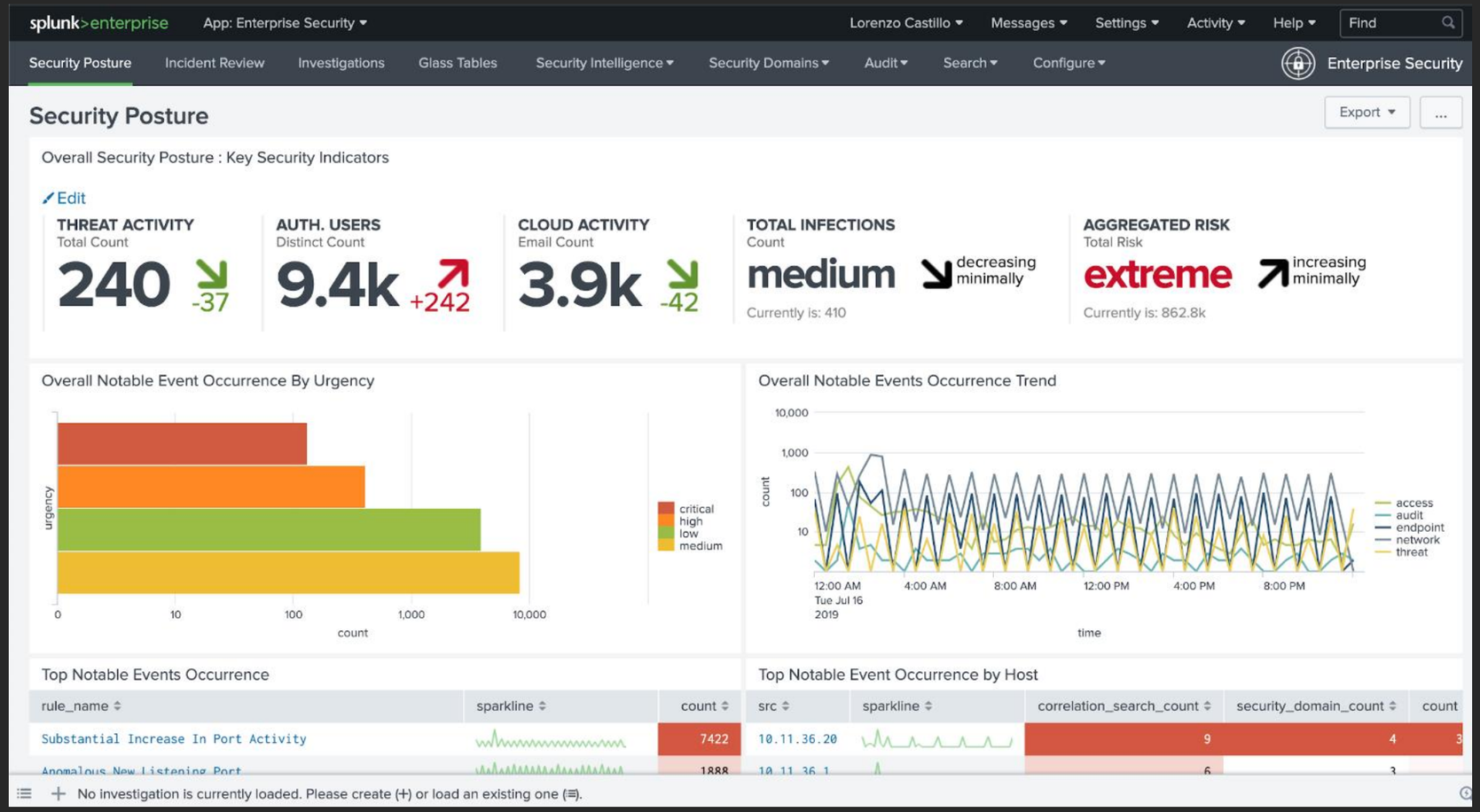
## 500+ GB

- 500 GB/day of data because of Zoom growth rate
- Splunk driving SecOps for Zoom service (SaaS) and corporate IT infrastructure

## 30–40

- Number of data sources ingested on an average day
- Ingesting AWS services, applications within AWS, systems/servers outside AWS logs

# Securing AWS environment



# Tl;dr

## THE PROBLEM

- Zoom is high-scale and rapid growth, leveraging AWS and co-located datacenters
- Needed a tool and infrastructure that could support and scale with Zoom’s growth

## THE SOLUTION

- Deployed and implemented Splunk in the cloud as the preferred tool for aggregating security information and events to provide visibility and predictability
- Leveraging Splunk to drive SOC processes for identifying, detecting, responding to, and recovering from security incidents

## THE HOW

- Leveraged AWS Marketplace for efficient procurement process
- Opted into AWS ISV Workload Migration Program for infrastructure cost coverage

"With Splunk, we were able to eliminate blind spots in a cost-efficient manner and predict threats before they happened."

**—Richard Farley**

Chief Information Security Officer,
Zoom Communications, Inc.

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

# Key takeaways

- Consider **separating out your security infrastructure** from the rest of your infrastructure
- Leverage single pane of glass tools, such as Splunk, to help SOC team stay productive
- Don’t just think about how you protect your environment **now**, think about **how to scale for the future, and invest in a tool and infrastructure that can scale for the future**
- Customer data protection is not just a security team priority, it’s **everyone’s priority**

# Join us at Topgolf tonight!

Don’t forget your AWS re:Invent badge for entry

**When?**

December 4, 2019

7:30PM – 10:30PM

**Where?**

**Topgolf Las Vegas**

4627 Koval Ln

Las Vegas, NV 89109

# Thank you!

**Visit Splunk**

Booth #3003

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Please complete the session survey in the mobile app.

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.