



## AI/ML and the future of Cybersecurity

Prepared for CS4HS

24th November, 2022

Patrick Sullivan, Google NZ





10 min

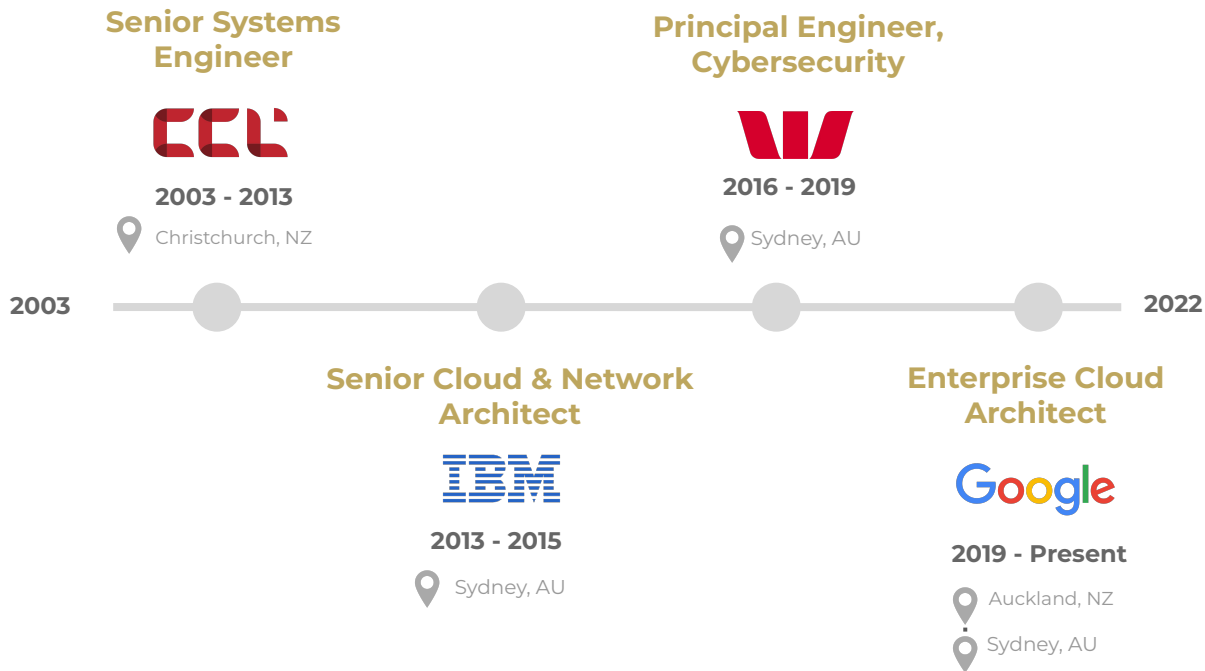
Intros

1

# A bit about me and my background



**Patrick Sullivan**  
Enterprise Cloud Architect  
Google Cloud  
Auckland, NZ



## In your own words

- Name, role and background
- Level of familiarity with Cloud & Cybersecurity
- One thing (or more) you're hoping to get out of today.





# Agenda

1

Intros

2

What is 'Cloud' anyway and why does it matter?

3

Google's security journey (we got hacked and it was a good thing)

2

Some AI fun to get us started!

5

Gamifying cybersecurity as a way of learning

6

The future of cybersecurity skills & career pathways



10 min

What is Cloud anyway and why does it matter?

2

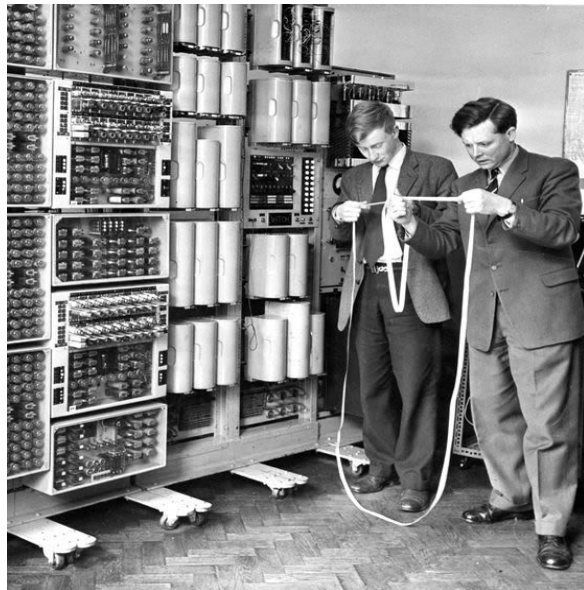
**Two examples of the old way of doing things:**

- 1. Infrastructure**
- 2. Security**

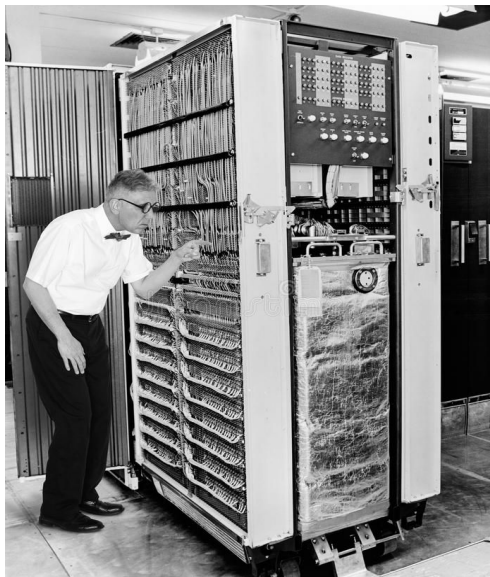
What's the first thing that comes to mind when you hear the word  
**Infrastructure**?



In the world of technology, we generally think of servers and mainframes as being **infrastructure**.



1950's



1970's



1990's

They **store and process data** (websites, cat videos etc)

Hewlett Packard  
ML350 Server



Back in 2011, 85% of all Christchurch businesses ran on servers, **usually hidden in a broom closet somewhere**, in their office.

Christchurch, Feb 22 2011 12:51pm





Immediately after the earthquake, businesses were **no longer allowed to access their offices**, power was out all across the city.

**In many parts of the city it wasn't restored. They lost access to all their data, HR systems, email, files, docs company software, inventories, products, balance sheets, accounting systems...**

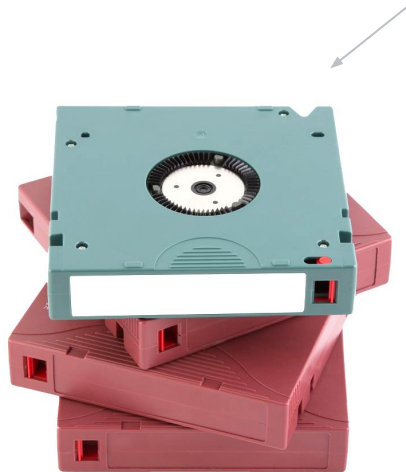
**Everything**



They **weren't allowed back in** until the buildings were deemed safe by civil engineers. This was taking many months in some cases.

For many, the only piece of their business they had left were **backup tapes like these**, with copies of their data on it.

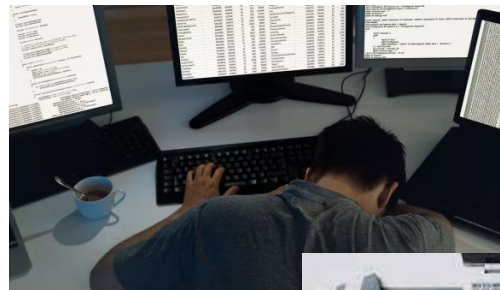
Backup Tapes



**Where I worked at CCL, our datacenter was one of the last surviving in the city. We had big servers and lots of available capacity.**



We spent the next 3-4 months working 80 hour weeks, restoring 100's of Canterbury businesses from backup tapes into our data center. It's a **painstaking, complex, error-prone** process

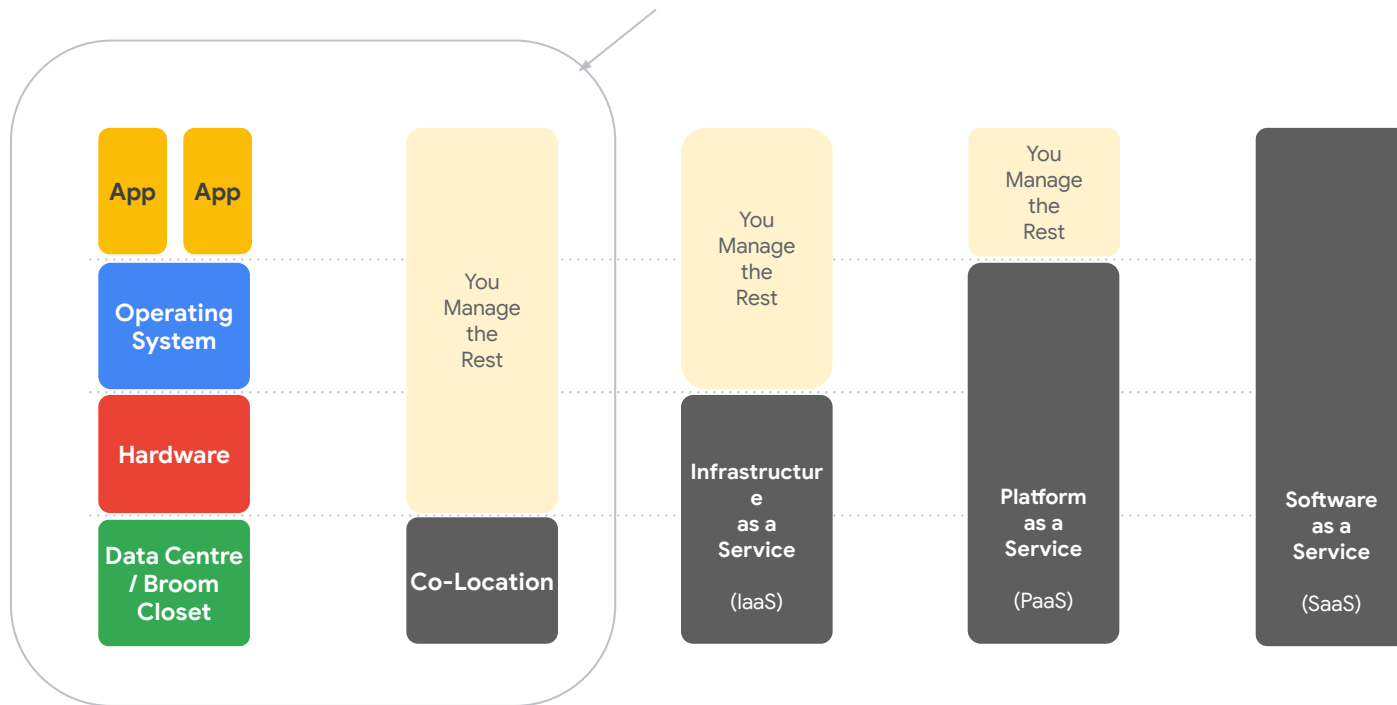


**This would not have happened if those customers were using Cloud**

# Enter the Cloud era!

Proprietary + Confidential

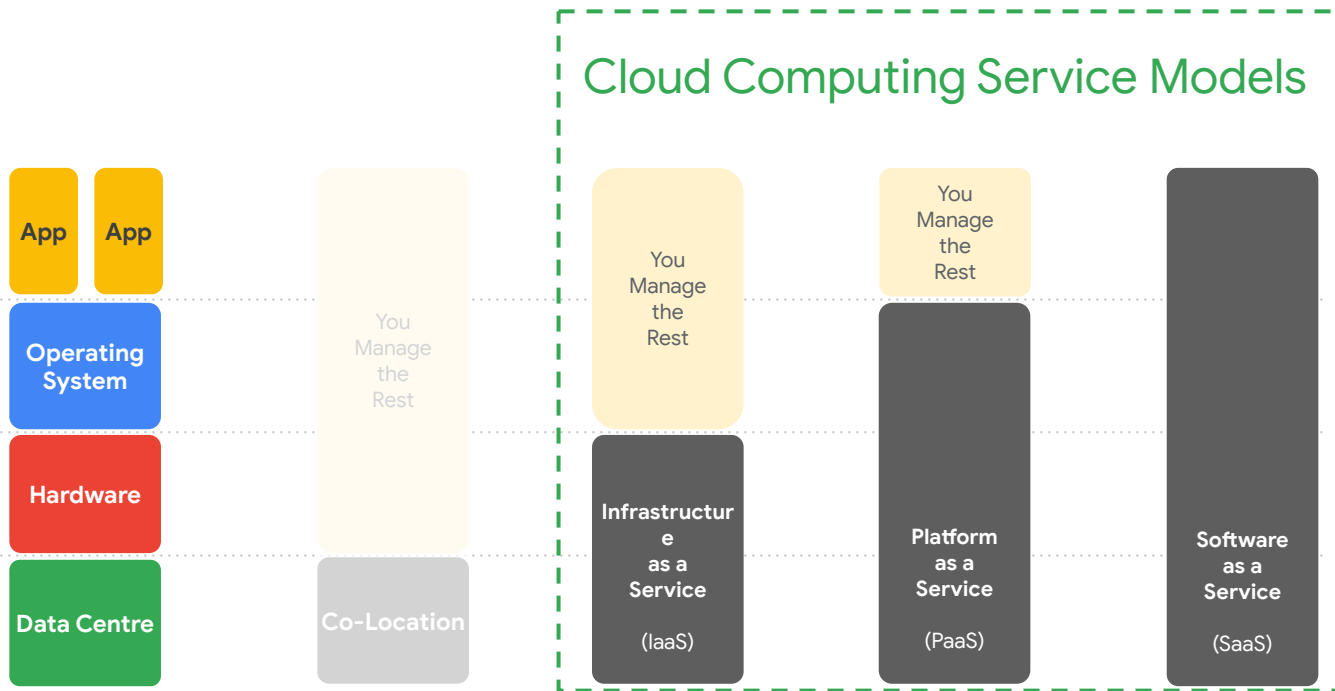
Christchurch, 2011





# What is considered “cloud computing”?


Proprietary + Confidential



Most people know Google for this, our ability to search entire world's information in 400ms and deliver the **cat video** you're really after.



🔍



Google Search

I'm Feeling Lucky

The background of the image is a perspective view of a server room aisle. On both sides of the aisle are tall server racks filled with hardware. Numerous small, bright lights in yellow, blue, and green are visible on the server units, creating a sense of activity and depth. The perspective leads the eye down the center of the aisle towards the vanishing point.

# Google



Google Search

I'm Feeling Lucky

What they may not realise, is we've built the largest global infrastructure platform in the world, and it's all around the world.

# Google Cloud Platform

34

REGIONS

103

ZONES

173

NETWORK EDGE LOCATIONS

AVAILABLE IN  
200+

COUNTRIES AND TERRITORIES

COMING SOON! Google Cloud will continue expanding into the following regions: Doha (Qatar), Turin (Italy), Berlin (Germany), Dammam (Kingdom of Saudi Arabia), Tel Aviv (Israel), Mexico, Malaysia, Thailand and New Zealand.



Current region  
with 3 zones



Future region  
with 3 zones



Edge point  
of presence

— Network

## Regions, PoPs, and network

Google Cloud

If those Christchurch businesses were using Cloud, they would have been up and **running again within minutes**, from another Google data center

**Two examples of the old way of doing things:**

**1. Infrastructure**

**2. Security**



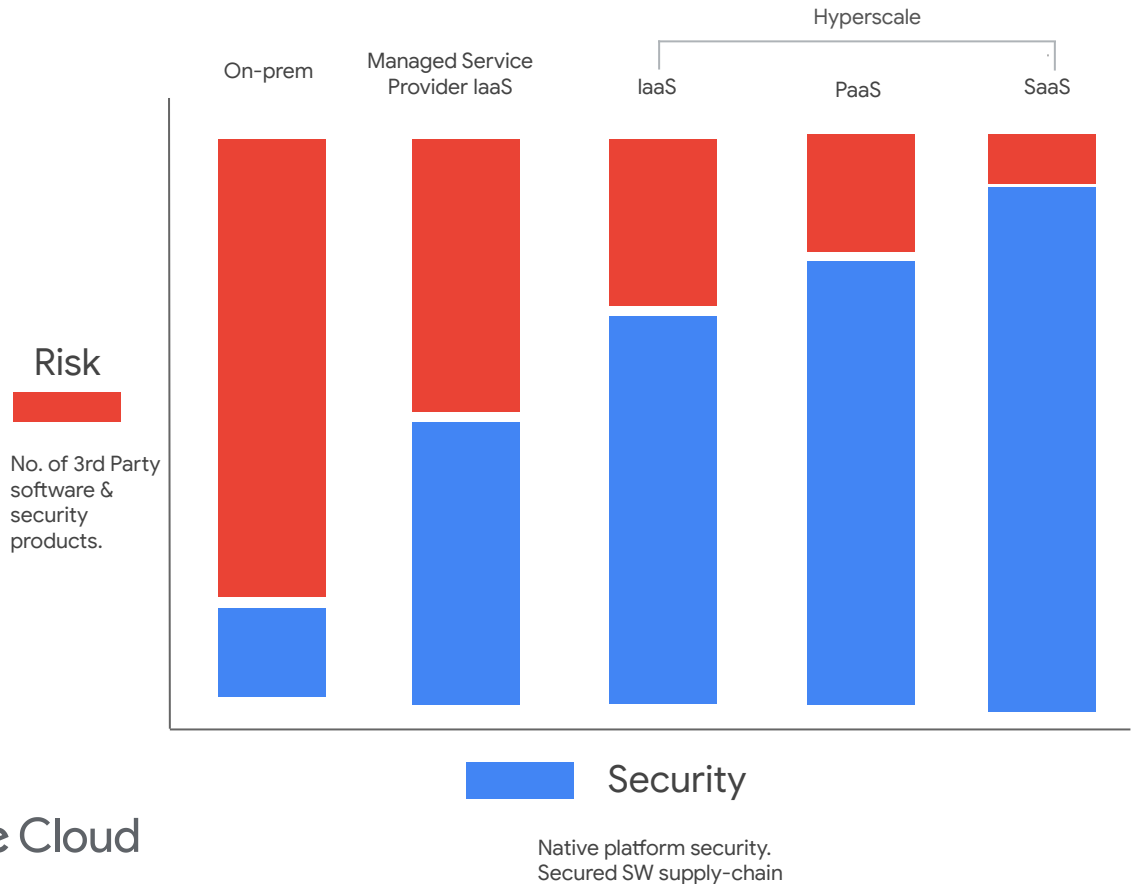
# How most large organisations approach security, lots and lots of products.



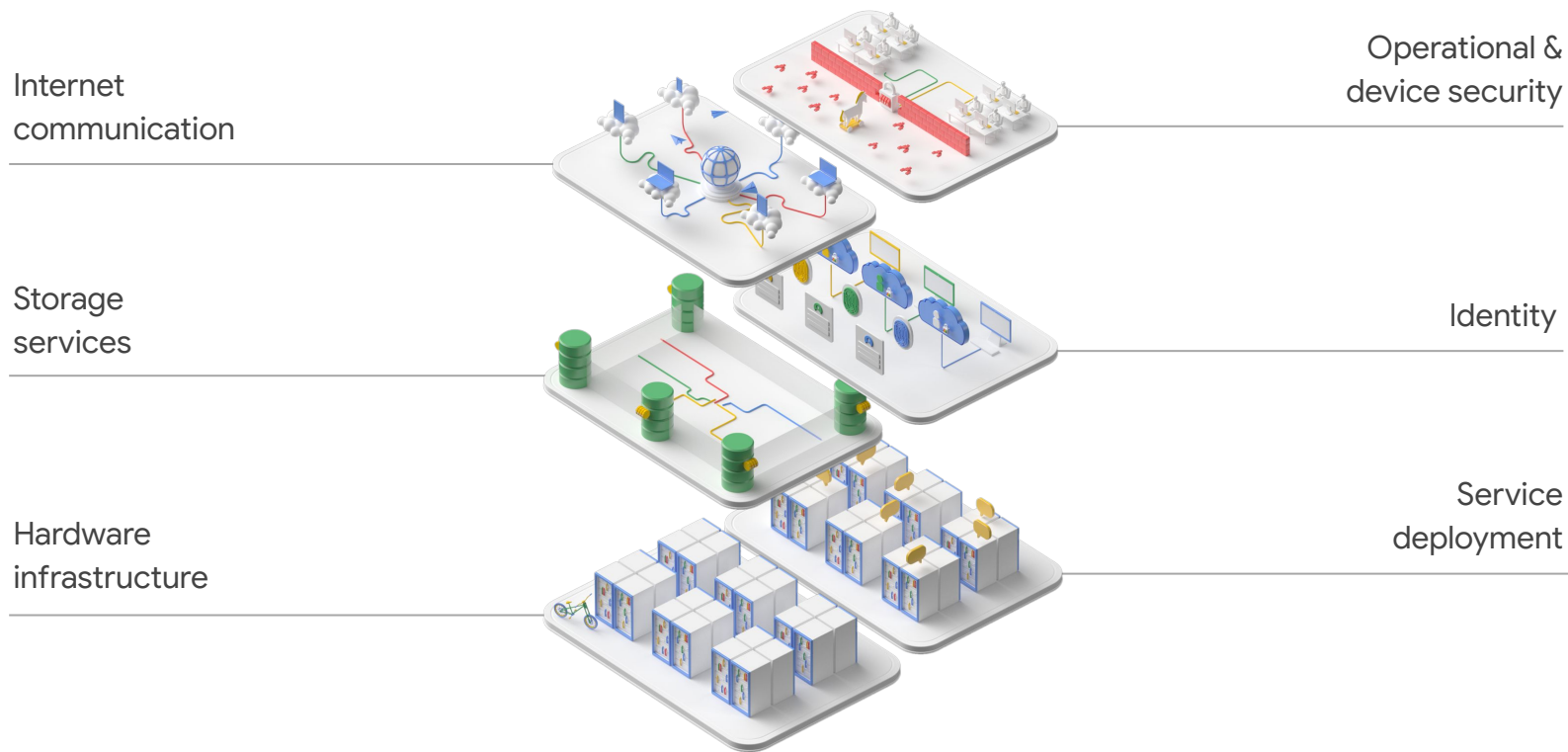
**Complexity is the enemy of security**



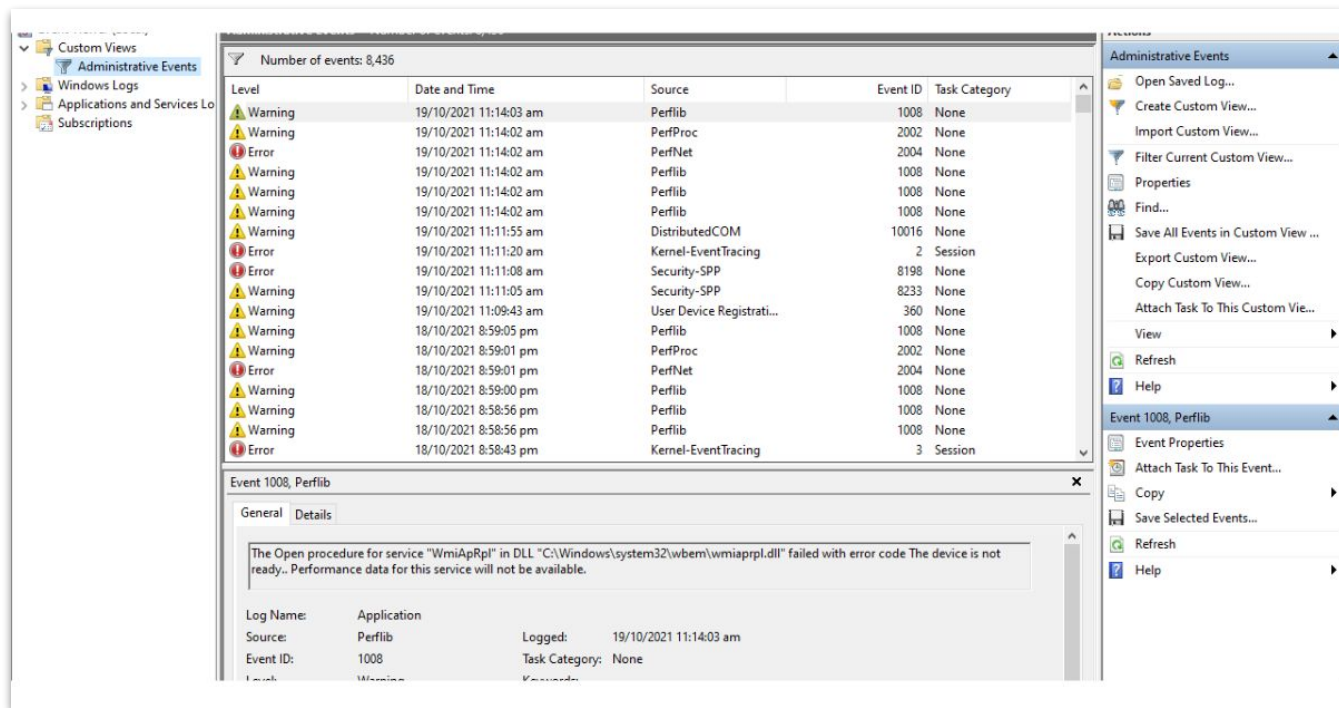
# Risk profiles of various computing models



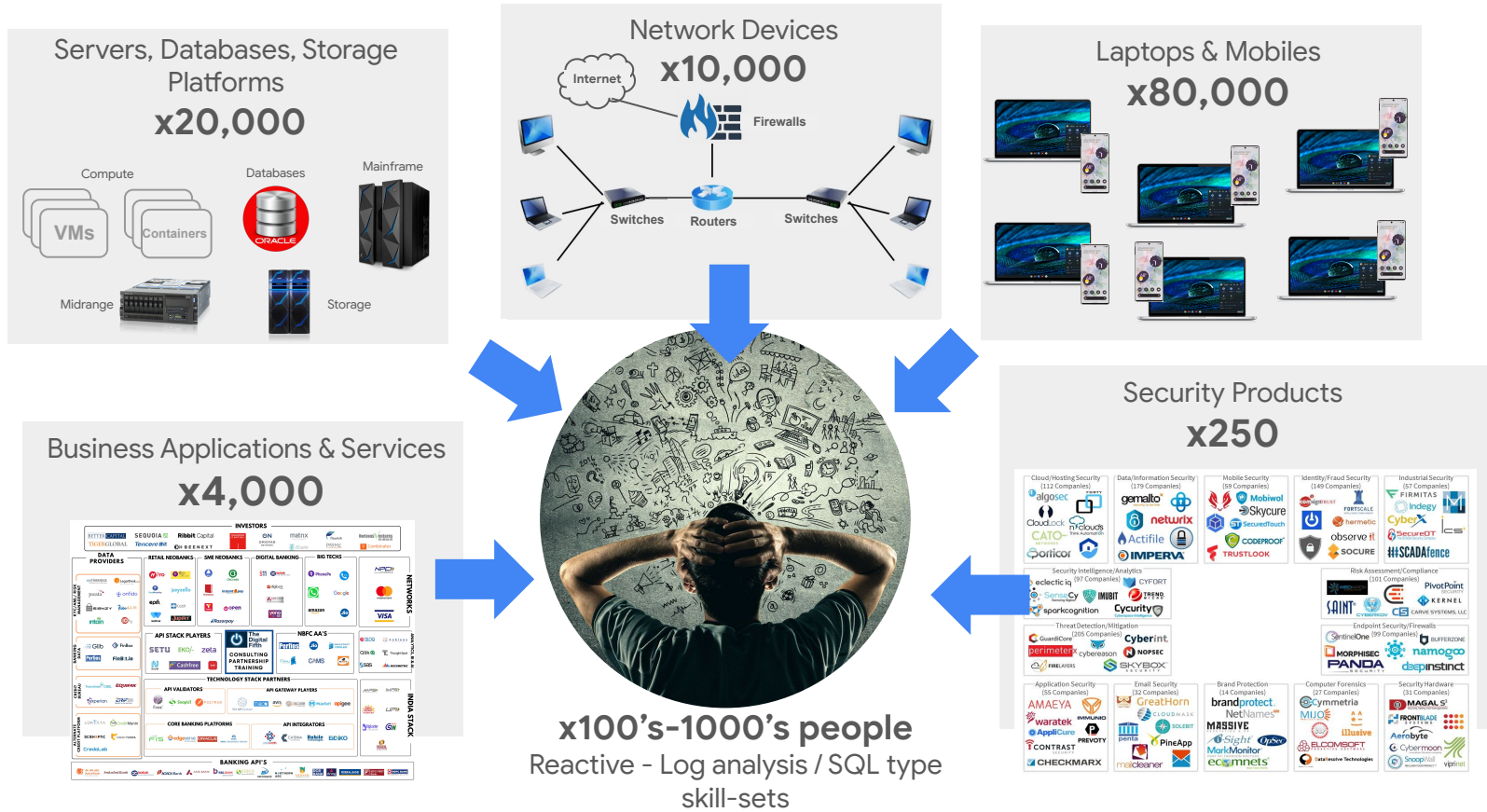
# At Google, we build the whole stack ourselves, including the security parts



**Your laptop produces 1000's of events every day. These need to be analysed by Security Operations Centers to find security problems.**



Combined with 10,000 other employees, applications, servers, network devices, the scale of the data problem is immense.



The average SOC in a large enterprise receives upwards of **2 billion events** per day

Finding a real security issue becomes like finding the proverbial **needle in a haystack**, and the likelihood we miss events goes up exponentially.



What this really comes down to is that Cybersecurity is a **data** problem

A security operations center. **With more complexity, companies generally require more people** to respond to sheer volume of alerts.



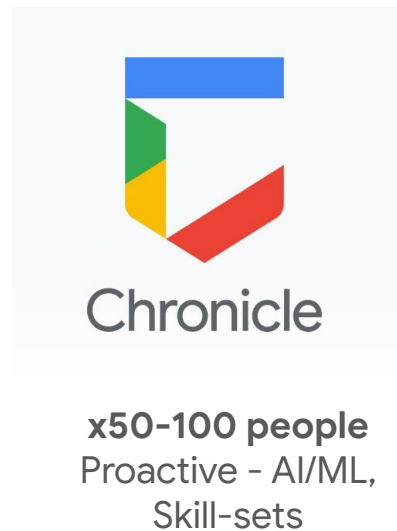
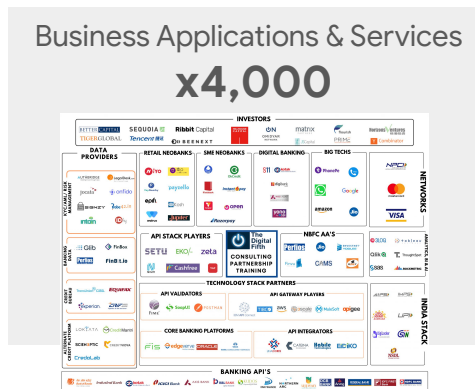
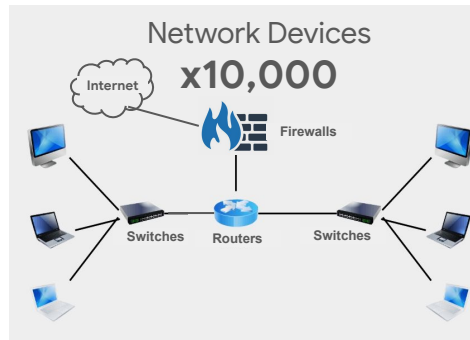


Complexity breeds a culture of 'No' and complexity makes our companies **far less secure** in the end.



The best Security Operations Centers, look like this. **Less people, simpler technology stacks, more automation.**







20 min

**Google's security journey** how we got hacked and why it was the best thing that happened to us

3

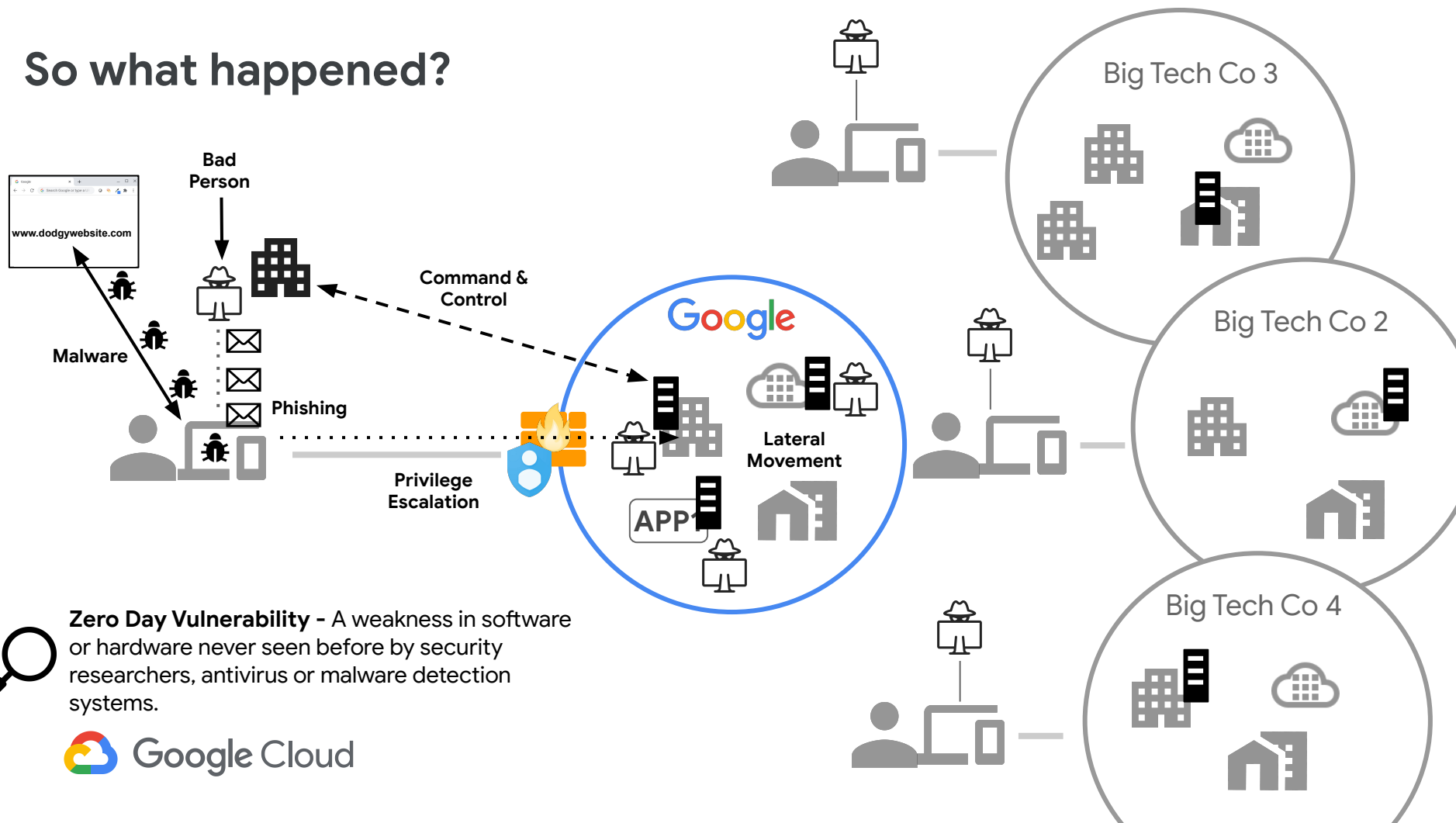




# HACKING GOOGLE

## EP000

# So what happened?



**Zero Day Vulnerability** - A weakness in software or hardware never seen before by security researchers, antivirus or malware detection systems.

# Why did it happen?

Because traditional Access assumes too much trust

Trusting passwords

91%

of information security  
attacks start with  
phishing\*

Trusting networks

70%

of all attacks involve  
attempts at lateral  
movement\*\*

Trusting users

34%

data breaches involve  
internal actors\*\*\*

Source: \* PhishMe study, [cofense.com/enterprise-phishing-susceptibility-report/](https://www.cofense.com/enterprise-phishing-susceptibility-report/)

\*\* Global Incident Response Threat Report (GIRTR), , Carbon Black

\*\*\* 2019 Verizon Data Breach Investigations Report

# Trust nothing. Detect everything.

## Trust Nothing:

Zero-trust, 2FA identity and context-aware global access to internal applications

Zero-trust

## Detect Everything:

Telemetry-based, intelligence-driven high volume detection, investigation, and hunting leveraging AI/ML everywhere

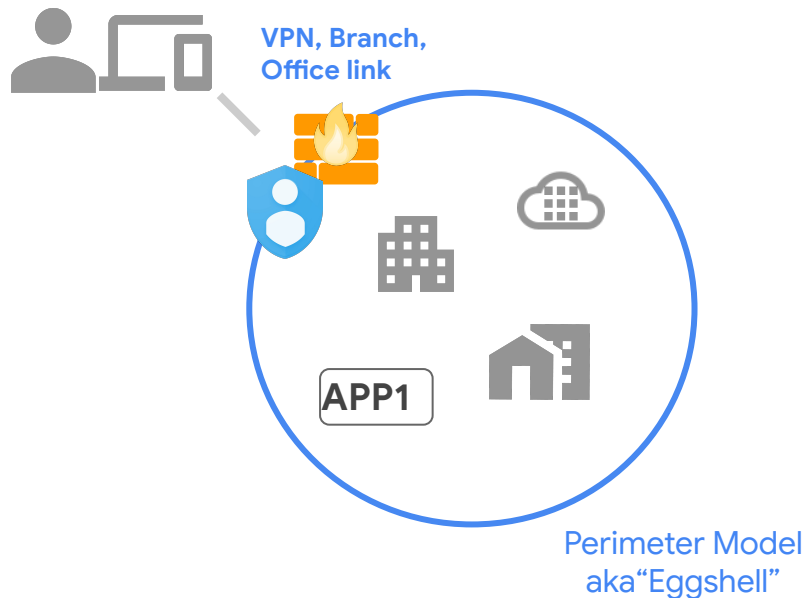
Chronicle



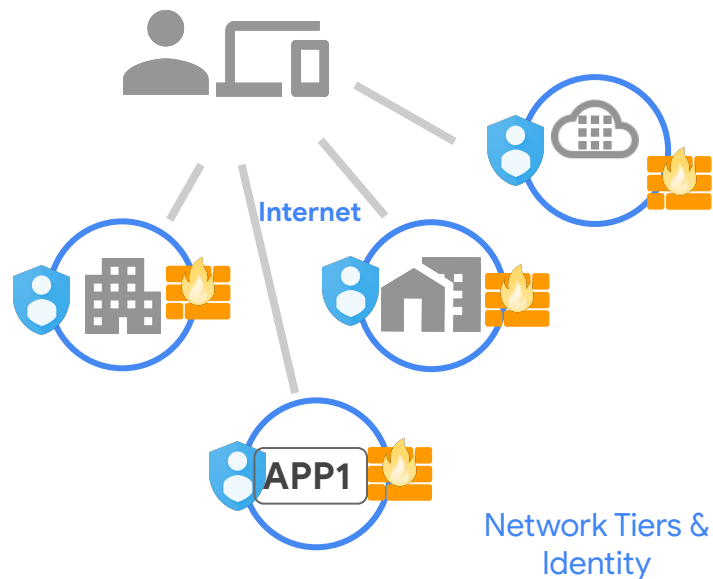


# Traditional Security vs Trust Nothing (Zero Trust)

## Traditional



## Trust Nothing





10 min

Some AI fun to get us started!























4

The last 10 years have  
been about mobile-first,  
over the next 10 years, we  
will **shift to a world that  
is AI-first.**

- Sundar Pichai  
CEO Google & Alphabet  
2016




# Alphabet

 <b>Google Ventures</b> Venture and Capital Funding	 <b>Calico</b> Longevity Research	 <b>Google X</b> Innovation Lab and Research			
 <b>Verily</b> Improving Quality of Life	 <b>DeepMind</b> Artificial Intelligence and Machine Learning	 <b>SideWalk Labs</b> Solving Big Urban Problems	 <b>Search Advertising SEM</b>	 <b>Google Cloud</b> Cloud Services, Workspace	 <b>Maps</b> Mapping, Location Services and Logistics
 <b>Waymo</b> Self Driving Vehicles	 <b>CapitalG</b> Help Tech Companies Scale	 <b>Jigsaw</b> Online Global Security Solutions	 <b>Google Marketing Platform</b> Unified Ad Technology Stack	 <b>Google Analytics</b> 360 Suite Data Analytics Suite of Tools	 <b>Android</b> Mobile Operating System
 <b>Access</b> Internet to New Communities	 <b>Wing</b> Delivery Drones	 <b>FitBit</b> Wearables	 <b>Hardware</b> Pixel, Chromecast, Google Home, Daydream View	 <b>YouTube</b> Internet Video Service	 <b>Nest</b> Connected Home Devices

Big Bets

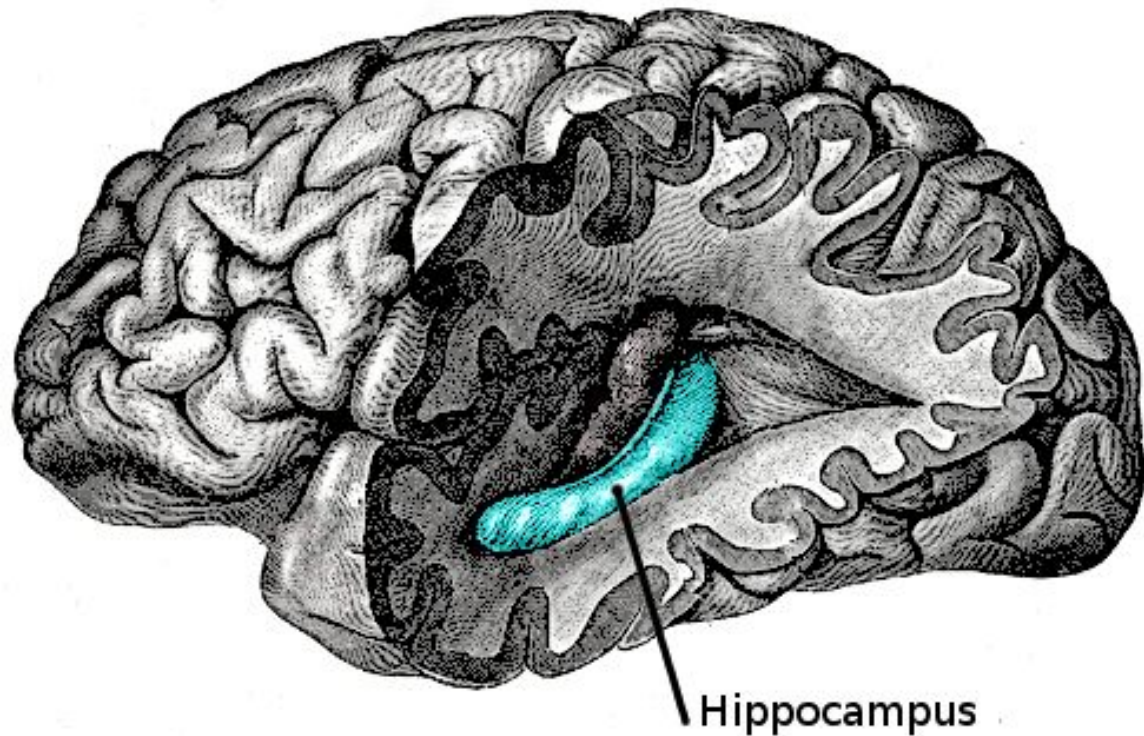
Google Cloud

A portrait of Demis Hassabis, CEO of DeepMind Technologies. He is a man with short dark hair and glasses, wearing a dark grey sweater. He is looking slightly to his right with a thoughtful expression. The background is a blurred indoor setting with warm lighting and a brick wall on the left.

“What we wanted to do at  
DeepMind was create an Apollo  
Program mission for AI.”

Demis Hassabis  
CEO DeepMind Technologies



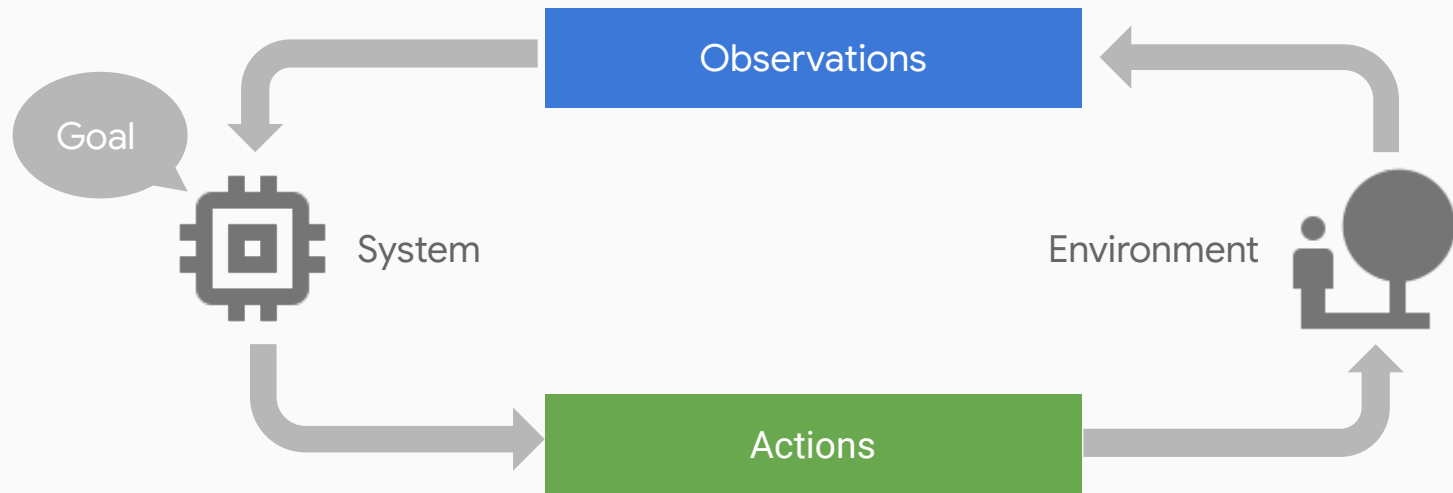


...Add the “high” and “dreaming while awake”

(Objective Function)

(Minibatch training)

## Build a *General* AI based on reinforcement learning



Demis sought to apply deep learning to “reinforcement learning,” where only reward guides adaptation.



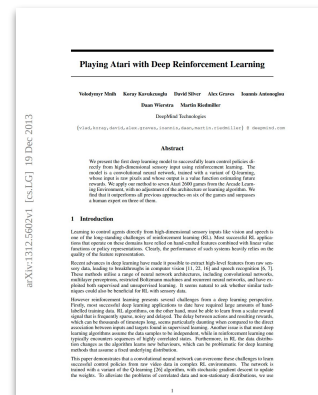
## Breakout - Invented by Steve Wozniak 1976

Google Cloud



## DeepMind - Playing Atari with Deep Reinforcement Learning

<https://arxiv.org/pdf/1312.5602v1.pdf>





- Pixels in, joystick out
- Just neurons
- 10 minutes...

Random luck.



120 minutes...

Flawless



240 minutes...

Strategy emerges



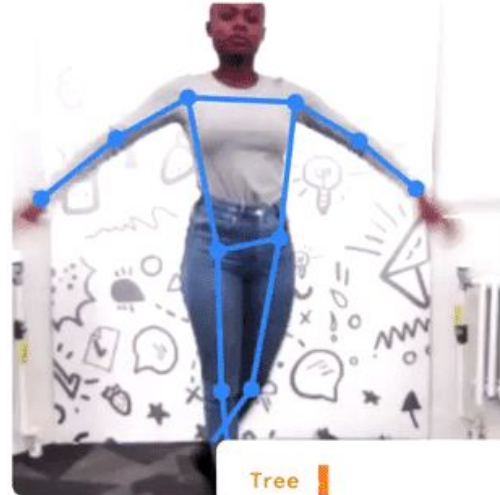
Grab your laptop and head to -  
[teachablemachine.withgoogle.com](https://teachablemachine.withgoogle.com)

# Teachable Machine

**Train a computer to recognize your own images, sounds, & poses.**

A fast, easy way to create machine learning models for your sites, apps, and more – no expertise or coding required.

Get Started



Tree

Wings

52%



10 min

Gamifying security to encourage curiosity and learning

5



Open your browser and go to:

**tryhackme.com**

1. Sign up and verify your email
2. Then go to:

**tryhackme.com/room/ohsint**

**Hint to get started:**

**Open attackbox > terminal >**

Hint: Type exiftool  
/root/Rooms/OhSINT/WindowsXP.jpg

# TryHackMe Classrooms

Assign fun pre-built security labs and challenges to your students. Manage assignments in a teaching dashboard and monitor user progress.

Teach **web app security**



## For your courses

Use our content as:

- Supporting Course Labs
- Assessments & Exams
- Real-world Challenges



## Student Management

Put students into groups and assign them security labs and challenges to complete.



## Monitor

View student activity and track their progress on your assignments.



## Reusable Lab Content

Save time creating exercises and choose from over 500 security labs to use in your classes.



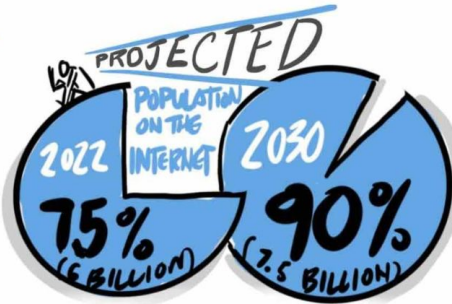
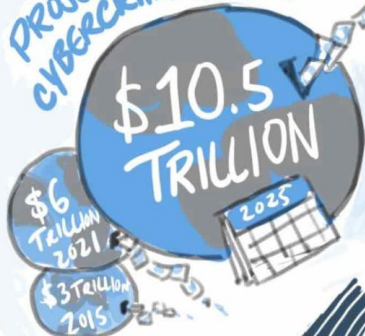
10 min

## The future of Cybersecurity skills and career pathways

6



PROTECTED  
CYBERCRIME COSTS:



GLOBAL  
RANSOMWARE  
DAMAGE:  
\$265 BILLION BY 2031

GLOBAL  
CYBERSECURITY  
SPEND:  
\$1.75 TRILLION  
2021-2025 CUMULATIVE

2022 CYBERSECURITY ALMANAC  
100 Facts, Predictions + Statistics  
published by CYBERSECURITY VENTURES  
READ AT: CYBERSECURITYALMANAC.COM

2031: A CONSUMER OR  
BUSINESS WILL SUFFER A  
RANSOMWARE  
ATTACK  
VS. EVERY  
11 SECONDS  
IN 2021

CYBER-  
INSURANCE  
MARKET  
\$8.5B 2021  
\$14.8B 2025  
\$34B 2031

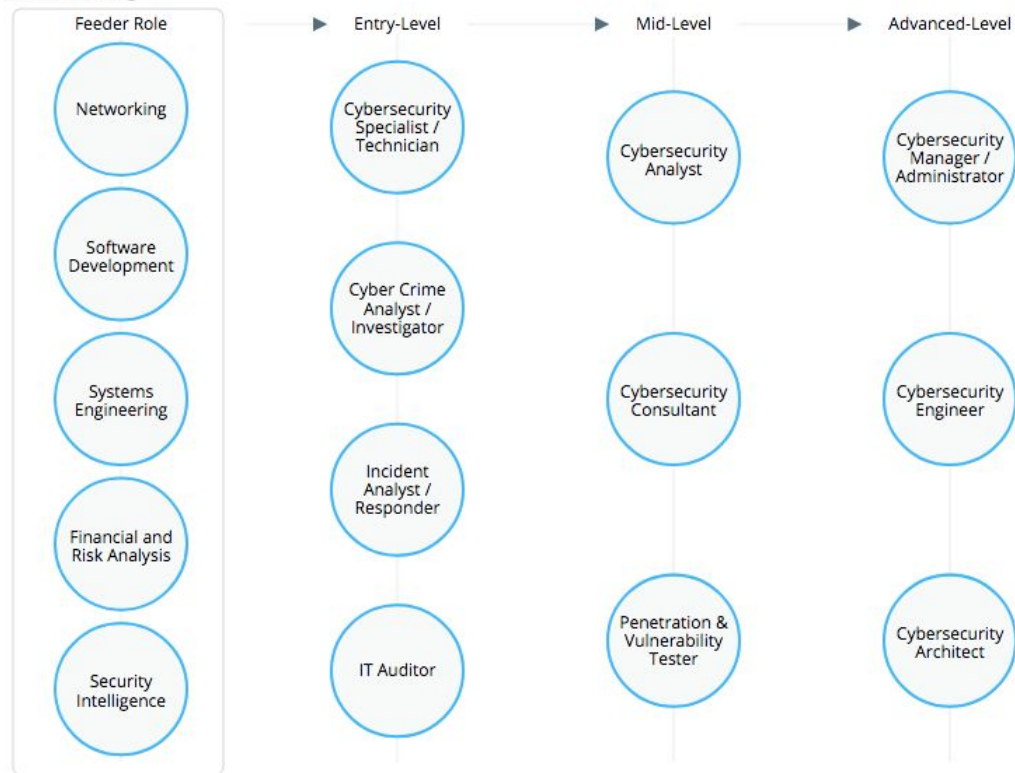
3.5M UNFILED JOBS  
EXPECTED TO REMAIN THROUGH 2025!

WE WILL NEED TO PROTECT 200 ZETABYTES OF DATA BY 2025...  
...50% OF THAT WILL BE STORED IN THE CLOUD  
SPONSORED BY CISCO

# Key Skills & Career Pathways

## Common Cybersecurity Feeder Roles ⓘ

## Core Cybersecurity Roles ⓘ



## Current Skills

### 1. Networking

- IPv4 / IPv6, Networks, switching, routing.
- Secure Protocols, mTLS, TLS, etc.
- Firewalls, IDS, IPS Systems

### 2. Operating Systems

- System administration
- Windows, Linux, and Mac OS. A, Kali Linux
- Computer Forensics

### 3. Cryptography

- Private/Public Key Cryptography

### 4. Ethical Hacking and Penetration testing

### 5. Automation

- CI/CD, YAML, IaC, Automation Tooling

### 5. App Development & Coding

- C, C# and C++ Python, JavaScript, PHP
- HTML, Go lang, Rust, Assembly

### 6. Cloud

- GCP, AWS, Azure.

### 7. Risk Modelling & Management

## Future Skills

1. Blockchain & Web 3.0
2. Internet of Things (IoT)
3. Data & Artificial Intelligence (AI)
4. Quant Analysis / Cyber-insurance
5. Quantum Computing

## Key Takeaways & Useful Resources



Historically, cybersecurity has been a **reactive** game, we build defences, then react to problems.



Moving forward, we will use AI/ML to **train computers how to recognise and respond to cybersecurity threats**

# Bringing Google Security to the World

## Strategic Advisory Services

Partner with executive leaders to advise and structure their digital security transformation. Proactive engagement and professional services support.

## Trust and Compliance

Maintain and develop and compliance certifications that help our customers meet their compliance requirements. Work with lawmakers, regulators, public officials, industry associations, trade groups and key influencers, to shape opinion on regulations.

## Customer and Solutions Engineering

Develop, launch, and scale anchor solutions that clearly solve business / organization risk issues while ensuring Google best practices with every solution.

## Threat Intelligence and Incident Response

Share macro thematic and product contextualized threat intelligence to enhance customer capabilities. Timely response and prescriptive guidance on relevant industry incidents and crises.

## GCAT Solutions



### Security and Resilience Framework

Help our customers to assess risk, protect their businesses from threats, maintain continuous operations, and enable rapid recovery in the event of a crisis



### Security Transformation

Provide customers with an ever-increasing, curated list of solutions and assets to evolve their security posture.



### Strategic Information Sharing

Series of threat and cyber intelligence publications and cyber-range training exercises.

[cloud.google.com/security/gcat](https://cloud.google.com/security/gcat)



## Cybersecurity Action Team

Google's premier security advisory team to support the security and digital transformation of government, critical infrastructure, enterprise, small business, consumers and society overall.

### Recent Google Security Commitments:



Invest \$10 billion over the next five years to strengthen cybersecurity,<sup>1</sup>



1 of 9 initial partners of the Joint Cyber Defense Collaborative under DHS.<sup>2</sup>

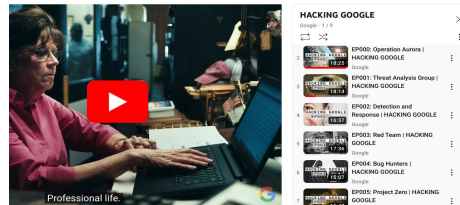


Pledge to train 100,000 Americans in fields like IT Support and Data Analytics.<sup>3</sup>

# Useful Resources

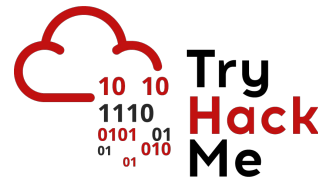
**Hacking Google** - 6 part mini-series

<https://g.co/safety/HACKINGGOOGLE>



**TryHackMe** - Online Cyber Security Modules, Challenges, CTF etc.

<https://tryhackme.com>



**Google Cybersecurity Action Team**

<https://cloud.google.com/security/gcat>



**2022 Cybersecurity Almanac** - Cybersecurity Ventures

[Cybersecurityalmanac.com](https://cybersecurityalmanac.com)



## Useful Resources

**Me** - I'm always happy to come and talk to students about Cloud, Cybersecurity, AI/ML & Data.

Add me on LinkedIn!

<https://www.linkedin.com/in/sullivanepatrick/>



**Patrick Sullivan**

Enterprise Architect, Google Cloud NZ

Auckland, Auckland, New Zealand · [Contact info](#)

