Zero Trust

The Evolution of Enterprise Security

Charlie Gero

CTO Akamai Technologies

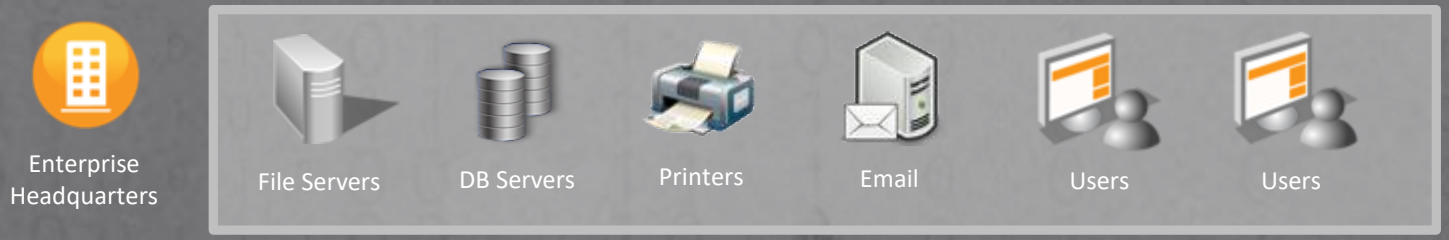
Enterprise Division and Advanced Projects Group

Akamai

Birth of Perimeter Security

Enterprise
Headquarters

Birth of Perimeter Security



Birth of Perimeter Security

Birth of Perimeter Security

Birth of Perimeter Security

Birth of Perimeter Security

Birth of Perimeter Security

Discoverability

HIGH

Birth of Perimeter Security

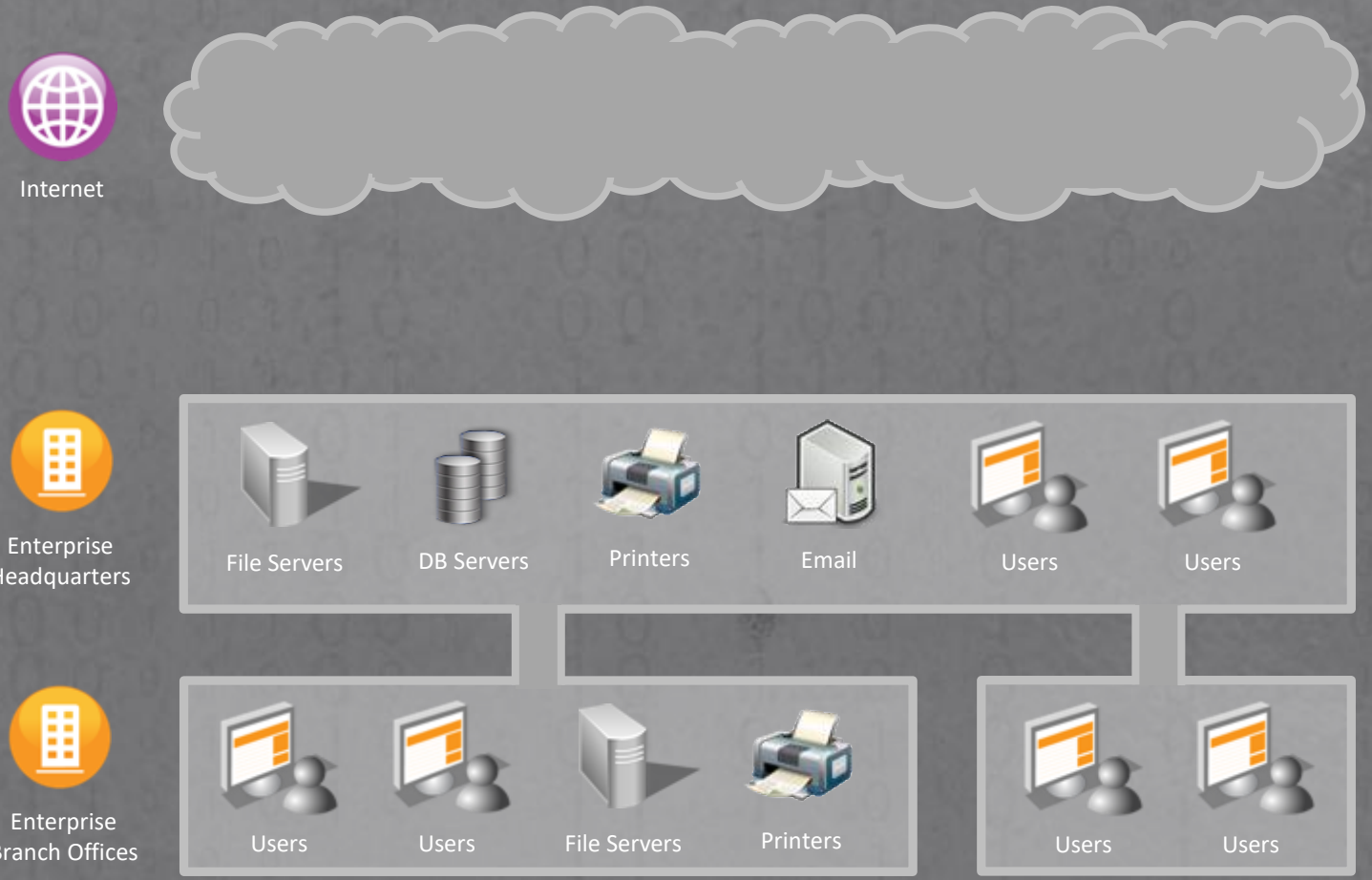
Discoverability

HIGH

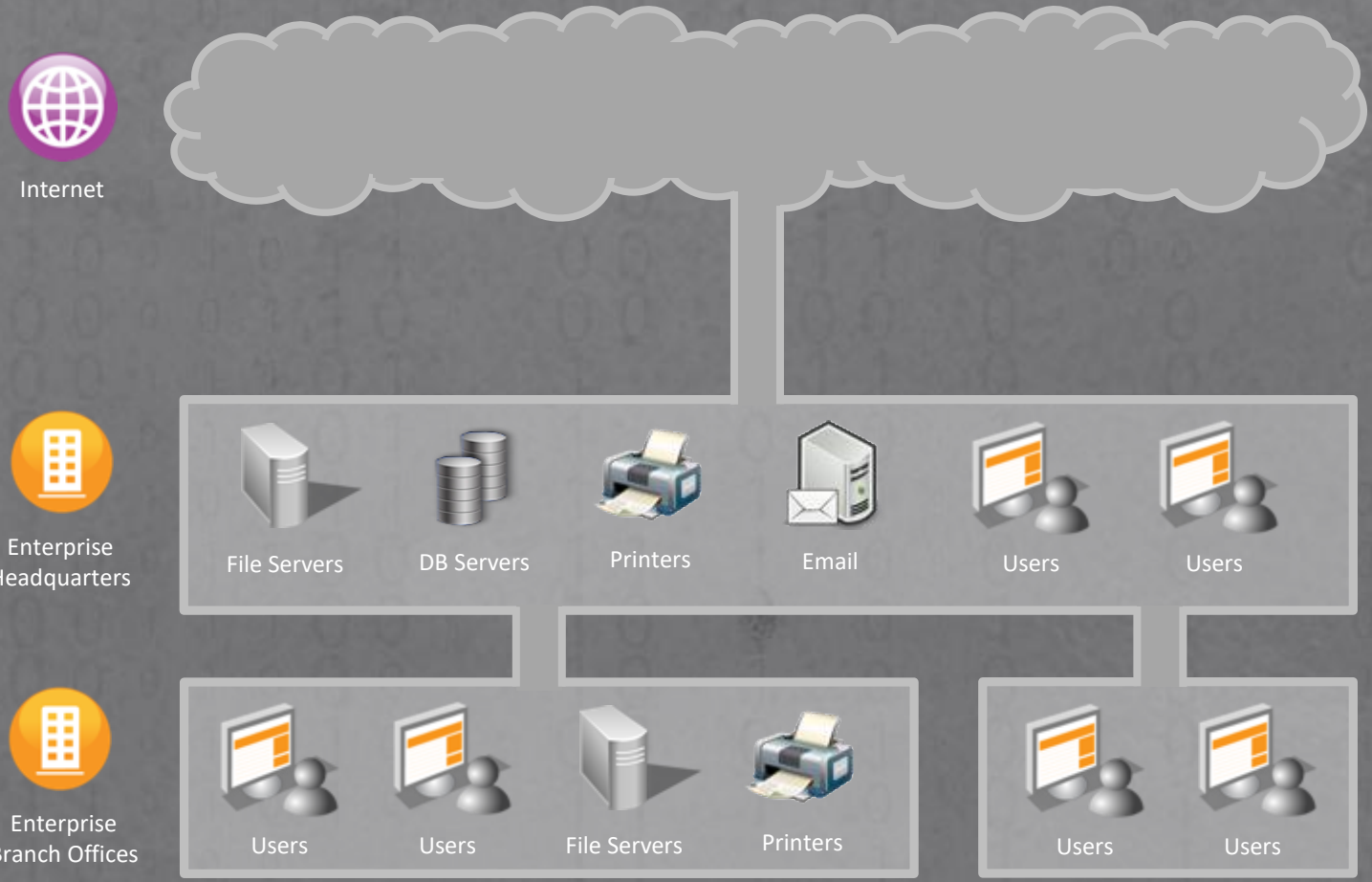
Repercussions

HIGH

Birth of Perimeter Security



Birth of Perimeter Security



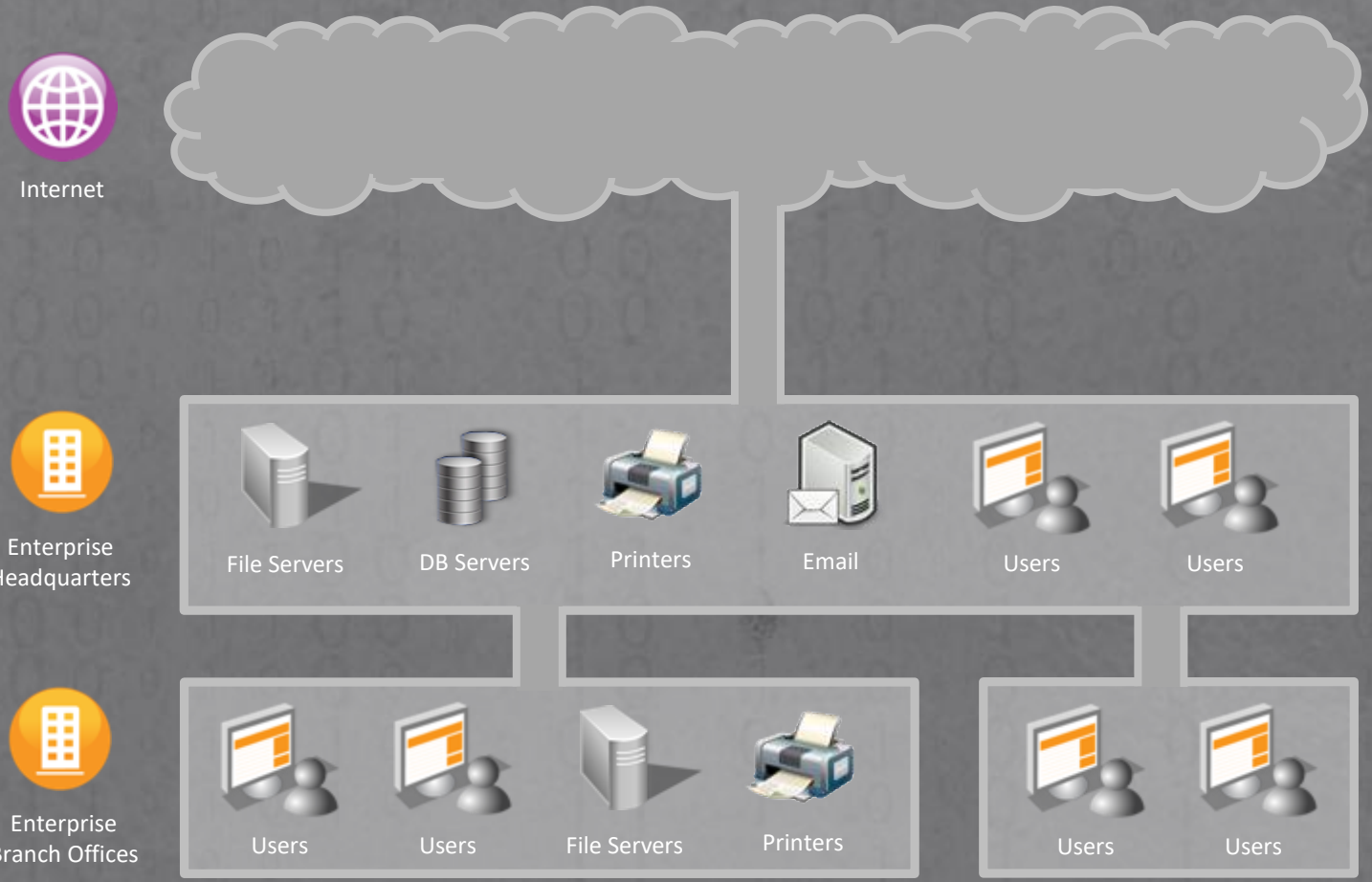
Discoverability

HIGH

Repercussions

HIGH

Birth of Perimeter Security



Discoverability

LOW

Discoverability

HIGH

Repercussions

HIGH

Birth of Perimeter Security

Discoverability

LOW

Repercussions

LOW

Discoverability

HIGH

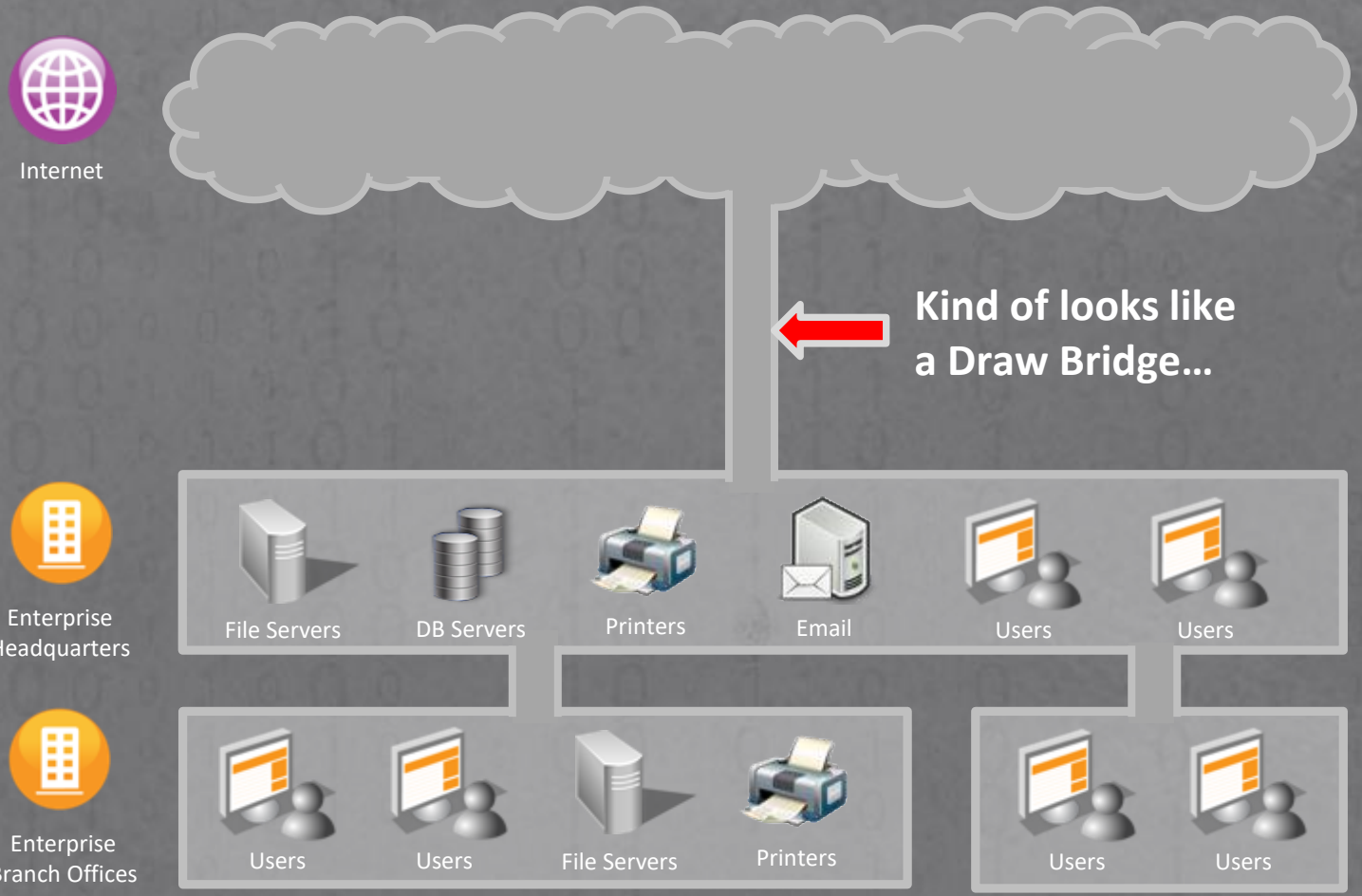
Repercussions

HIGH

Inside is good and outside is bad.


We have models for this.

Birth of Perimeter Security



Discoverability

LOW

Repercussions

LOW

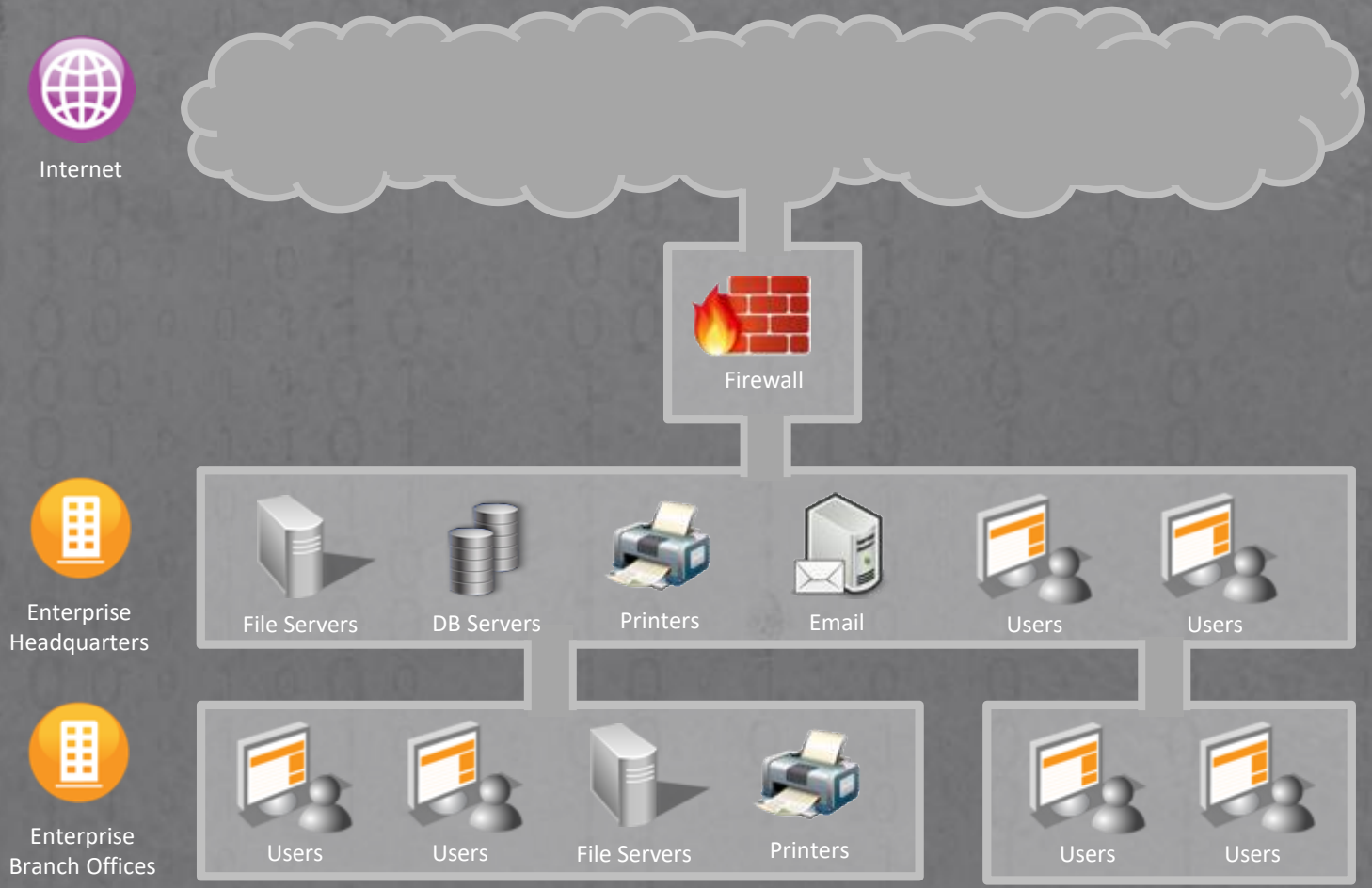
Discoverability

HIGH

Repercussions

HIGH

Birth of Perimeter Security



Discoverability

LOW

Repercussions

LOW

Discoverability

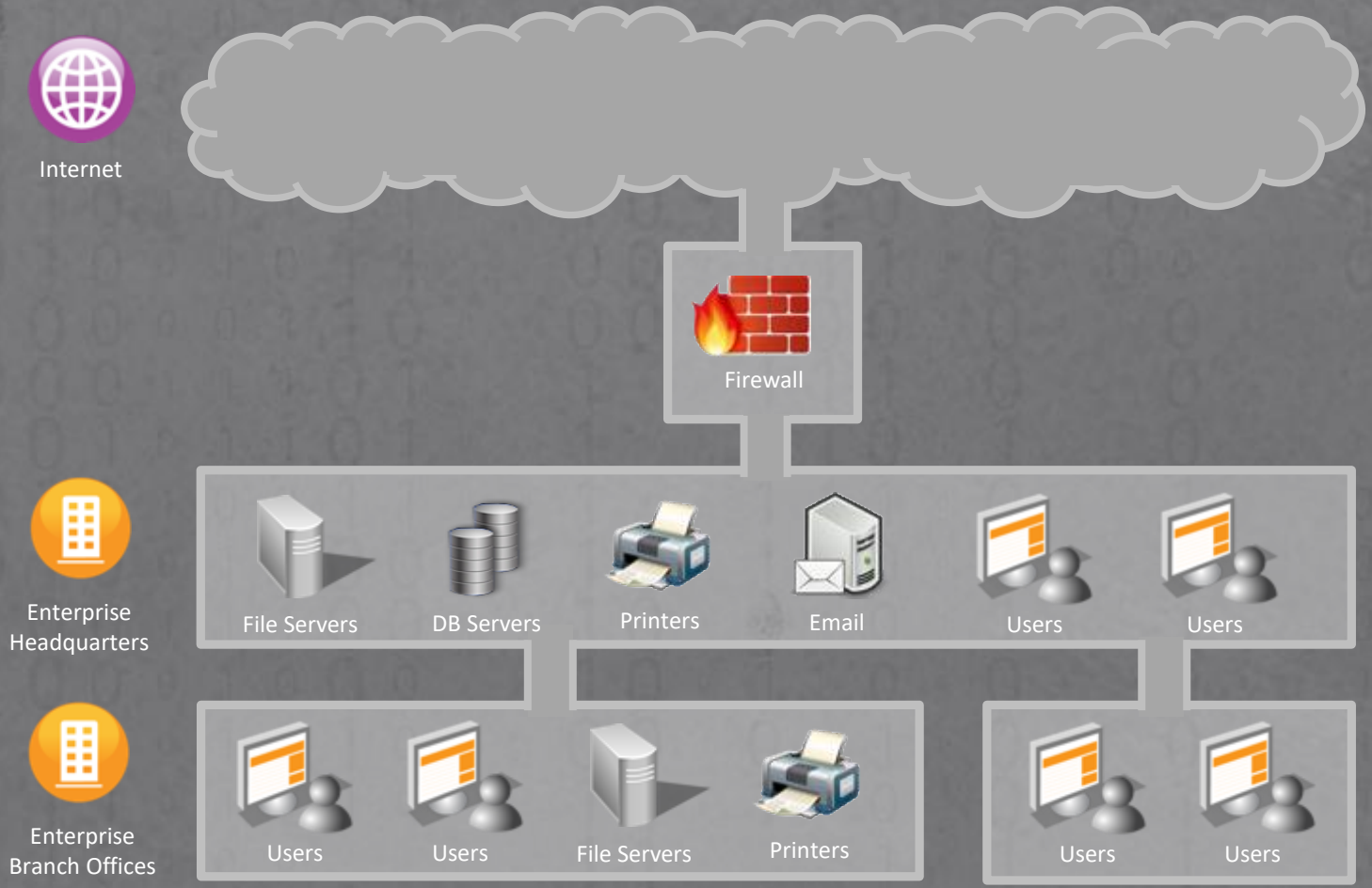
HIGH

Repercussions

HIGH


Wildly successful products spark business ecosystems.
Business ecosystems reinforce architectures.

Birth of Perimeter Security



Discoverability

LOW

Repercussions

LOW

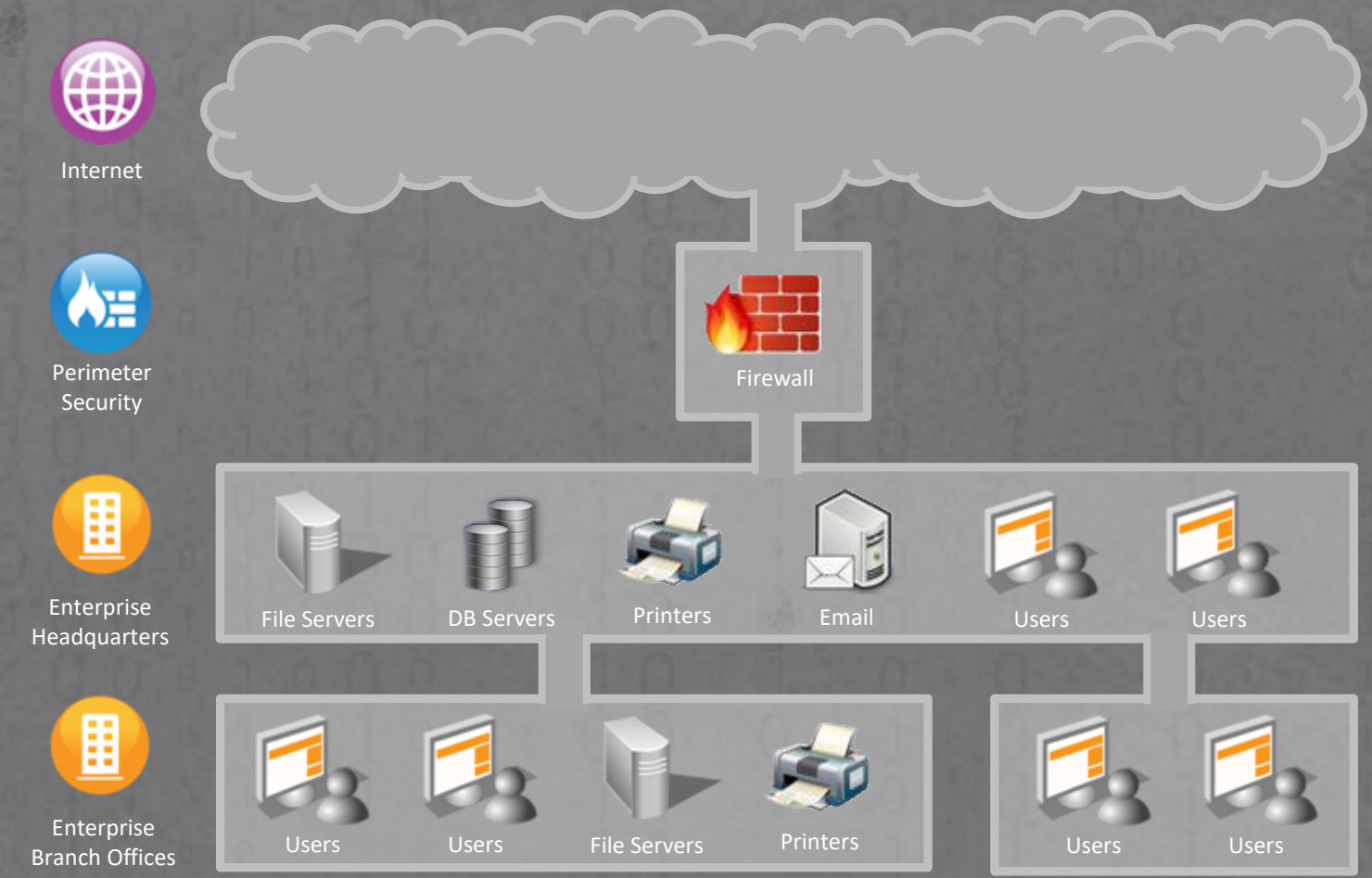
Discoverability

HIGH

Repercussions

HIGH

Birth of Perimeter Security



Discoverability

LOW

Repercussions

LOW

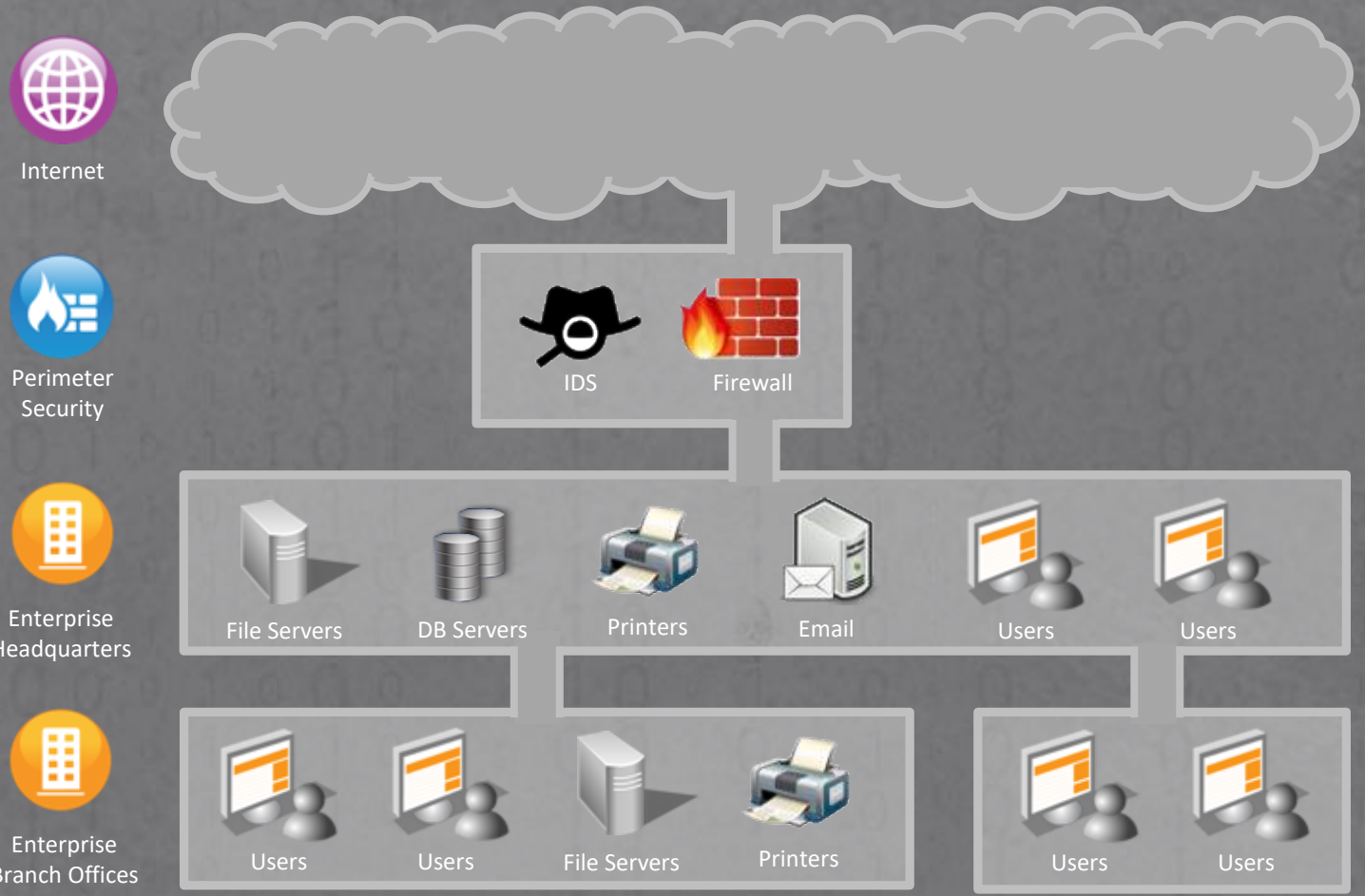
Discoverability

HIGH

Repercussions

HIGH

Birth of Perimeter Security



Discoverability

LOW

Repercussions

LOW

Discoverability

HIGH

Repercussions

HIGH

Birth of Perimeter Security

Discoverability

LOW

Repercussions

LOW

Discoverability

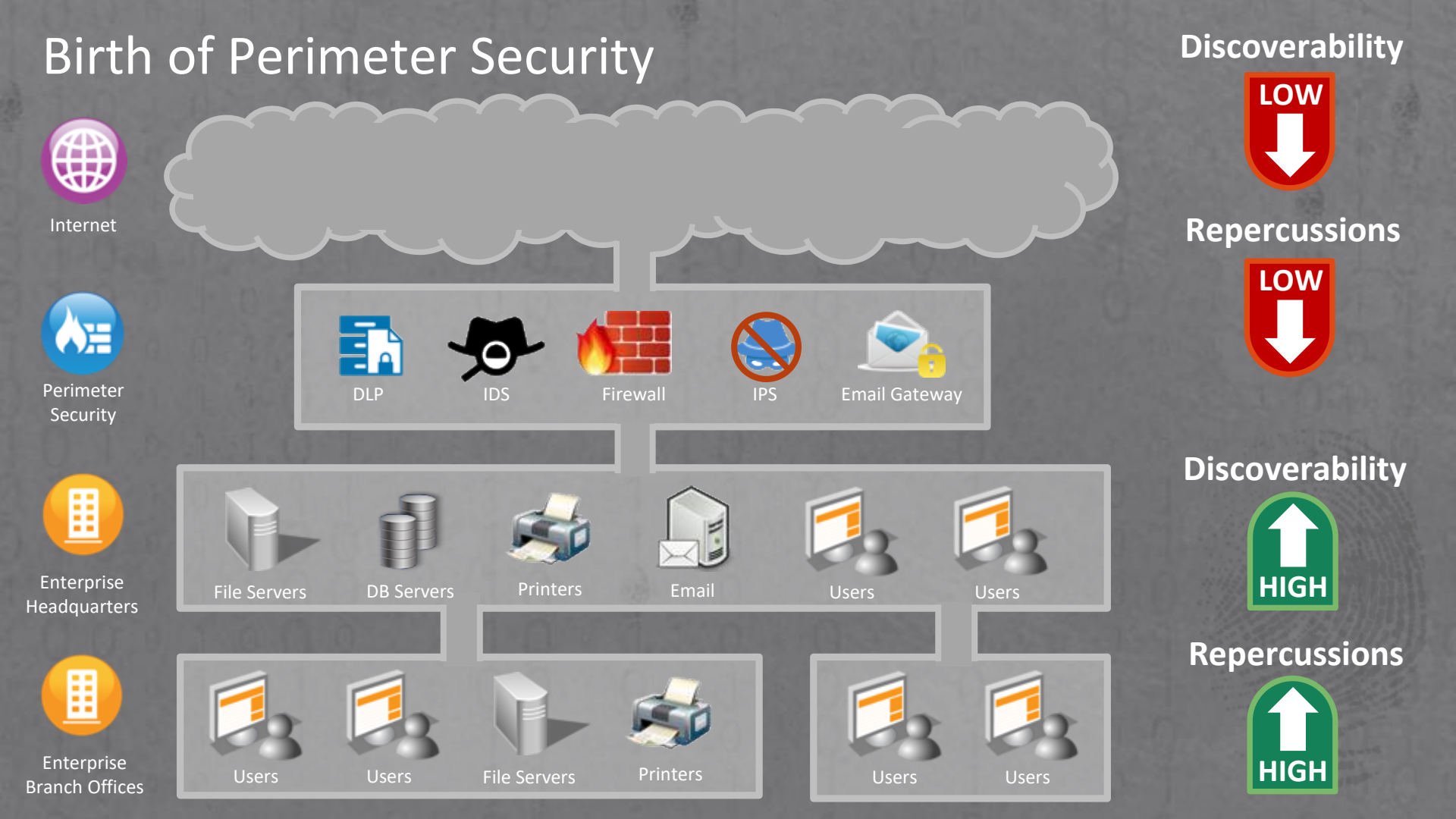
HIGH

Repercussions

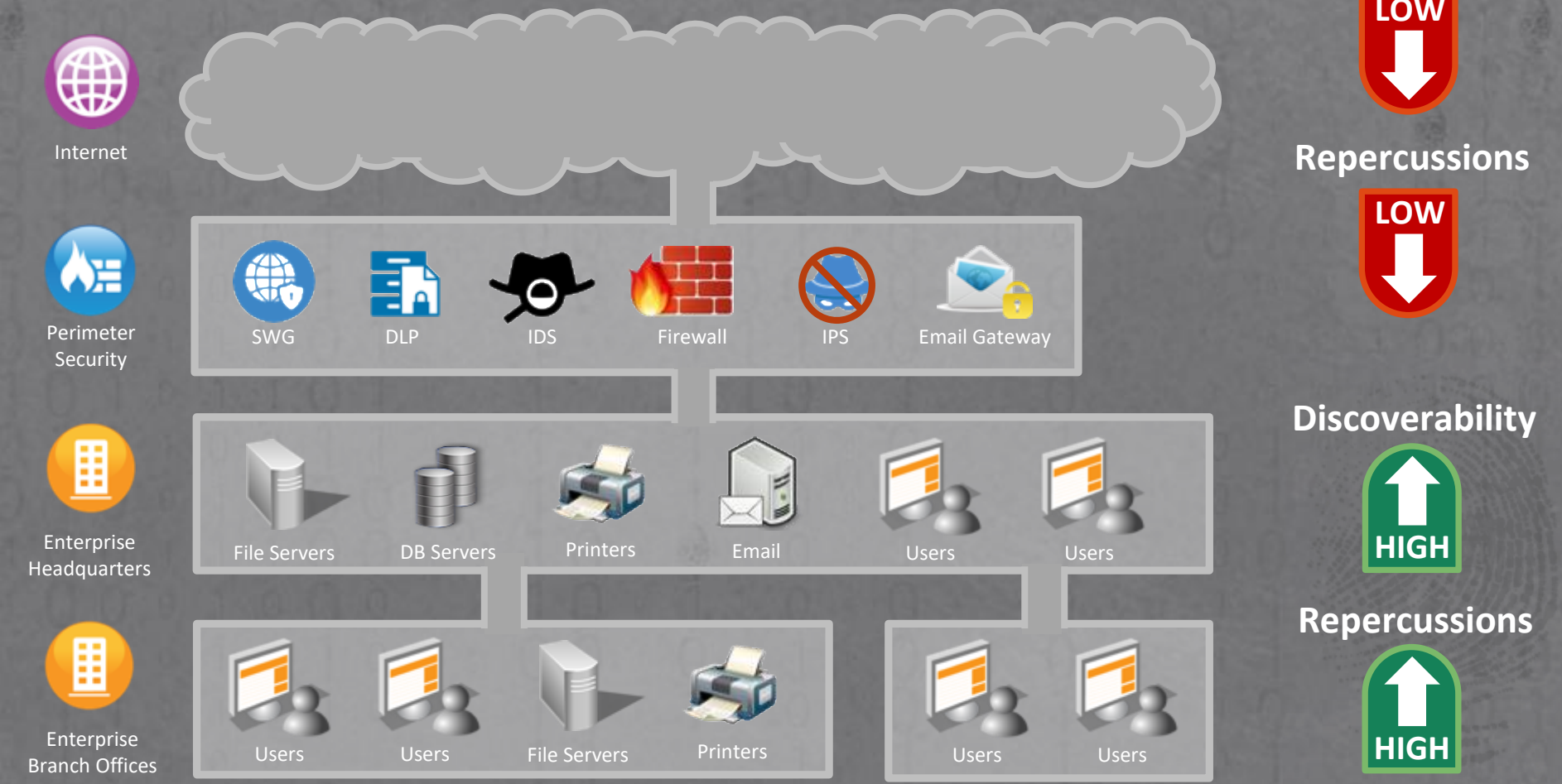
HIGH

Birth of Perimeter Security

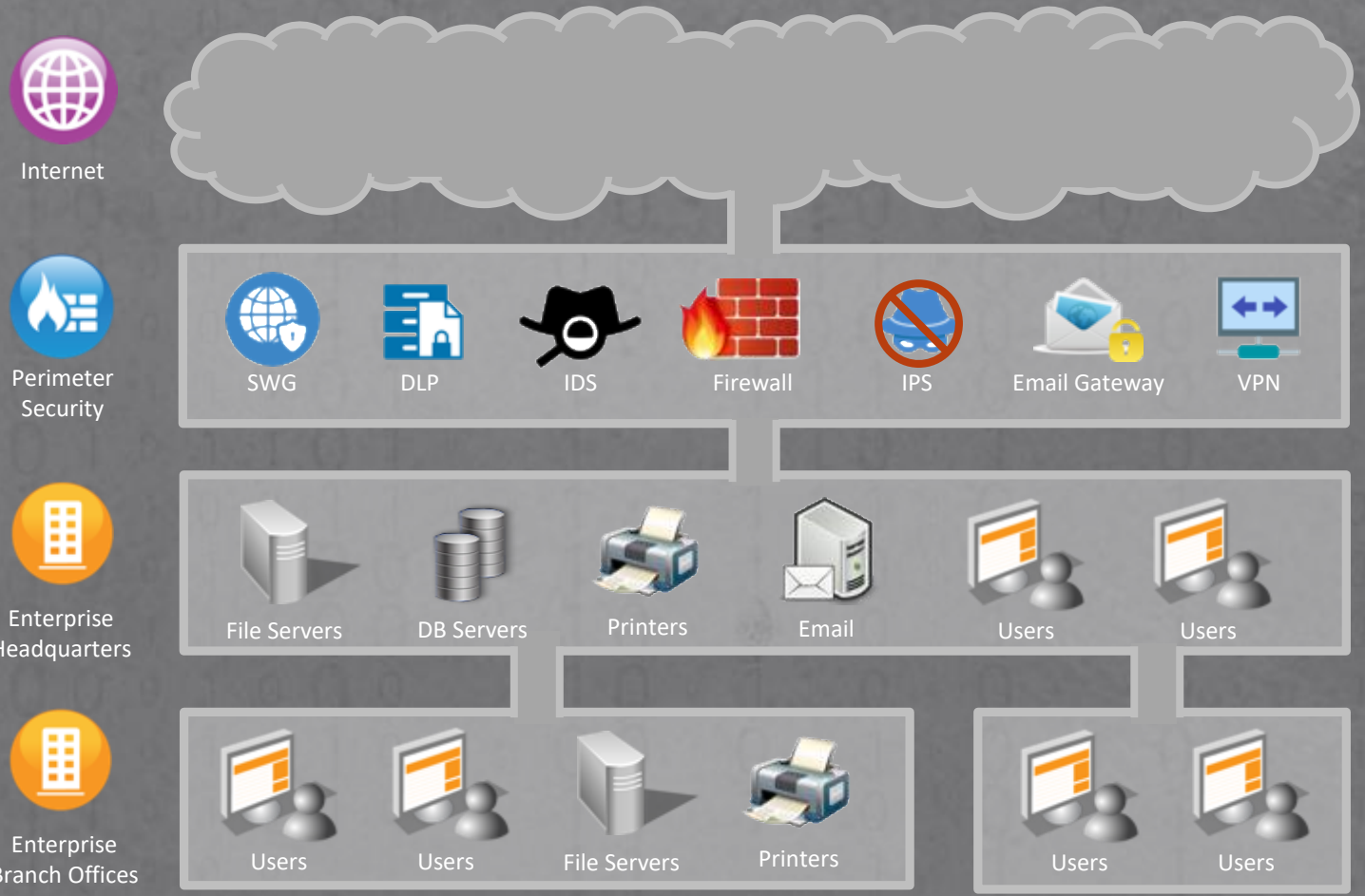
Birth of Perimeter Security



Birth of Perimeter Security



Birth of Perimeter Security



Discoverability

LOW

Repercussions

LOW

Discoverability

HIGH

Repercussions

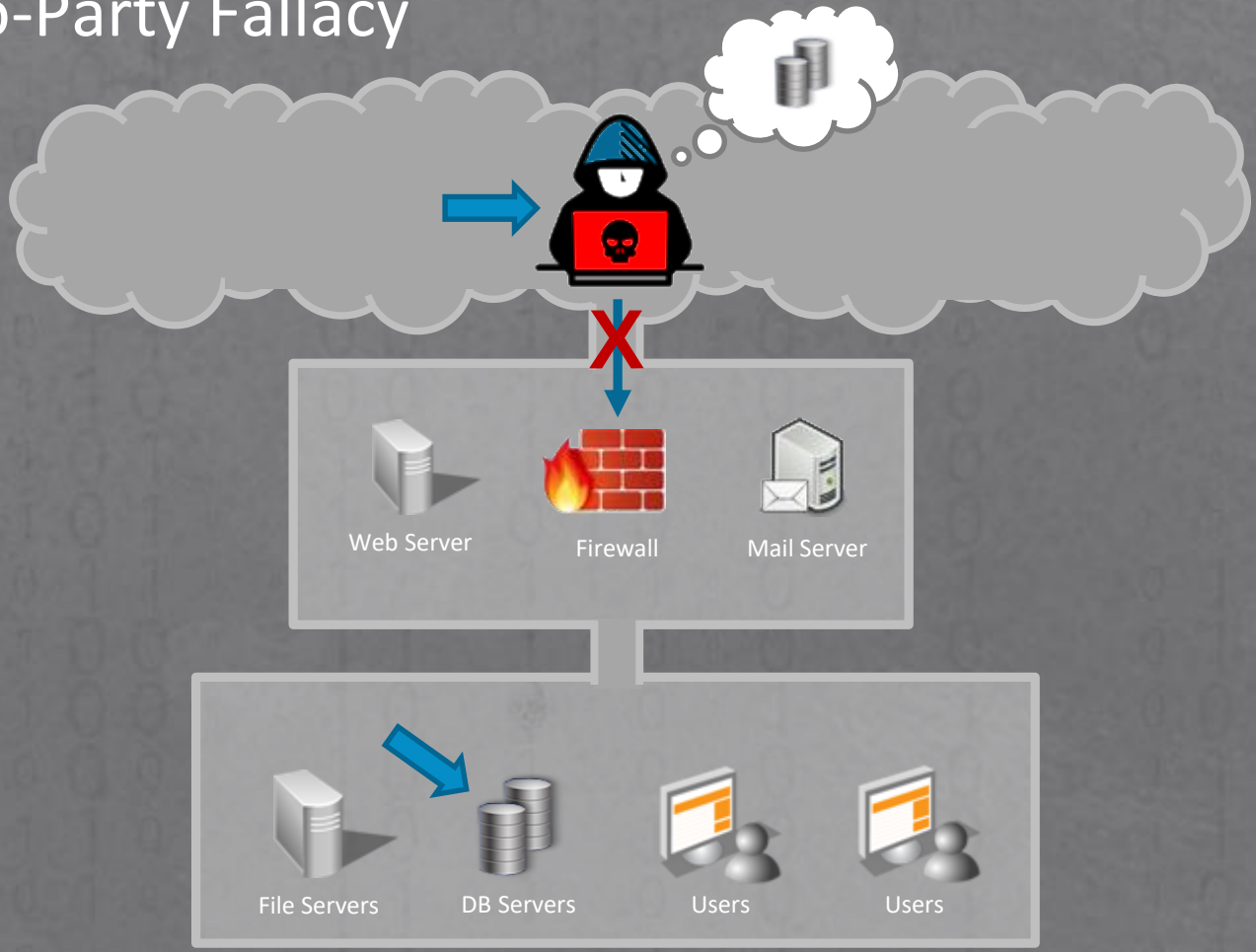
HIGH

We reached this architecture through logical steps.

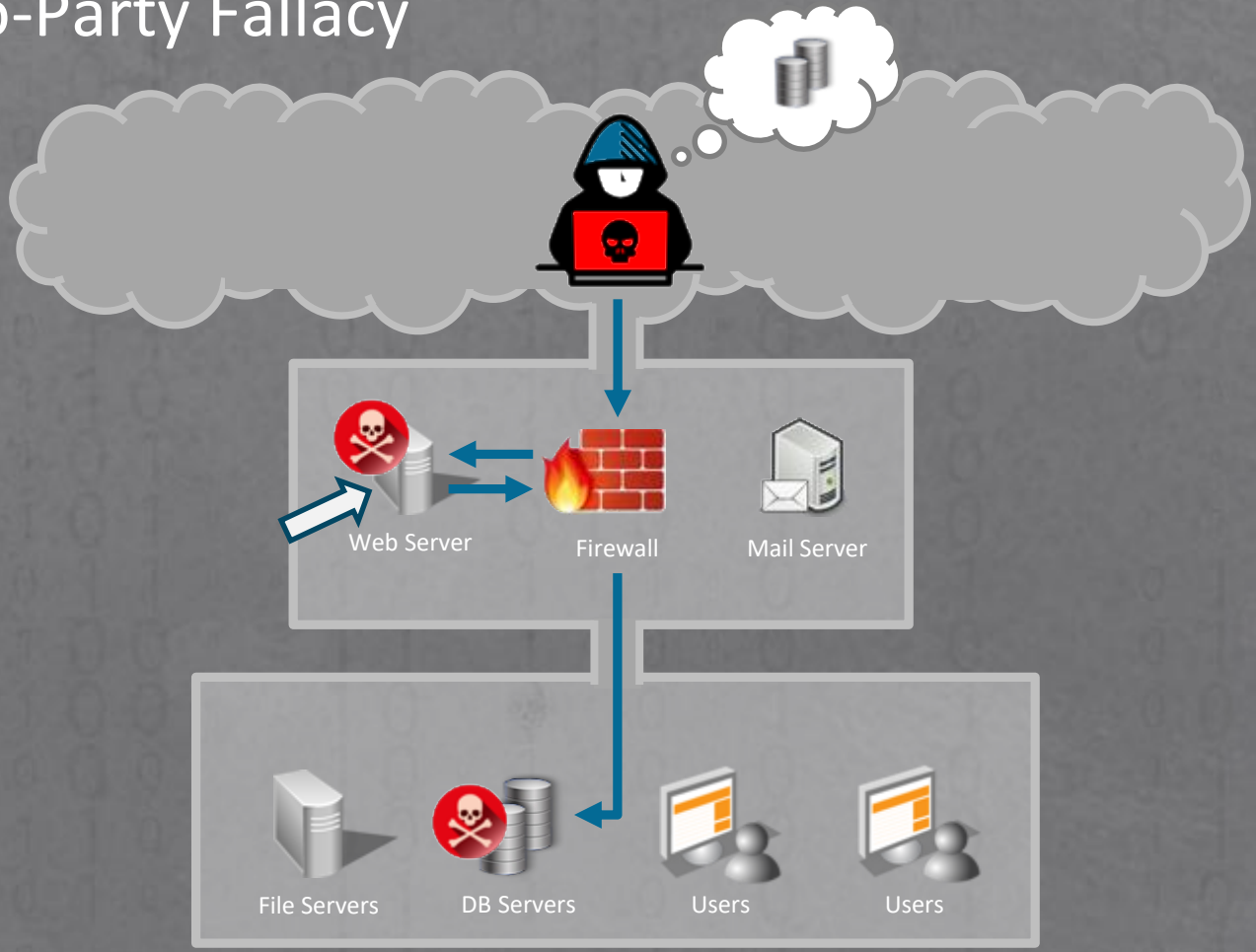
The business ecosystem reinforced it.

So why is it so DANGEROUS?

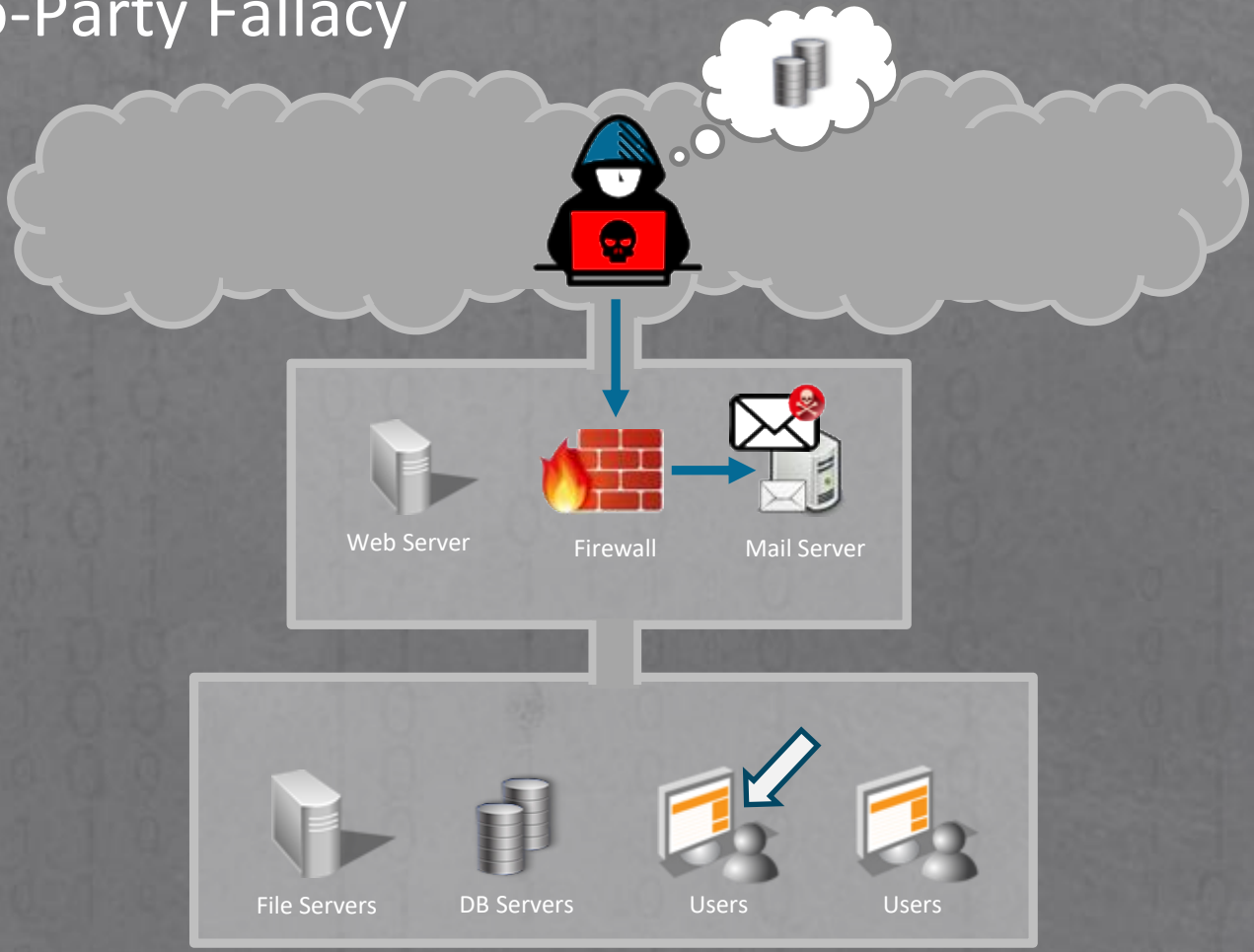
The Two-Party Fallacy



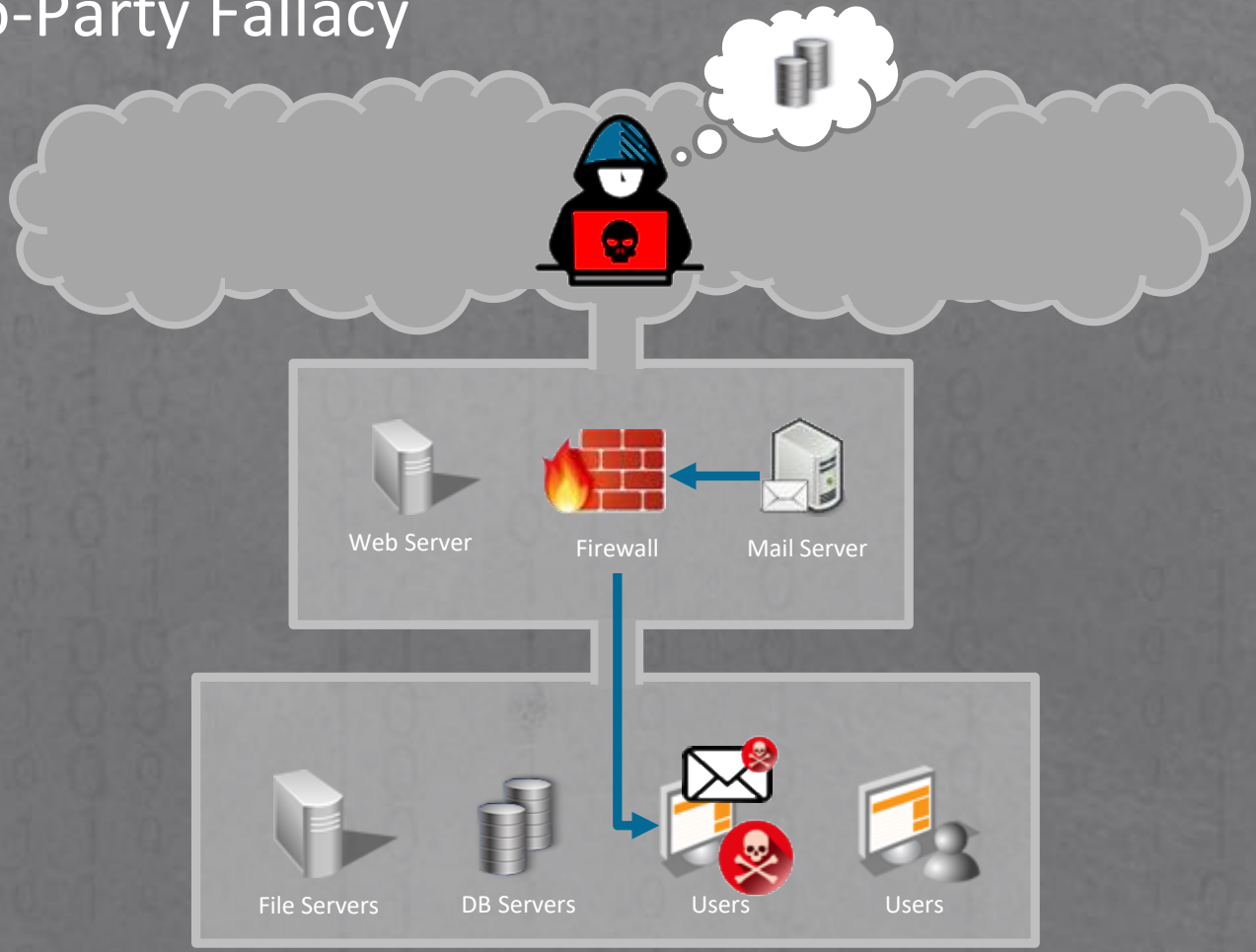
The Two-Party Fallacy



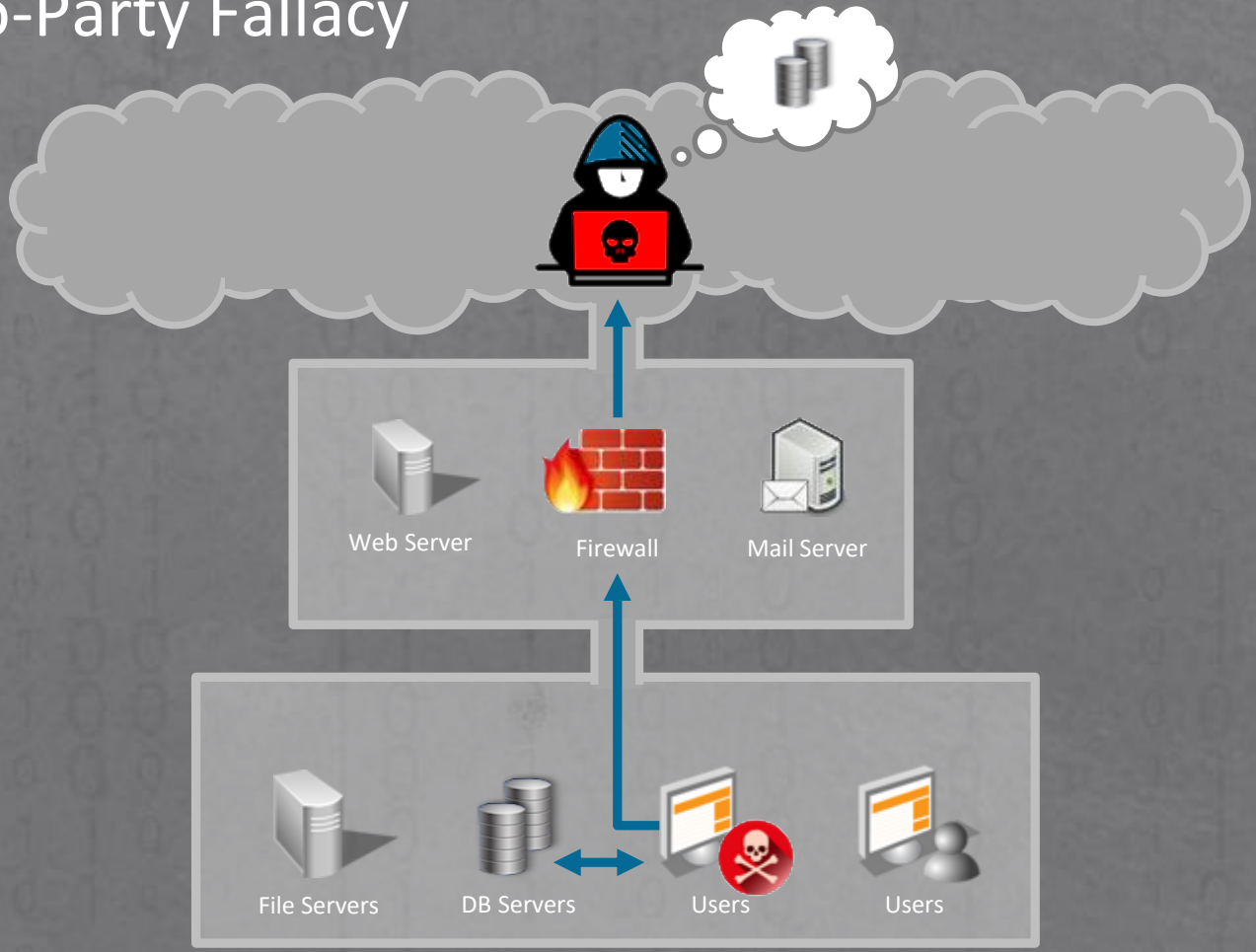
The Two-Party Fallacy

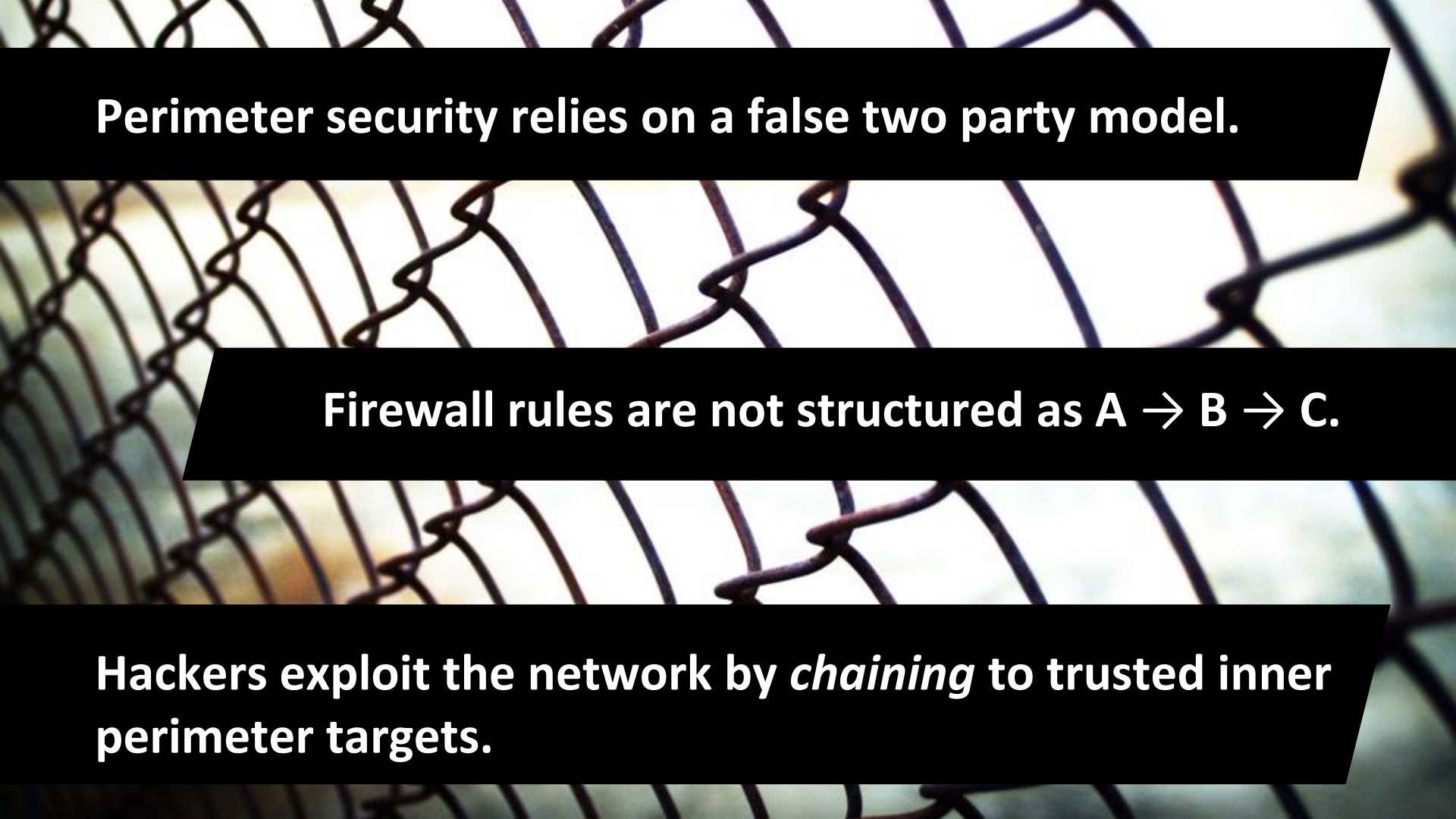


The Two-Party Fallacy



The Two-Party Fallacy

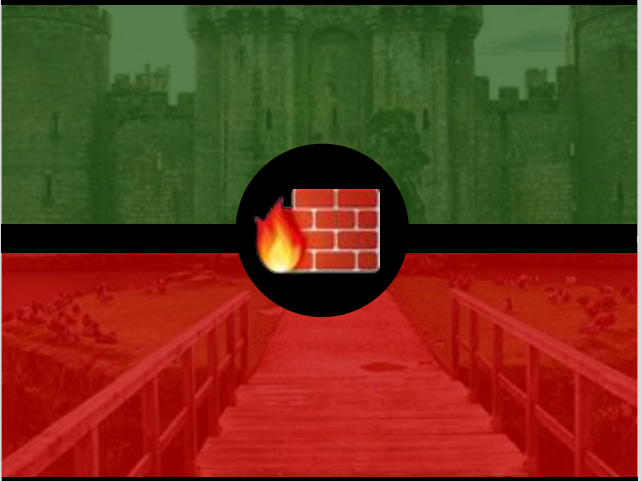



Perimeter security relies on a false two party model.
Firewall rules are not structured as A → B → C.
Hackers exploit the network by *chaining* to trusted inner perimeter targets.

It’s understandable how we arrived here.

We reached this architecture through logical steps.

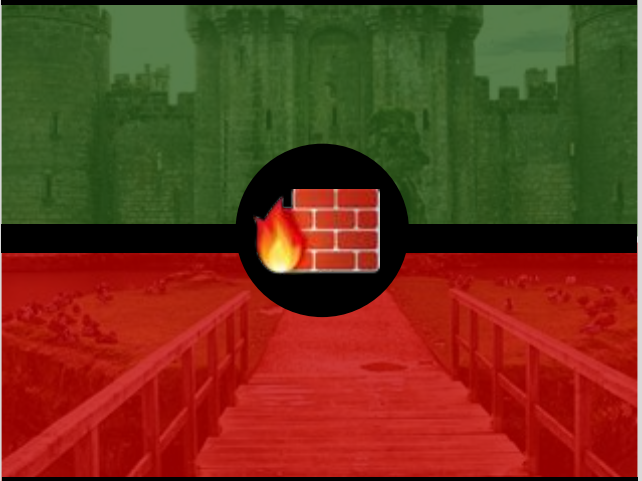
Inside is good



Outside is bad

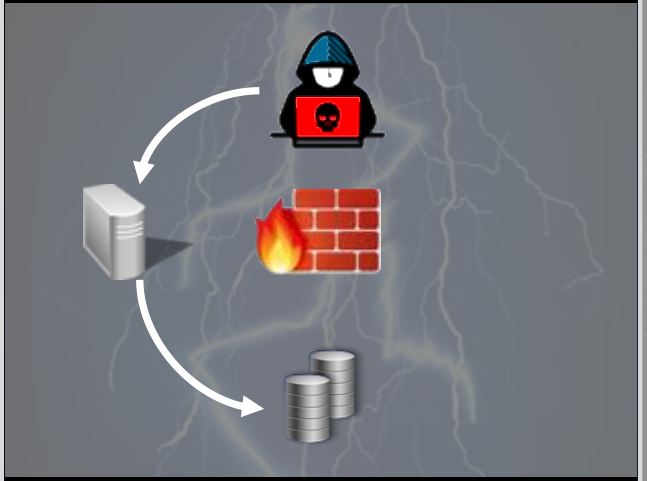
But the end result after 30+ years is highly dangerous.

Inside is good



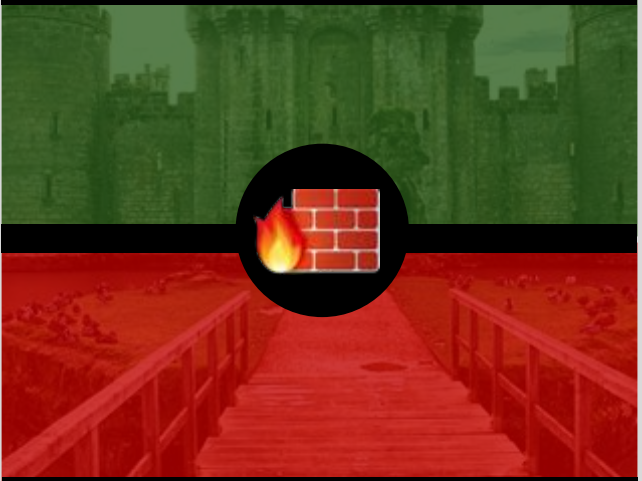
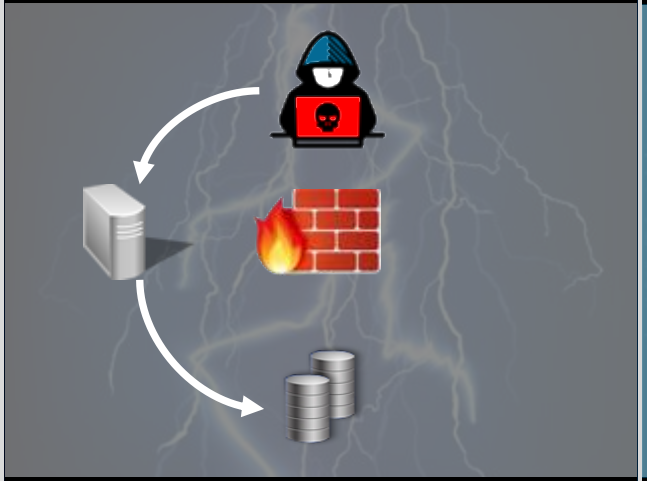
Outside is bad

Hackers take



Easiest path

So what comes next?

Inside is good	Hackers take	More point solutions
		
Outside is bad	Easiest path	vs. new architecture

ZERO TRUST

Acknowledgement by industry that more point solutions are not the answer.

Let’s fix the root problem: the architecture.

“Initial one-time block/allow security assessments for access and protection are flawed, leaving the enterprise open to zero-day and targeted attacks, credential theft, and insider threats.”

Excerpt from Gartner’s *Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats*

ZERO TRUST

PRINCIPLES

It is largely a

STRATEGY

There is no

INSIDE

Your users and apps can be

ANYWHERE

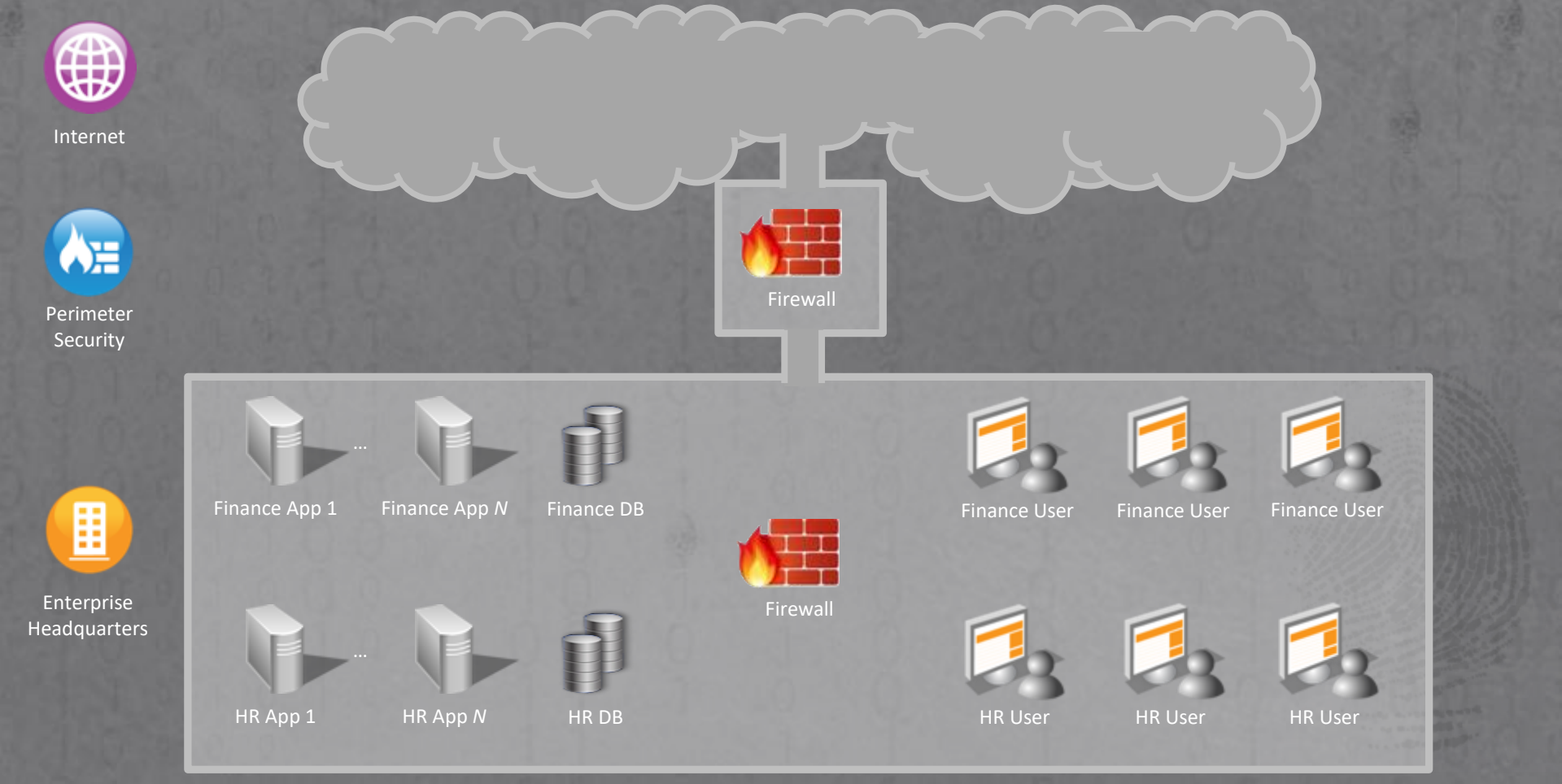

TRUST NO ONE
All access must be
AUTHENTICATED
AUTHORIZED &
VERIFIED

ZERO TRUST 1.0

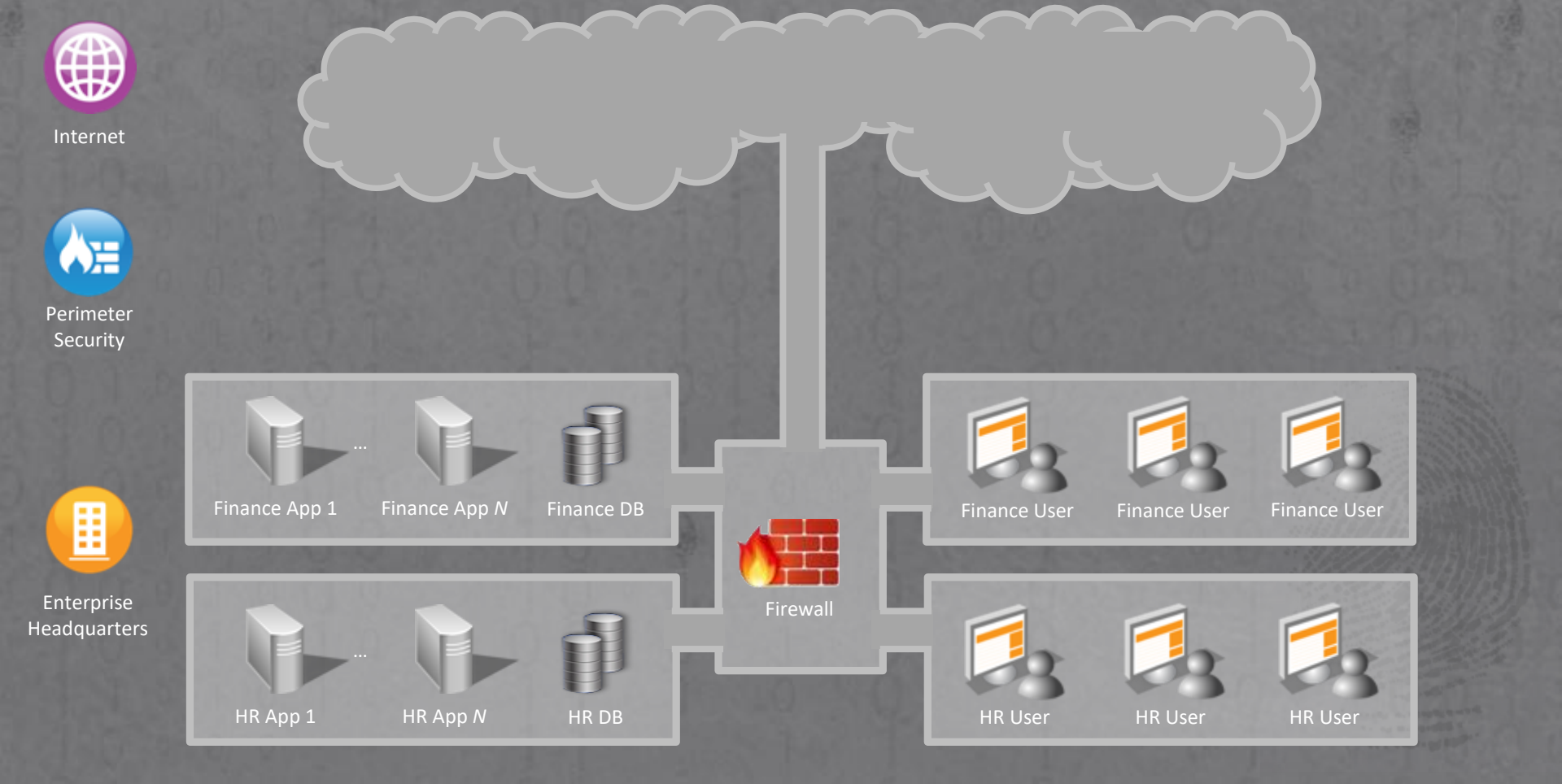
Control network flows between all assets.

Used to be called Micro-Segmentation.

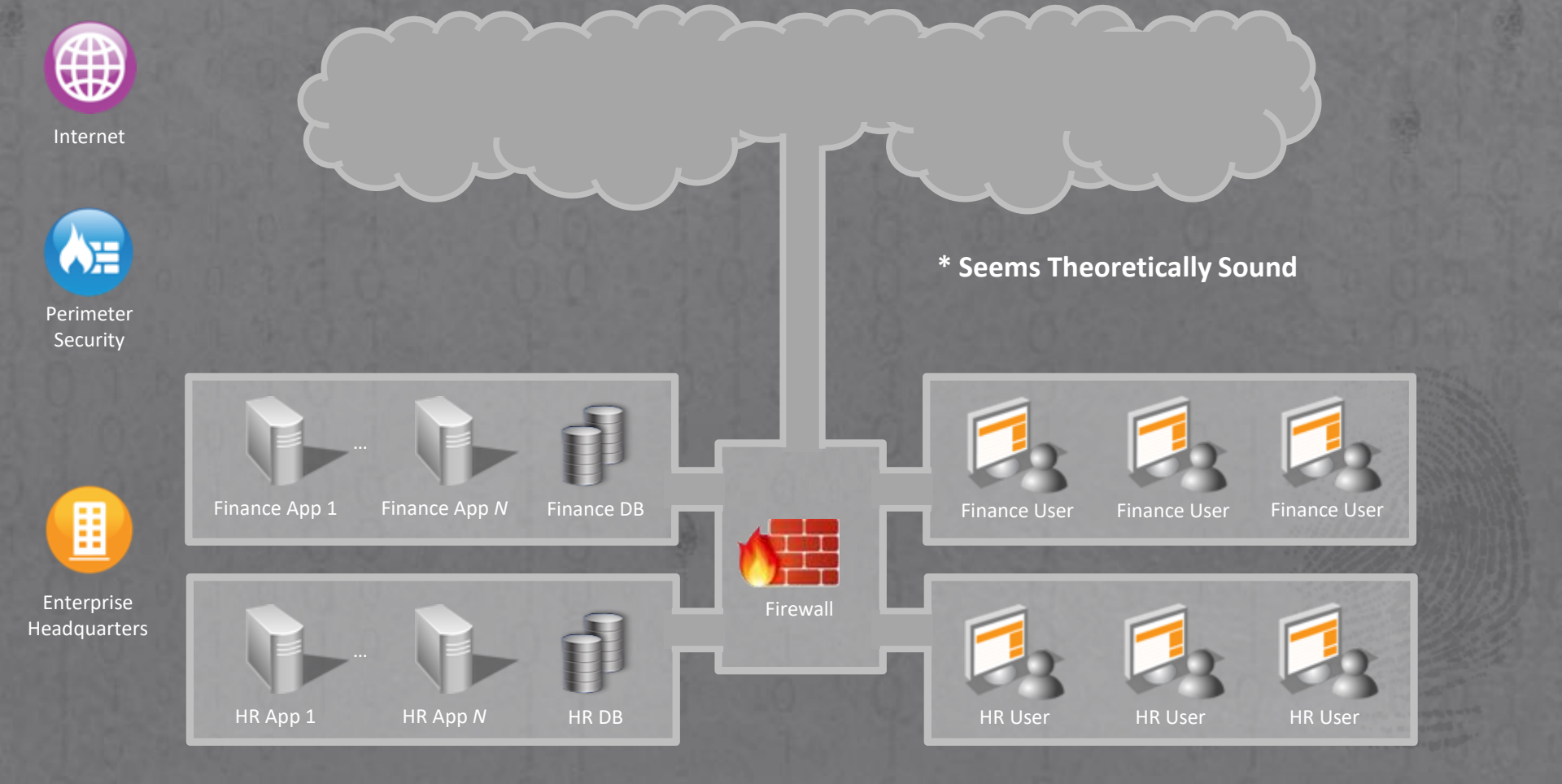
Zero Trust 1.0 – Micro-Segmentation



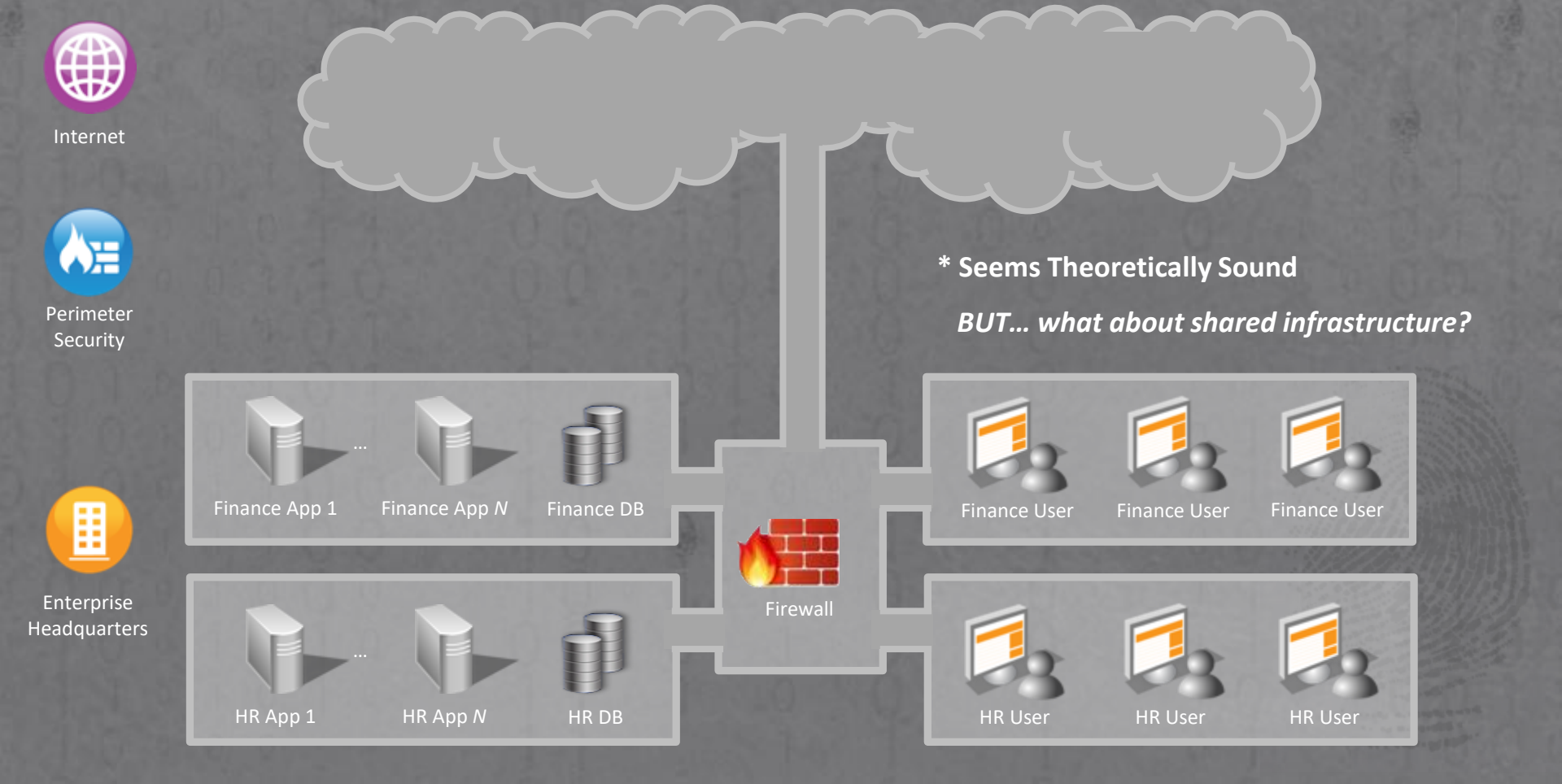
Zero Trust 1.0 – Micro-Segmentation



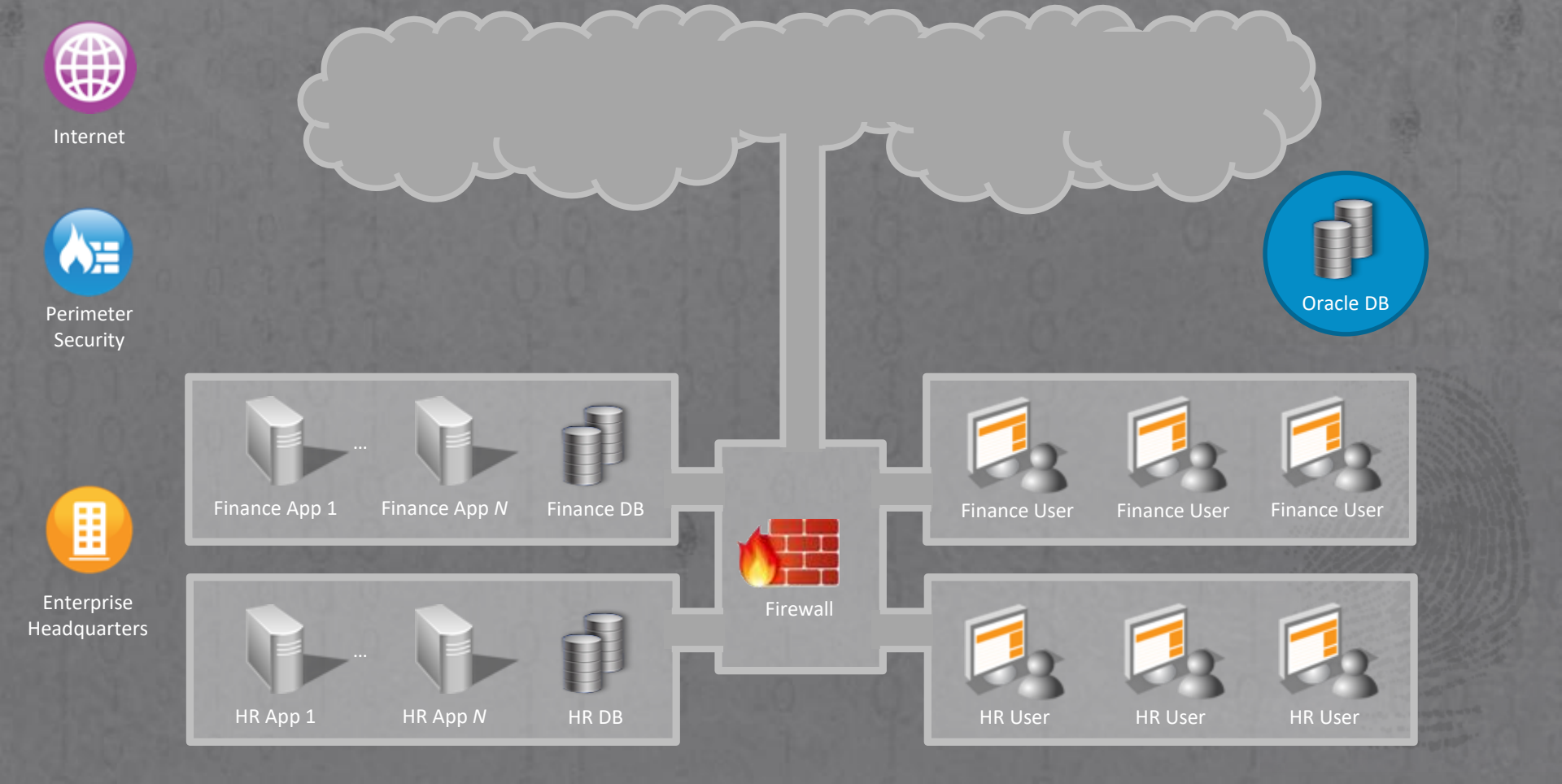
Zero Trust 1.0 – Micro-Segmentation



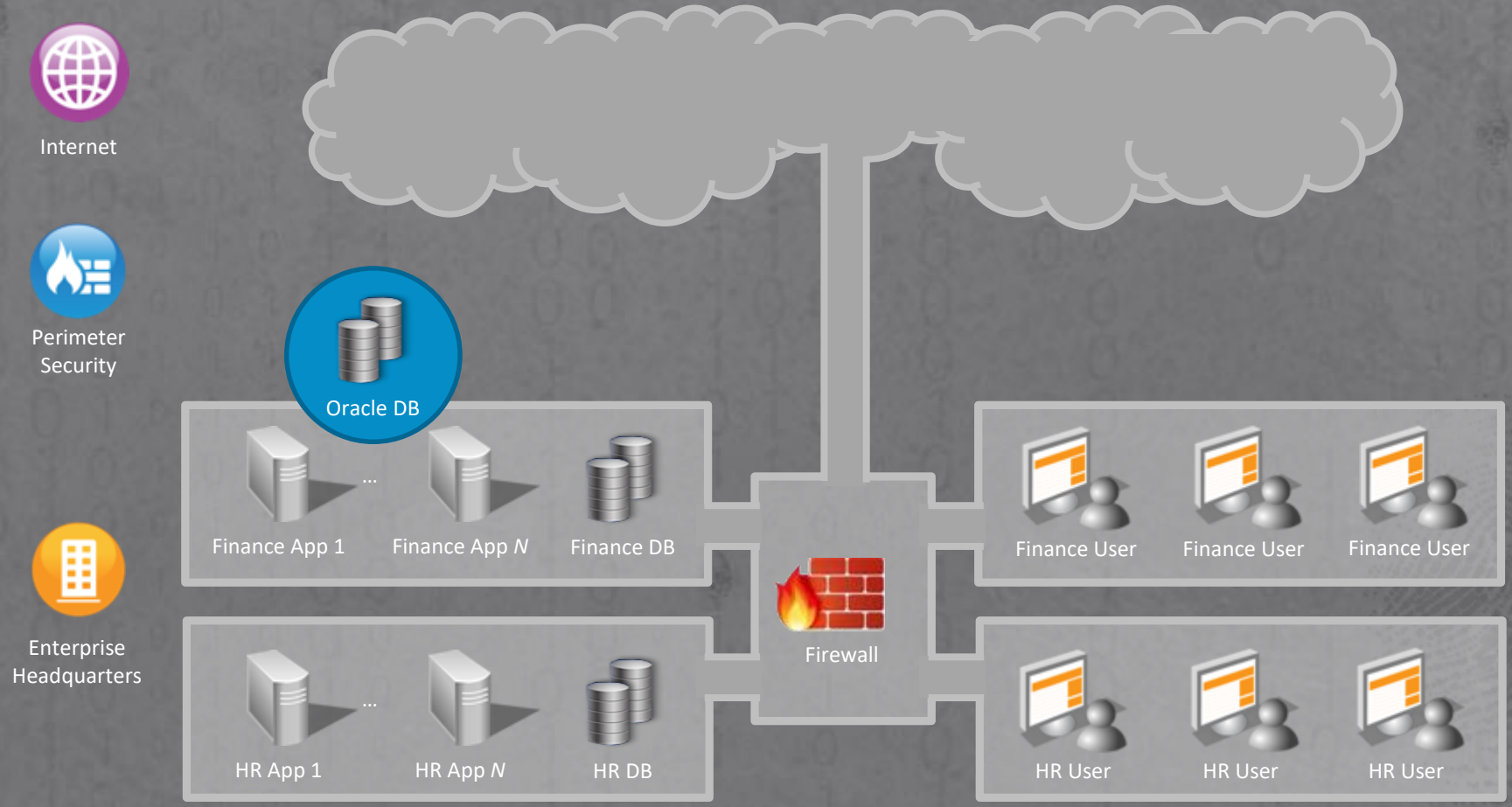
Zero Trust 1.0 – Micro-Segmentation



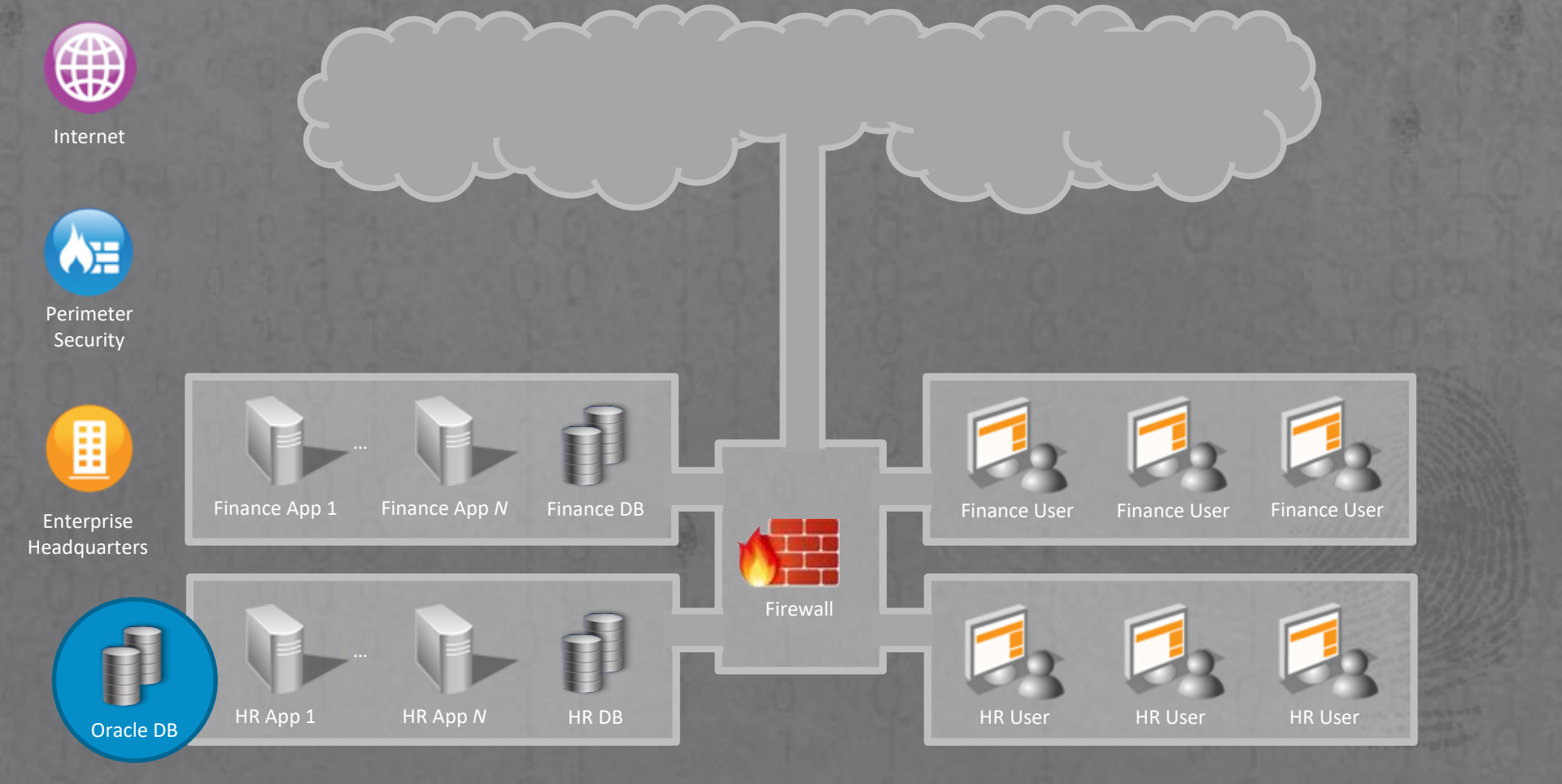
Zero Trust 1.0 – Micro-Segmentation



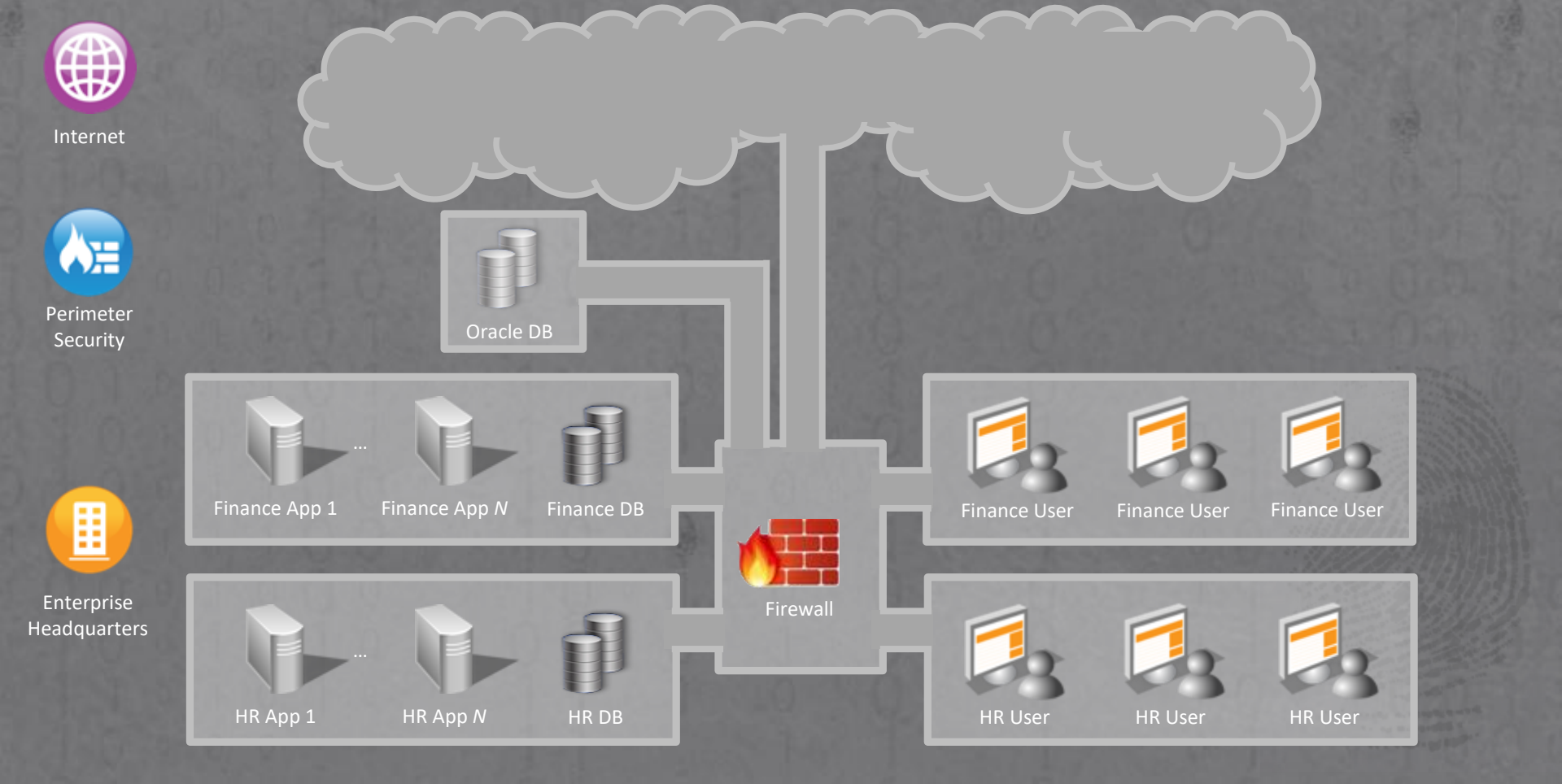
Zero Trust 1.0 – Micro-Segmentation



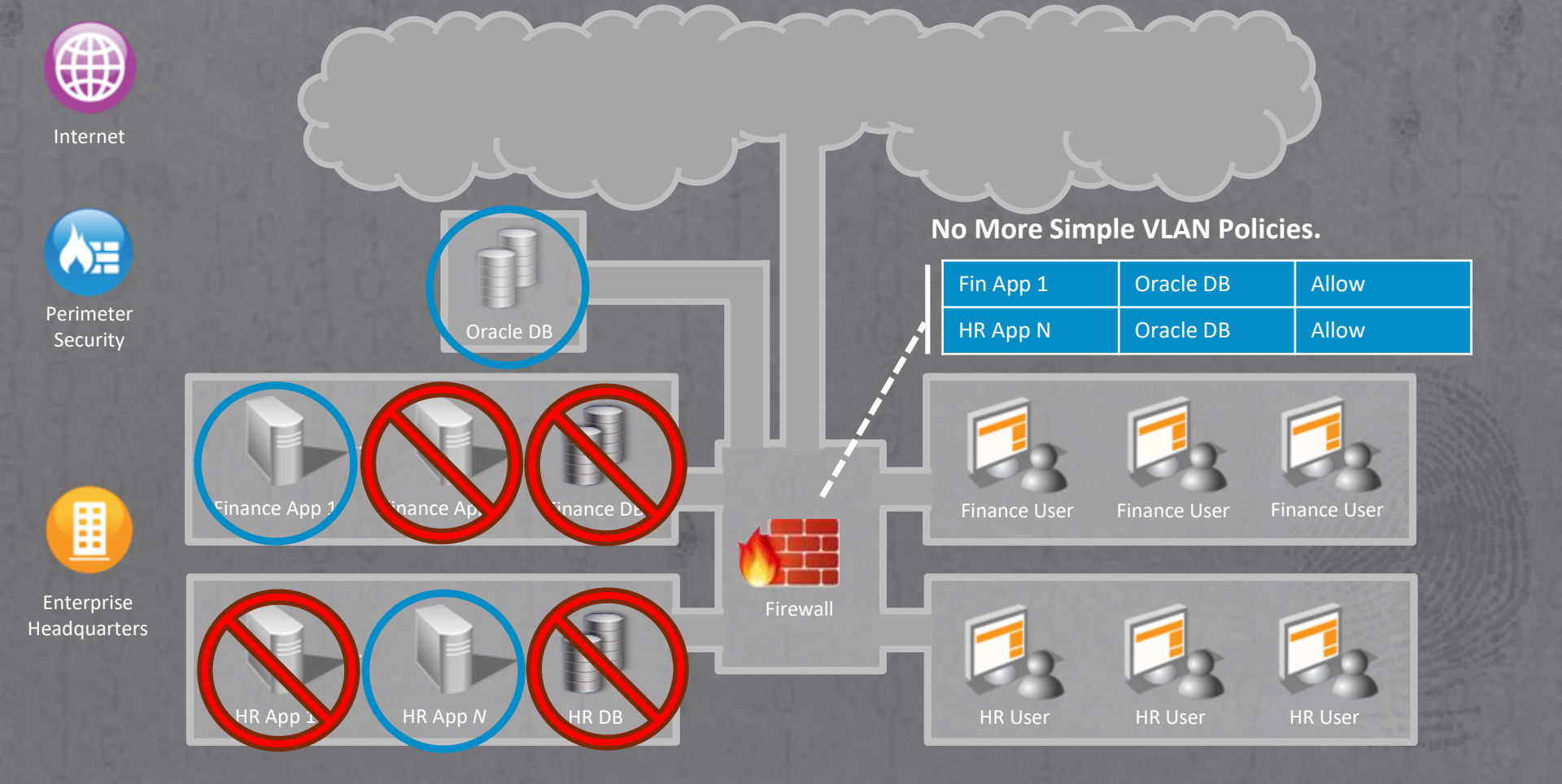
Zero Trust 1.0 – Micro-Segmentation



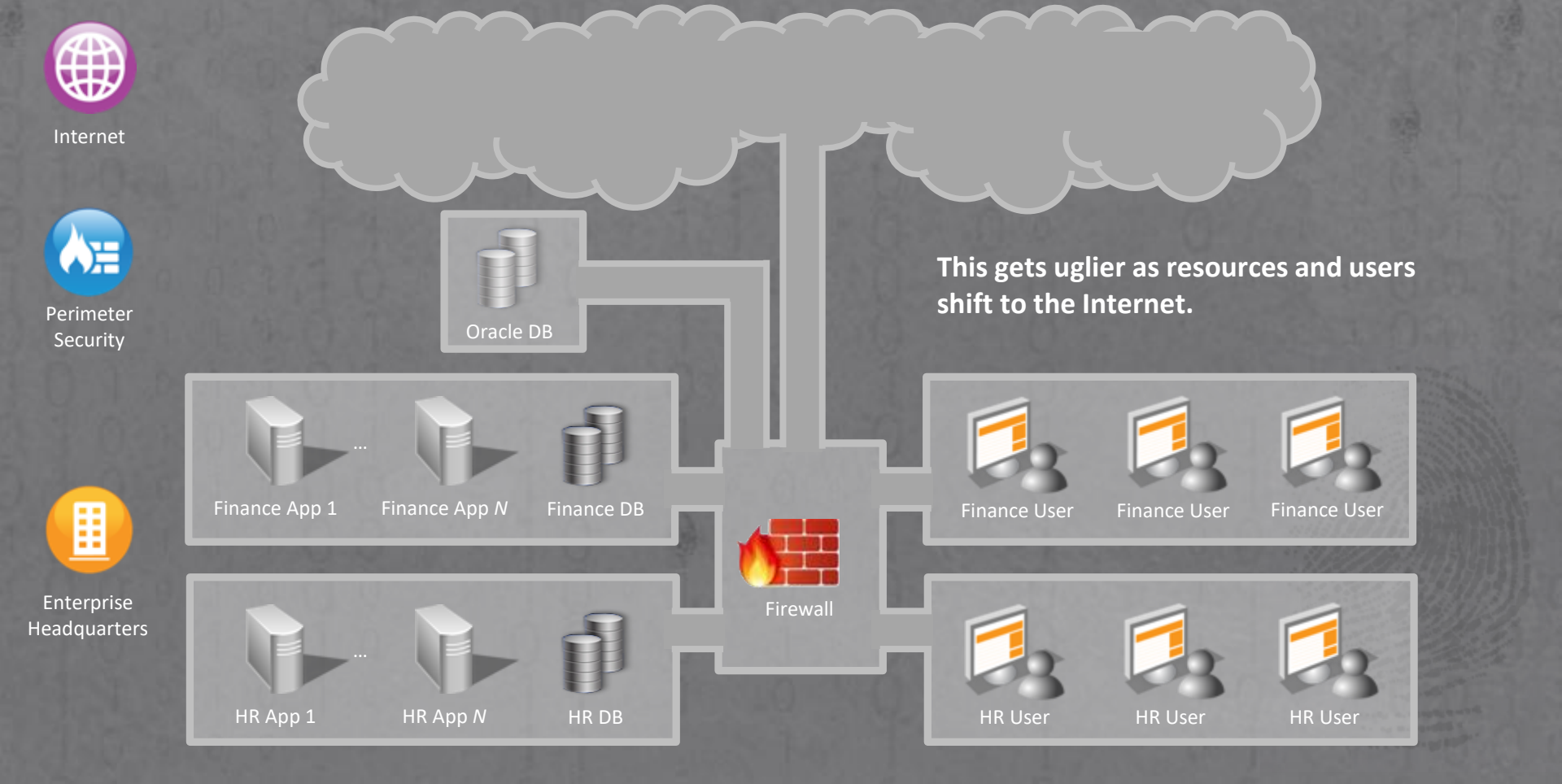
Zero Trust 1.0 – Micro-Segmentation



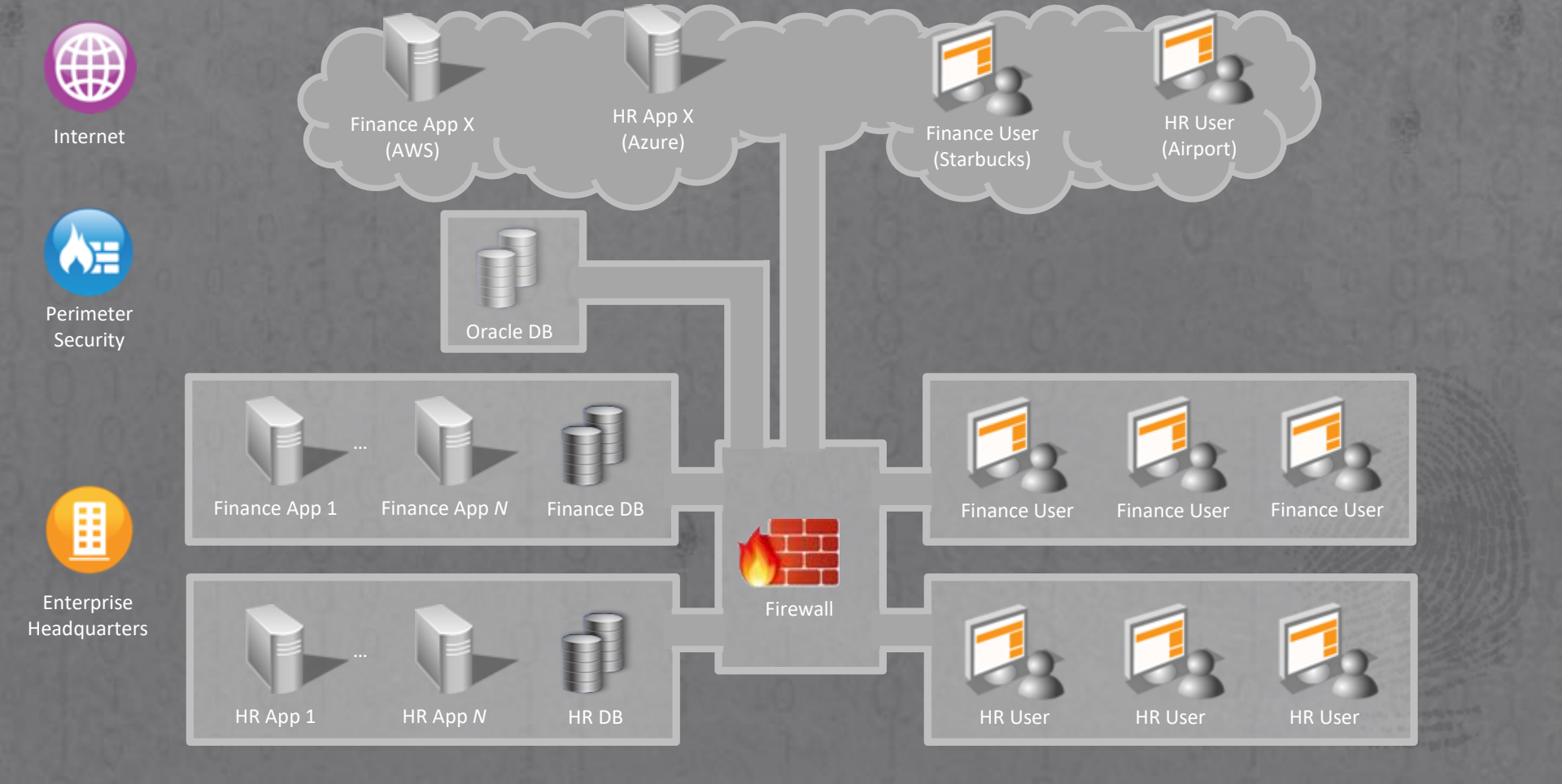
Zero Trust 1.0 – Micro-Segmentation



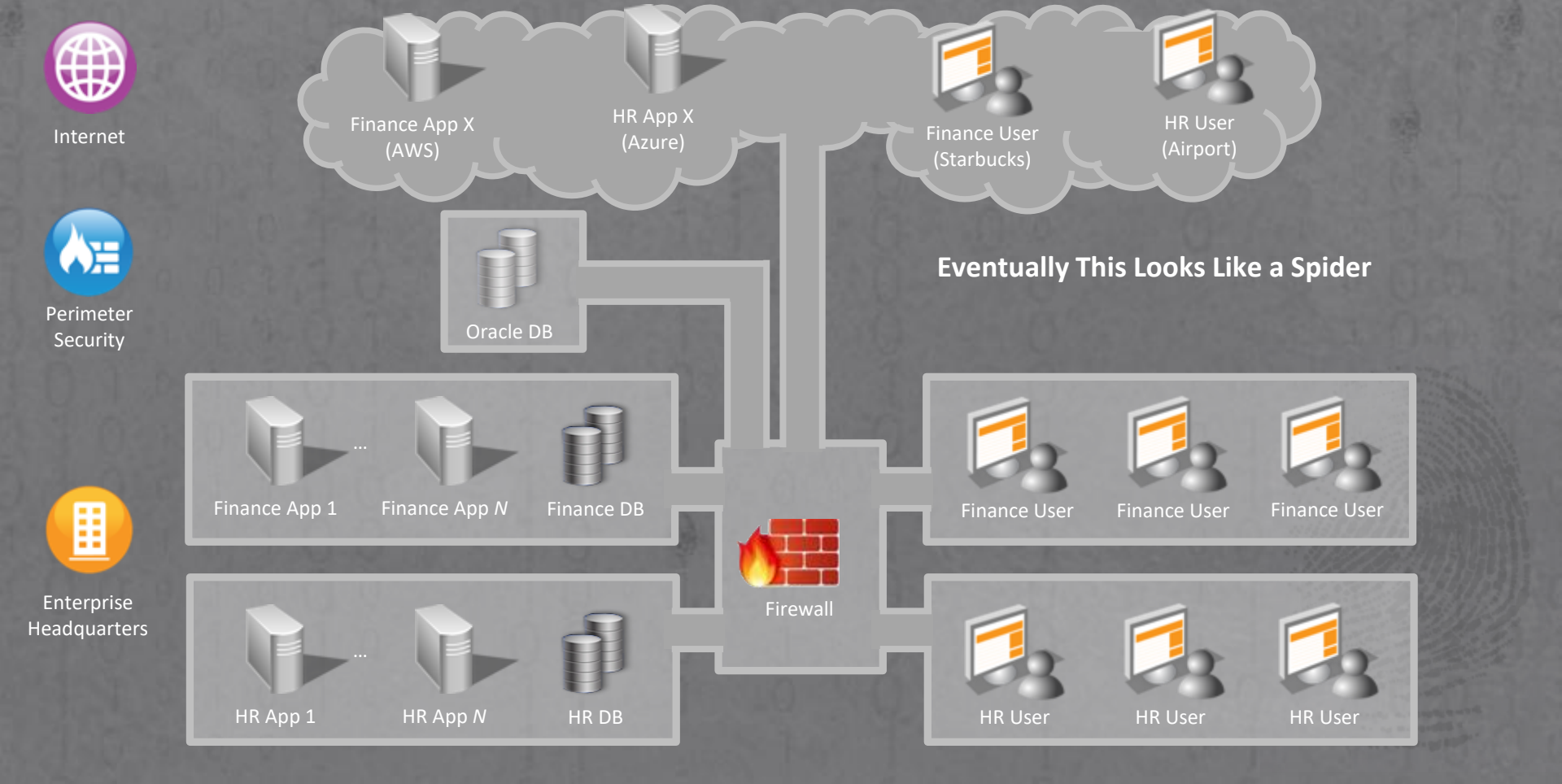
Zero Trust 1.0 – Micro-Segmentation



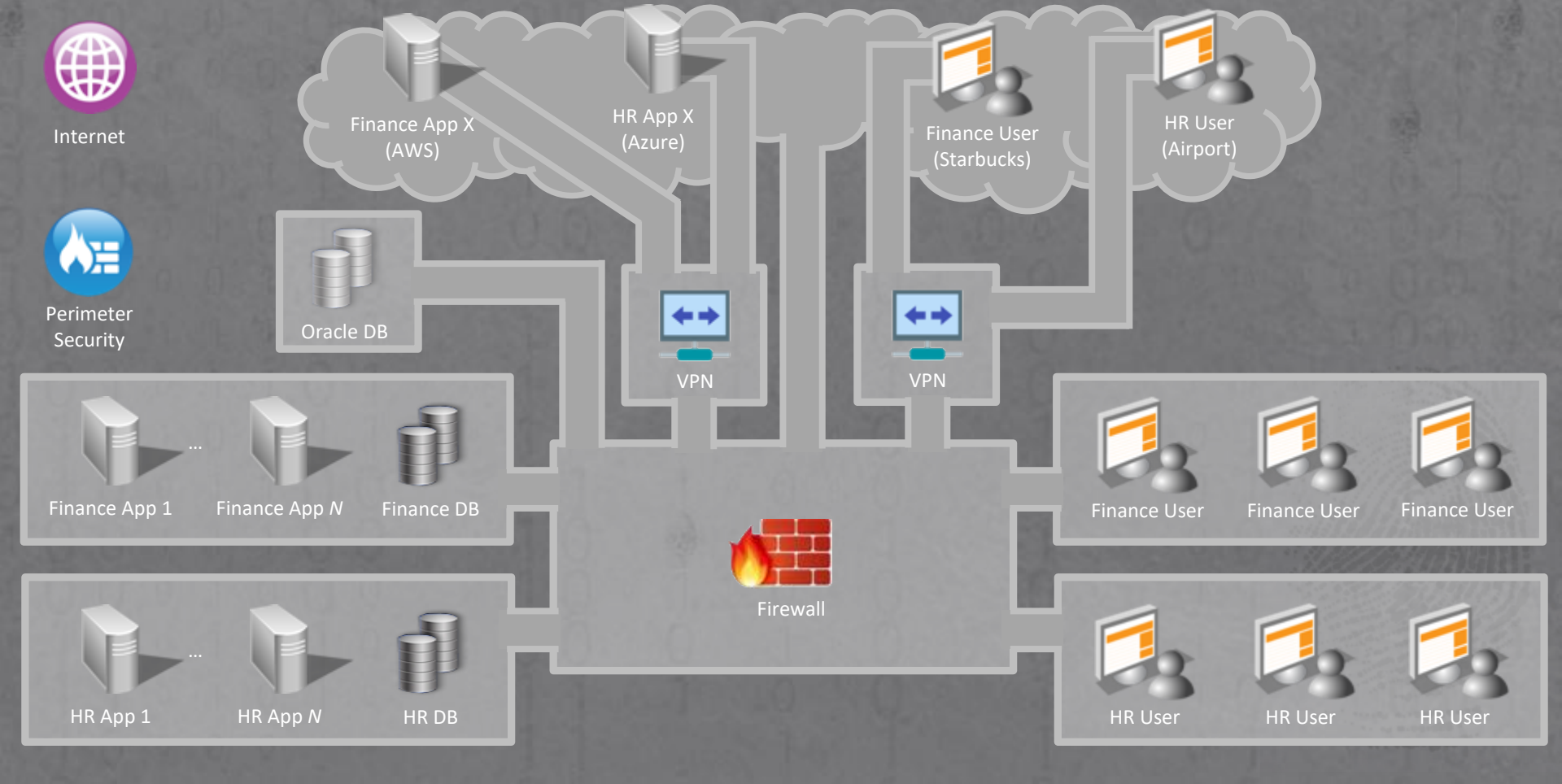
Zero Trust 1.0 – Micro-Segmentation



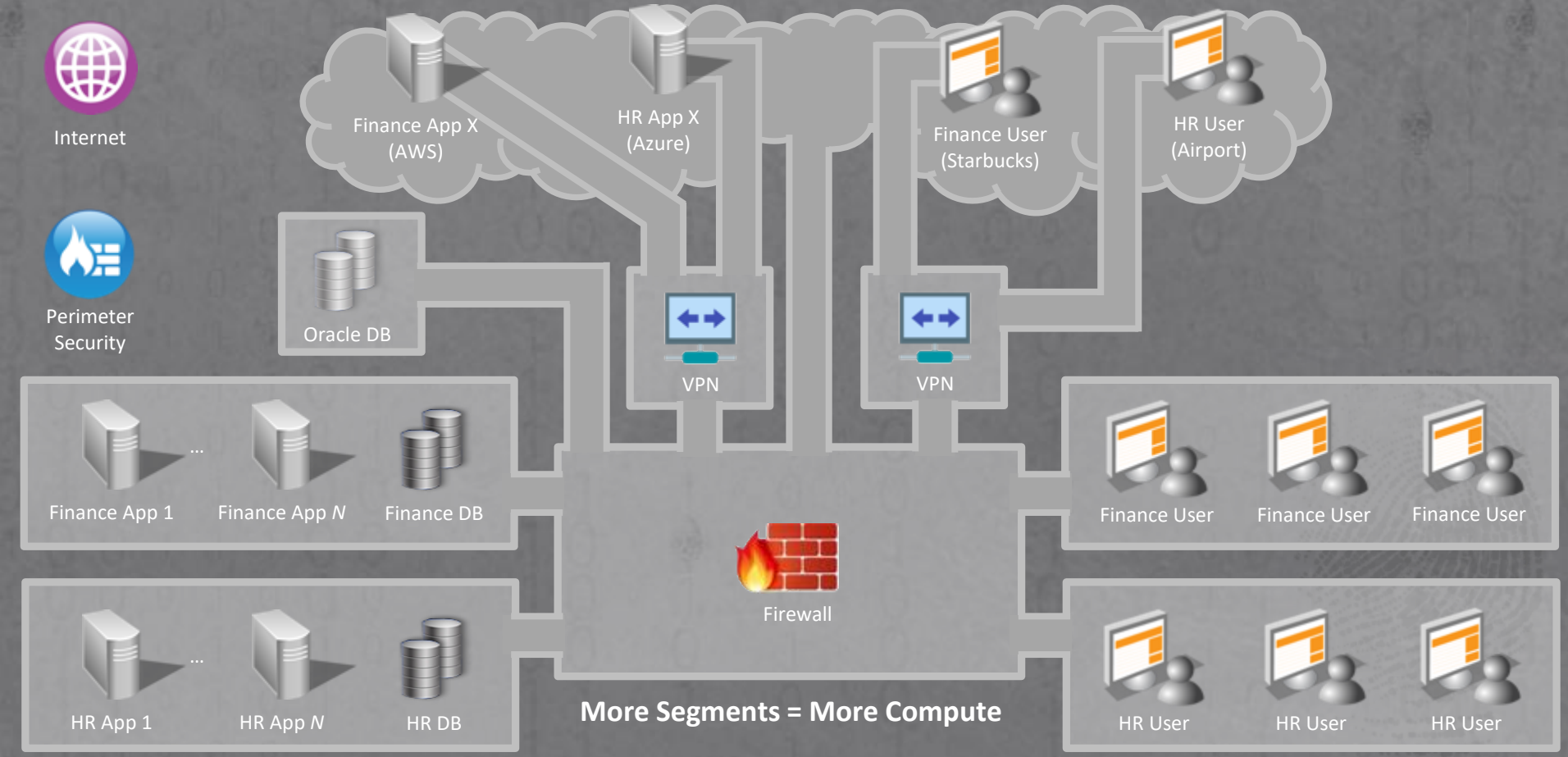
Zero Trust 1.0 – Micro-Segmentation



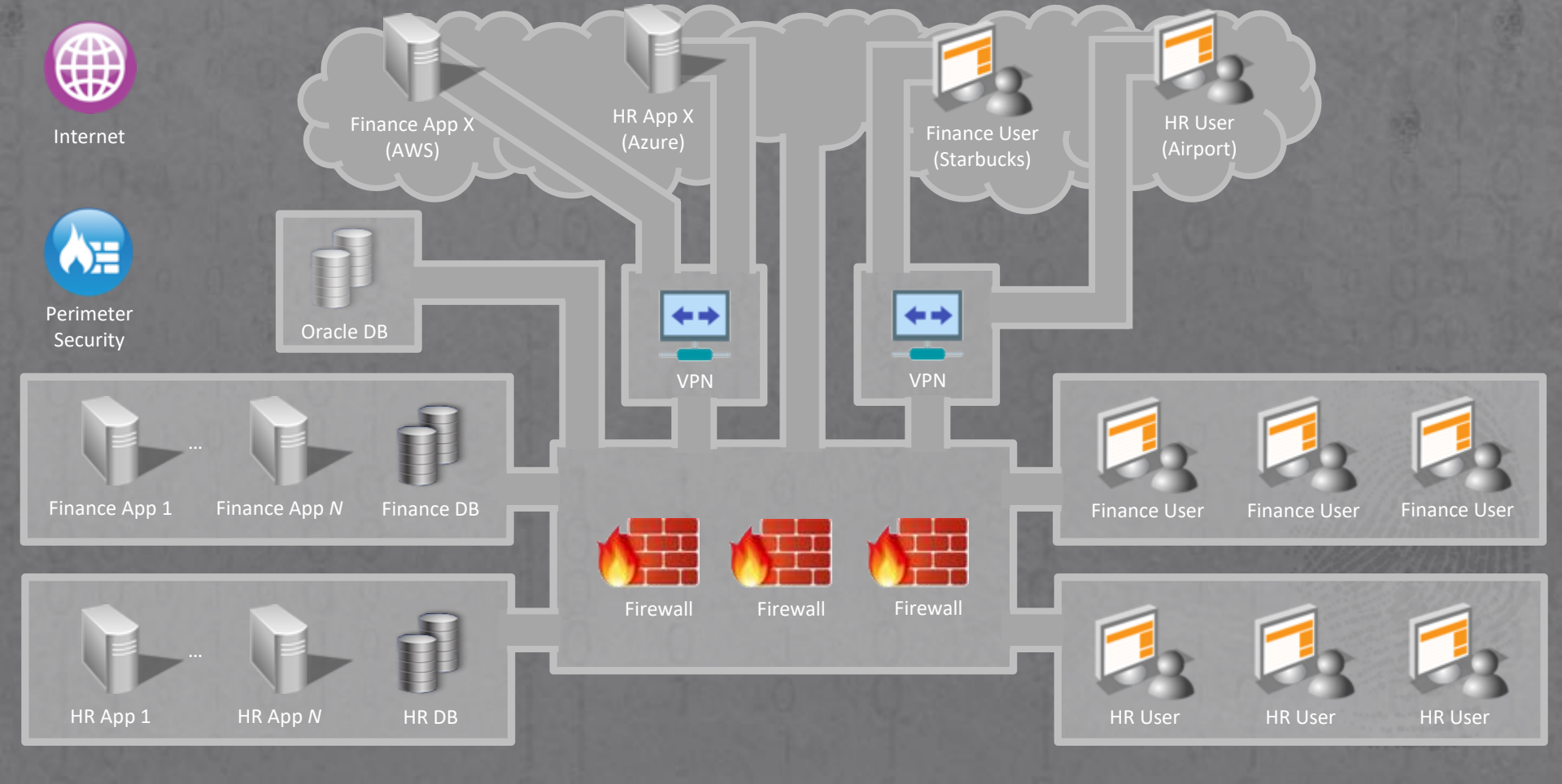
Zero Trust 1.0 – Micro-Segmentation



Zero Trust 1.0 – Micro-Segmentation



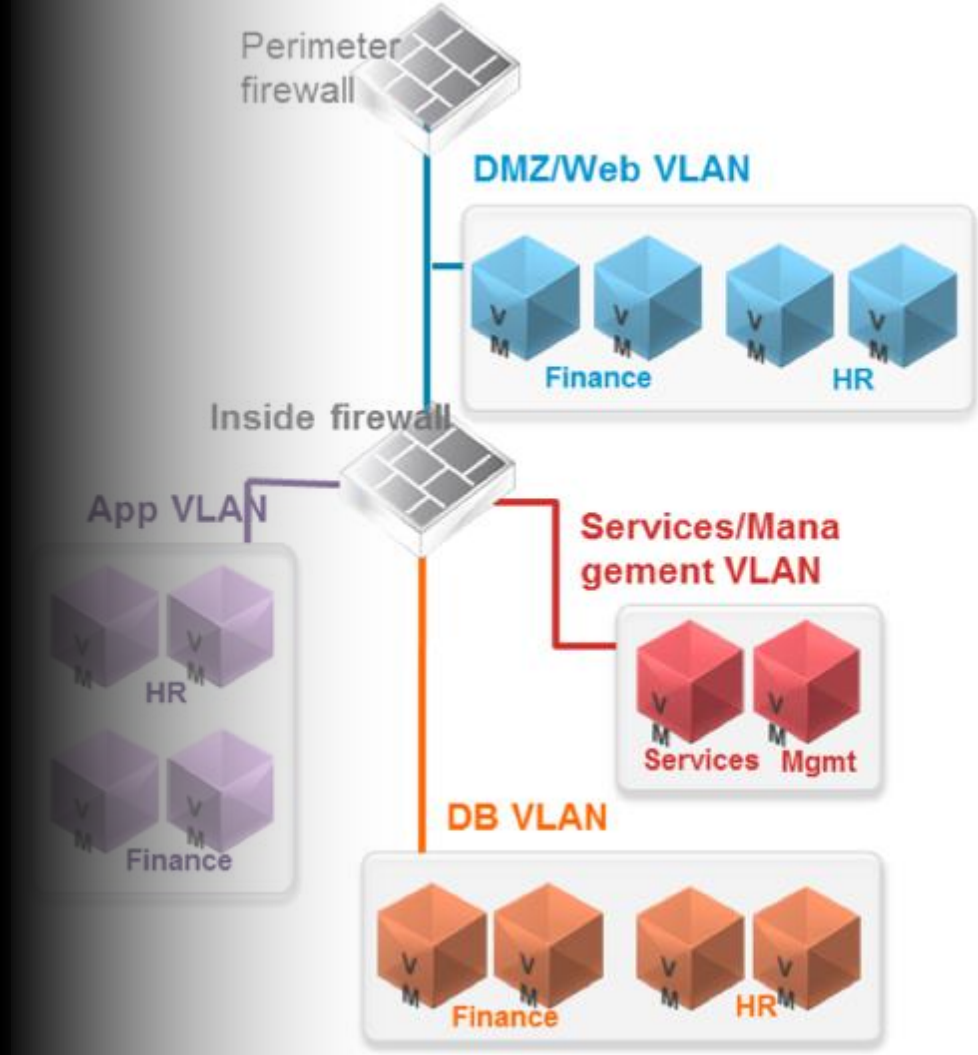
Zero Trust 1.0 – Micro-Segmentation



Things Get Complicated

VERY FAST

- Shared Infrastructure
- High Touch Points
- IaaS App Movement
- Mobile Workforce
- Maintenance



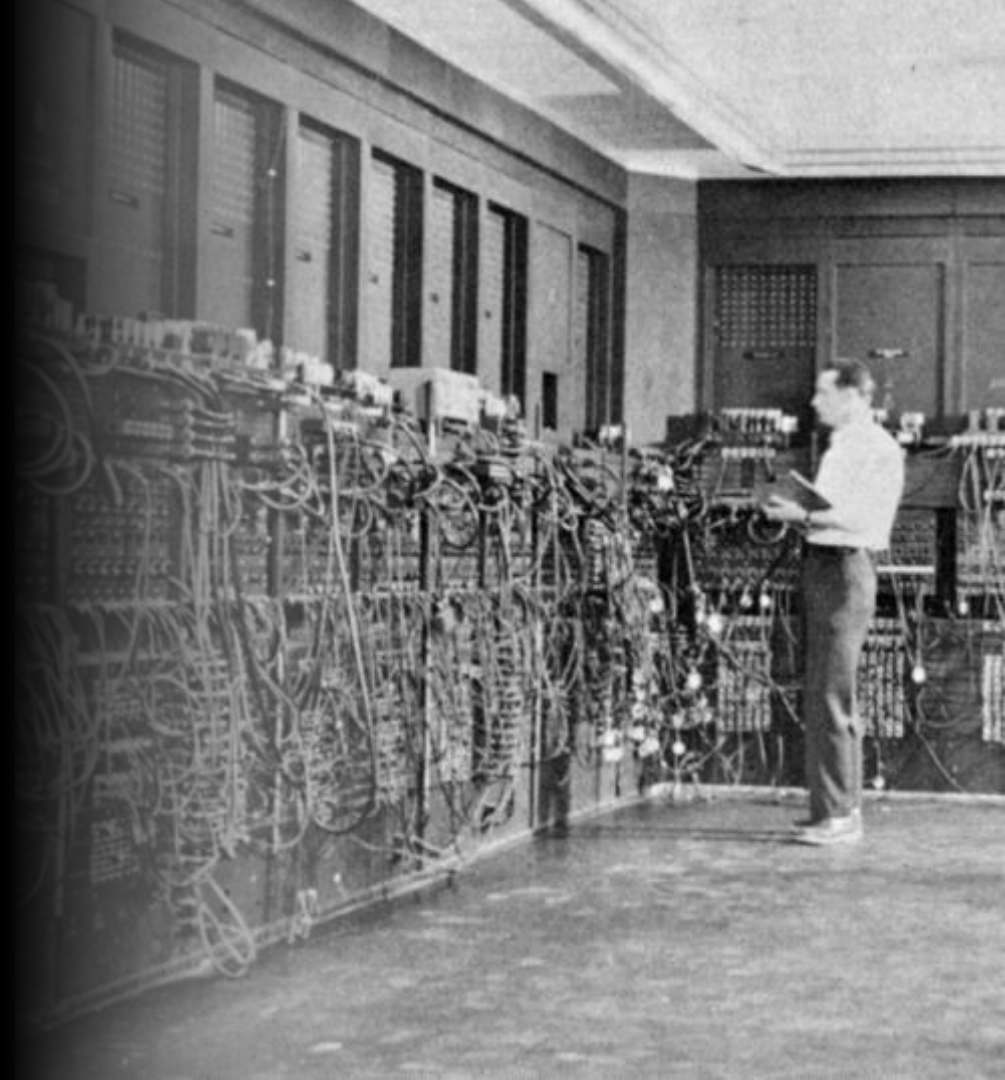
Implementation

VERY HARD

Security

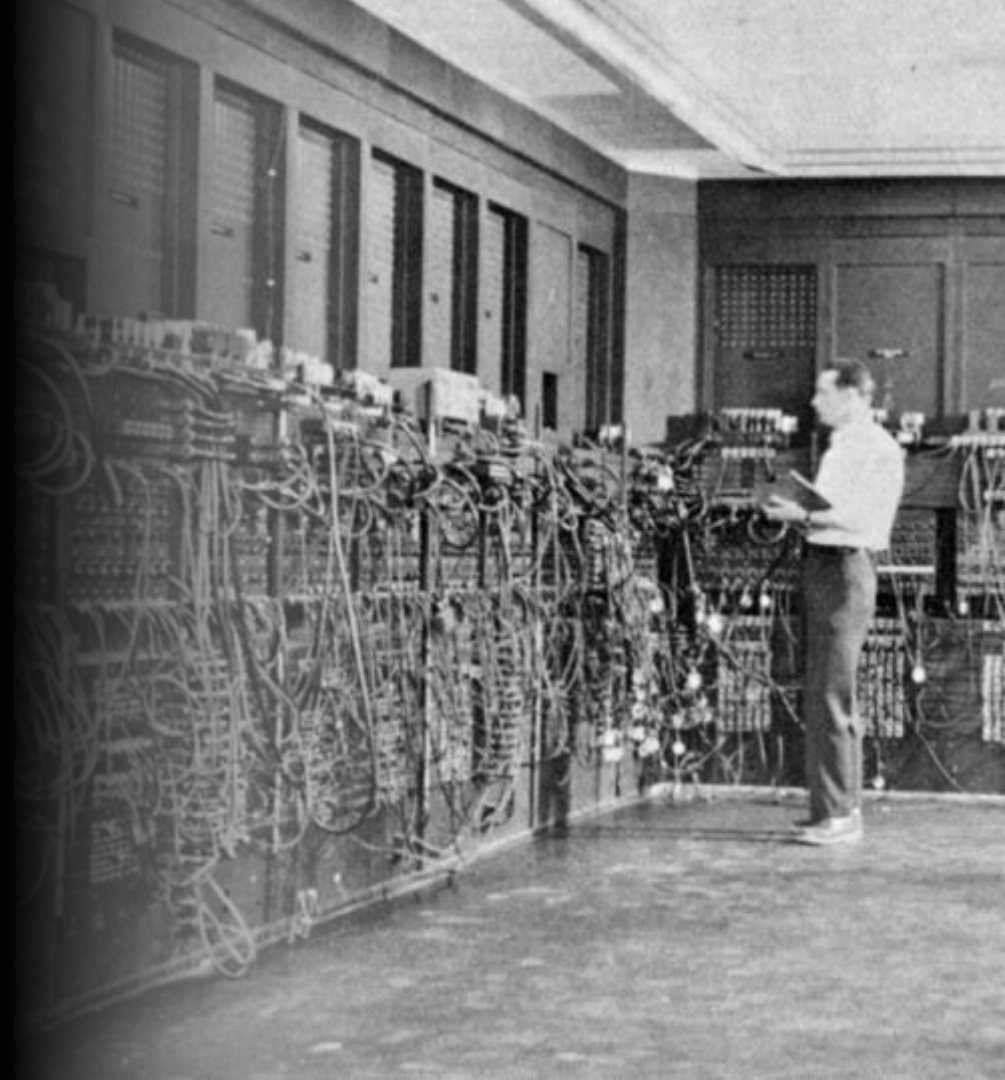
proportional to

Complexity



Is there a

BETTER WAY?



ZERO TRUST 2.0

Move identity and access to the Internet.

No perimeter. Users can live anywhere.

Everything is strongly authenticated.

Eliminate network based access.

Google BeyondCorp

RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: TECH-T11

BeyondCorp - How Google Protects Its Corporate Security Perimeter without Firewalls

Heather Adkins
Director of Security
Google

Rory Ward
Site Reliability Engineering Man
Google

Our Six Year Mission

To have **every** Google employee

work successfully from **untrusted networks**

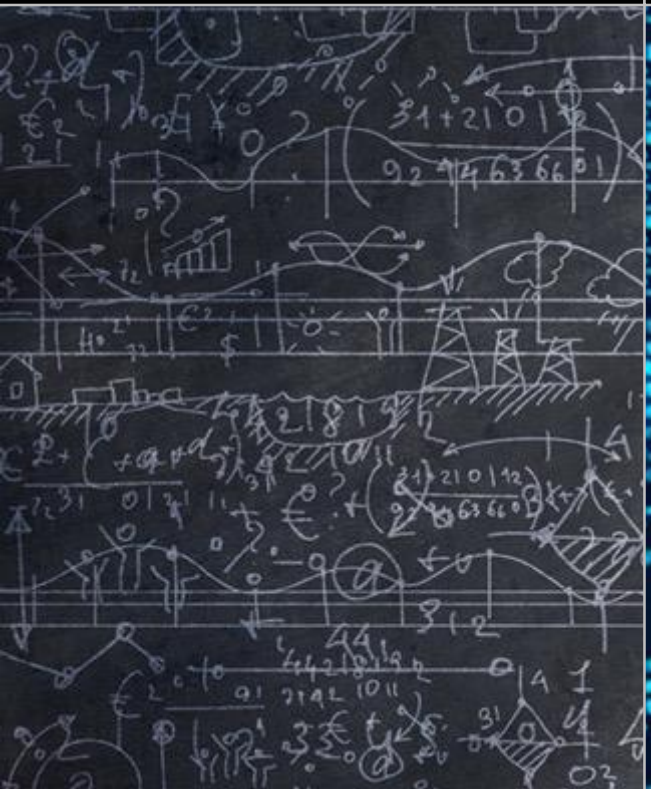
without use of a **VPN**.

RSAConference2017

Applying BeyondCorp

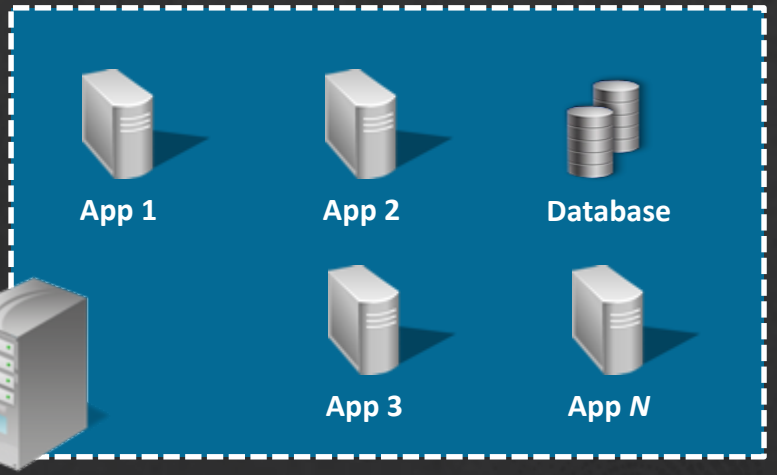
1. Have **zero trust** in your network.
2. Base **all** access decisions on **what you know** about the user and their device.

Google BeyondCorp

Decouple Complexity	Distribute Ops	Self Remediation
		

Google BeyondCorp

Managed Laptop with Agent and Certificate *X*



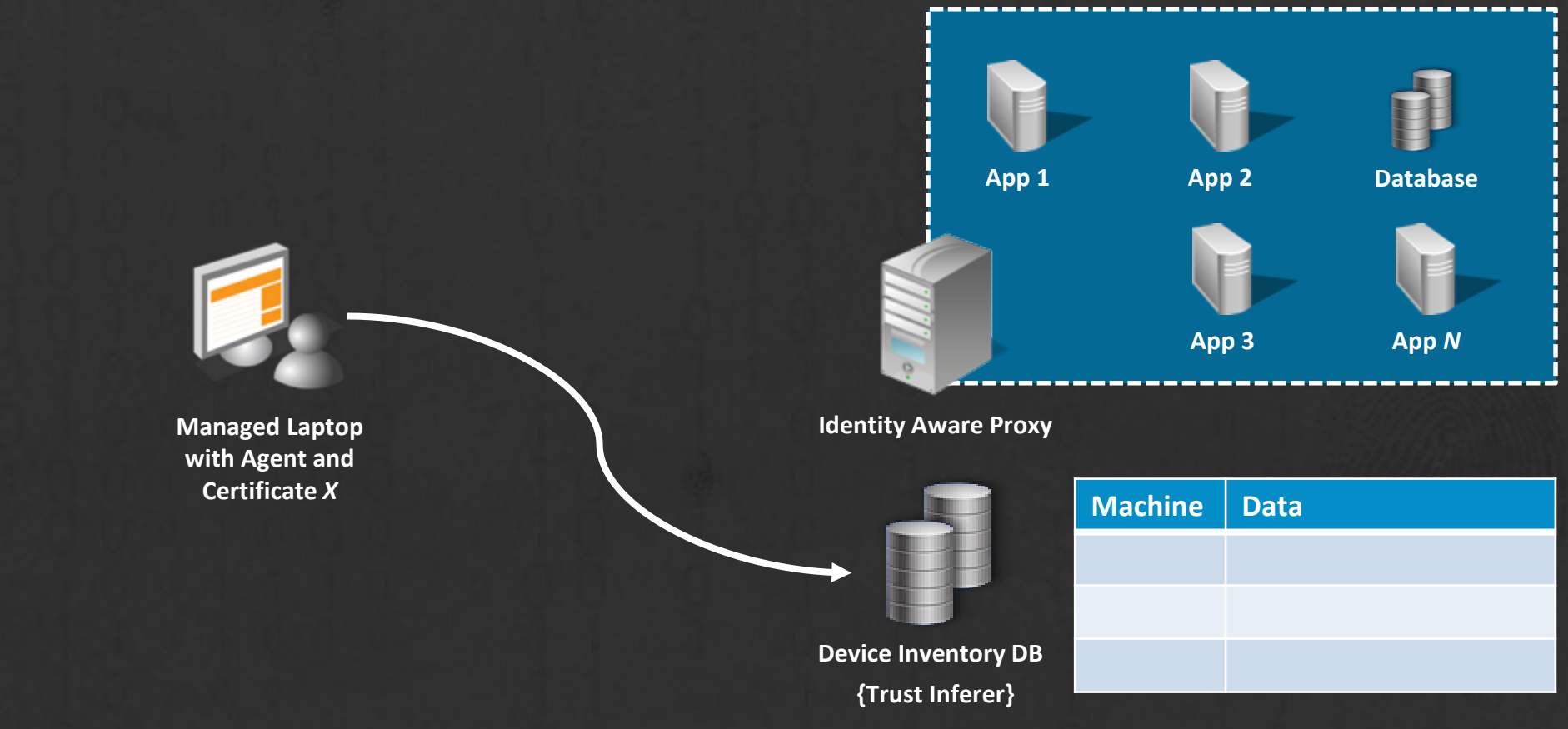
Identity Aware Proxy

Device Inventory DB

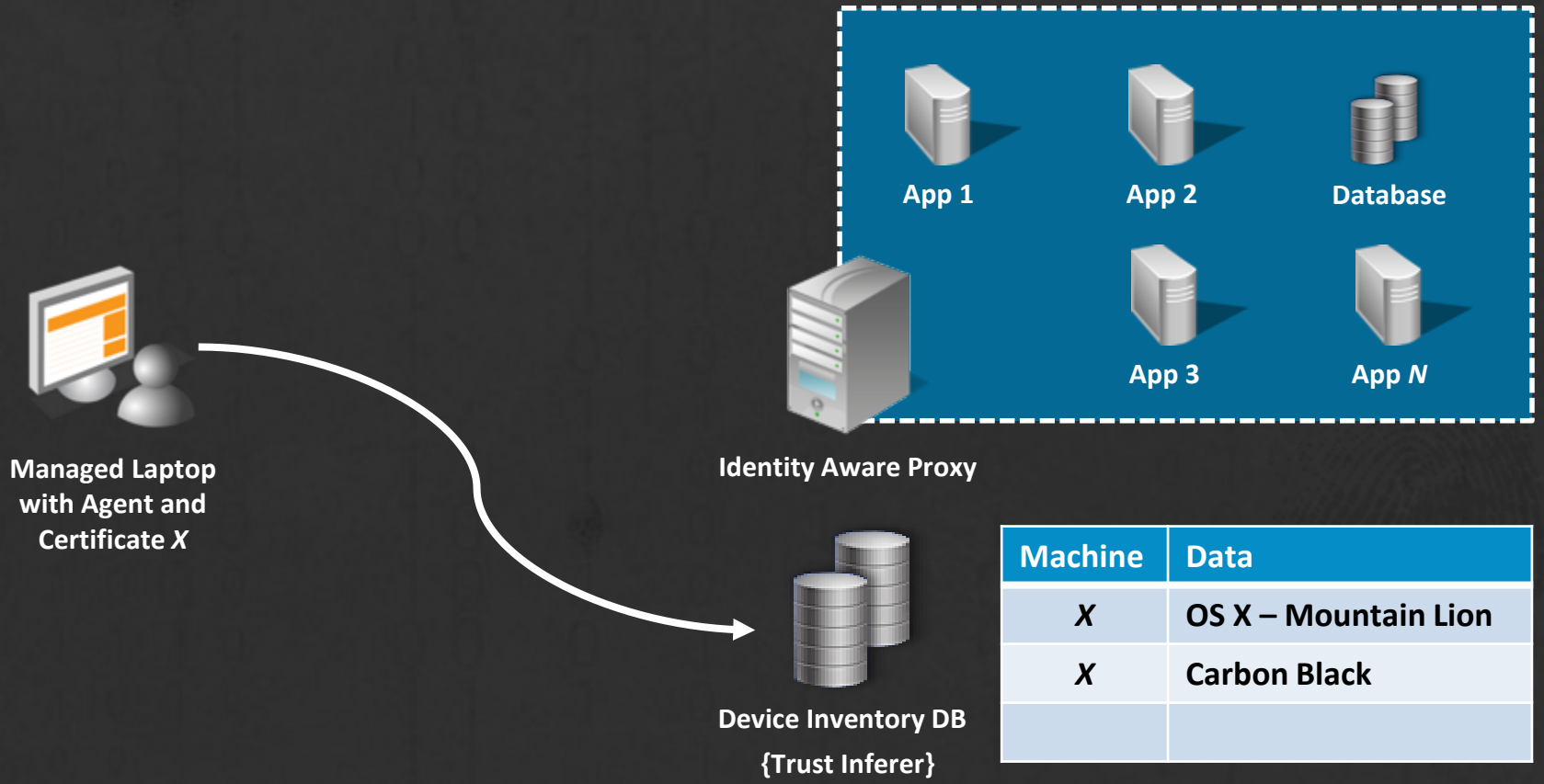
{Trust Inferer}

Machine	Data

Google BeyondCorp



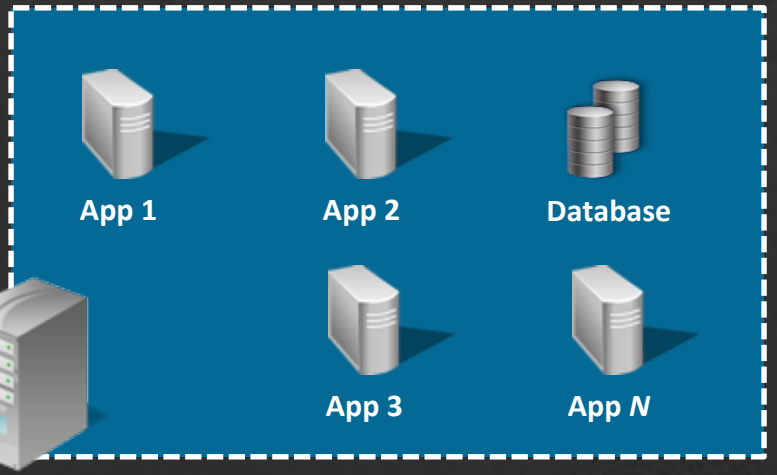
Google BeyondCorp



Machine	Data
X	OS X – Mountain Lion
X	Carbon Black

Google BeyondCorp

Managed Laptop with Agent and Certificate *X*



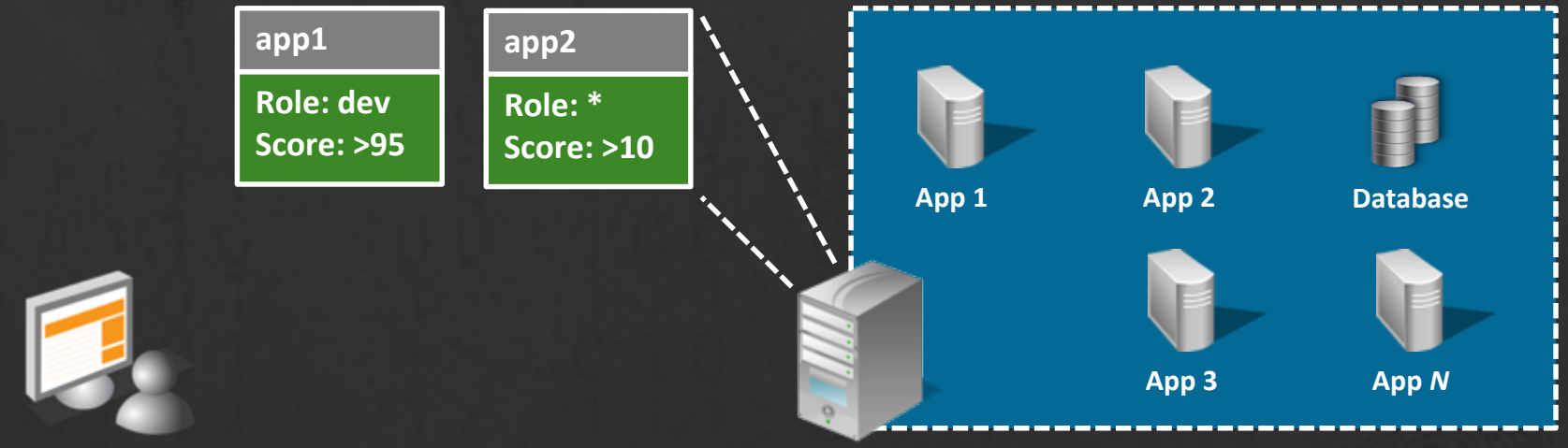
Identity Aware Proxy

Device Inventory DB

{Trust Inferer}

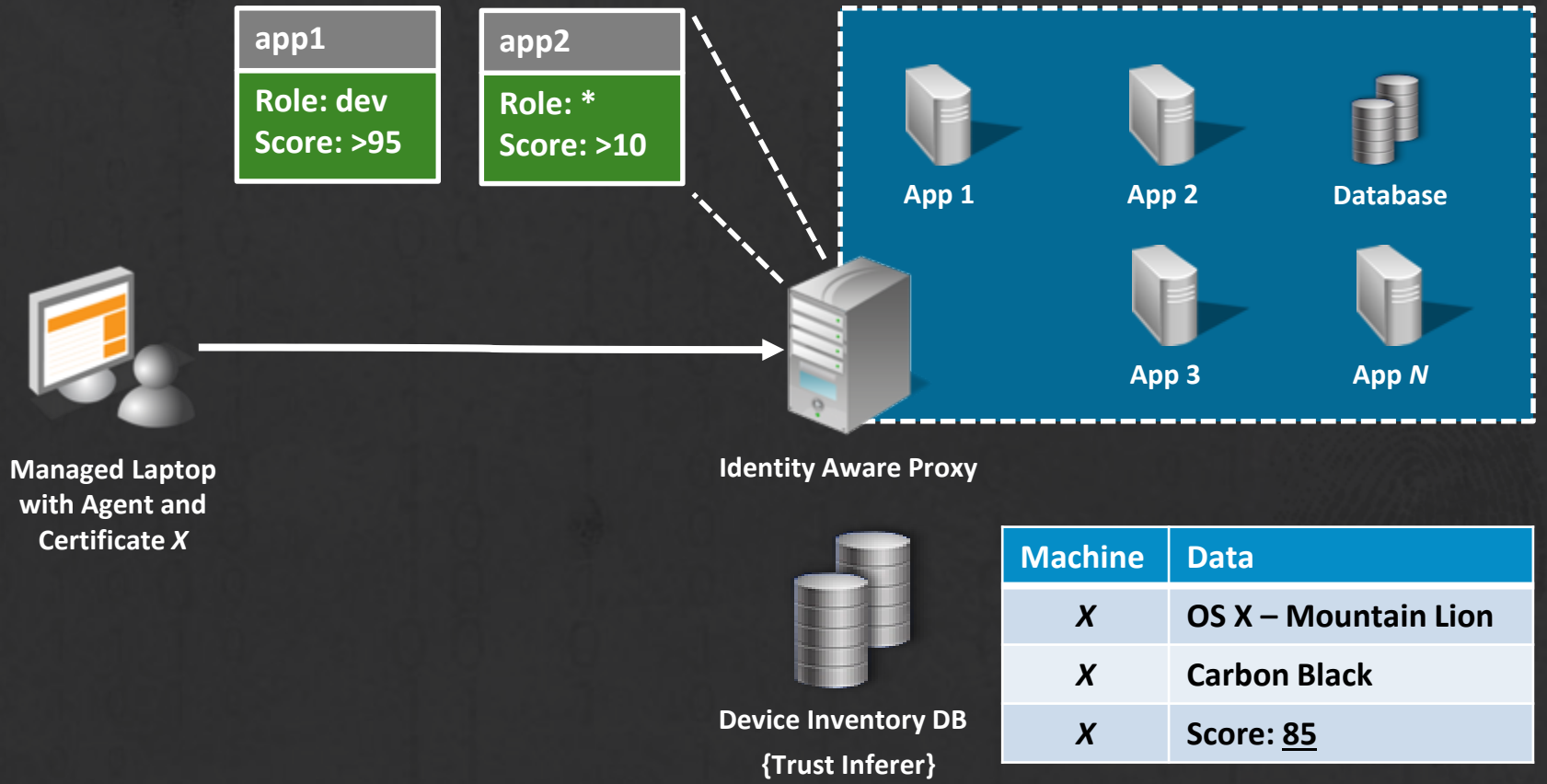
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



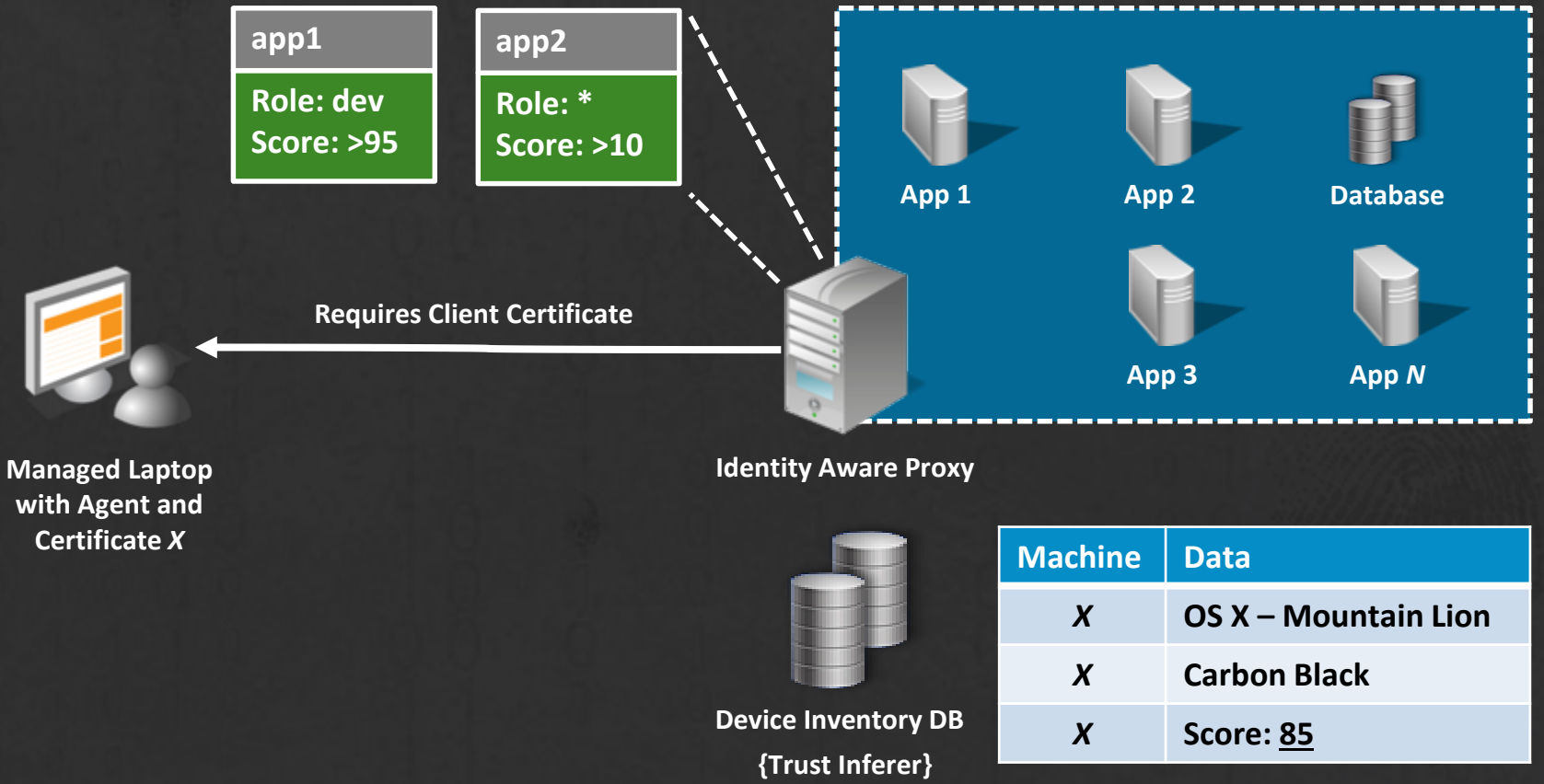
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



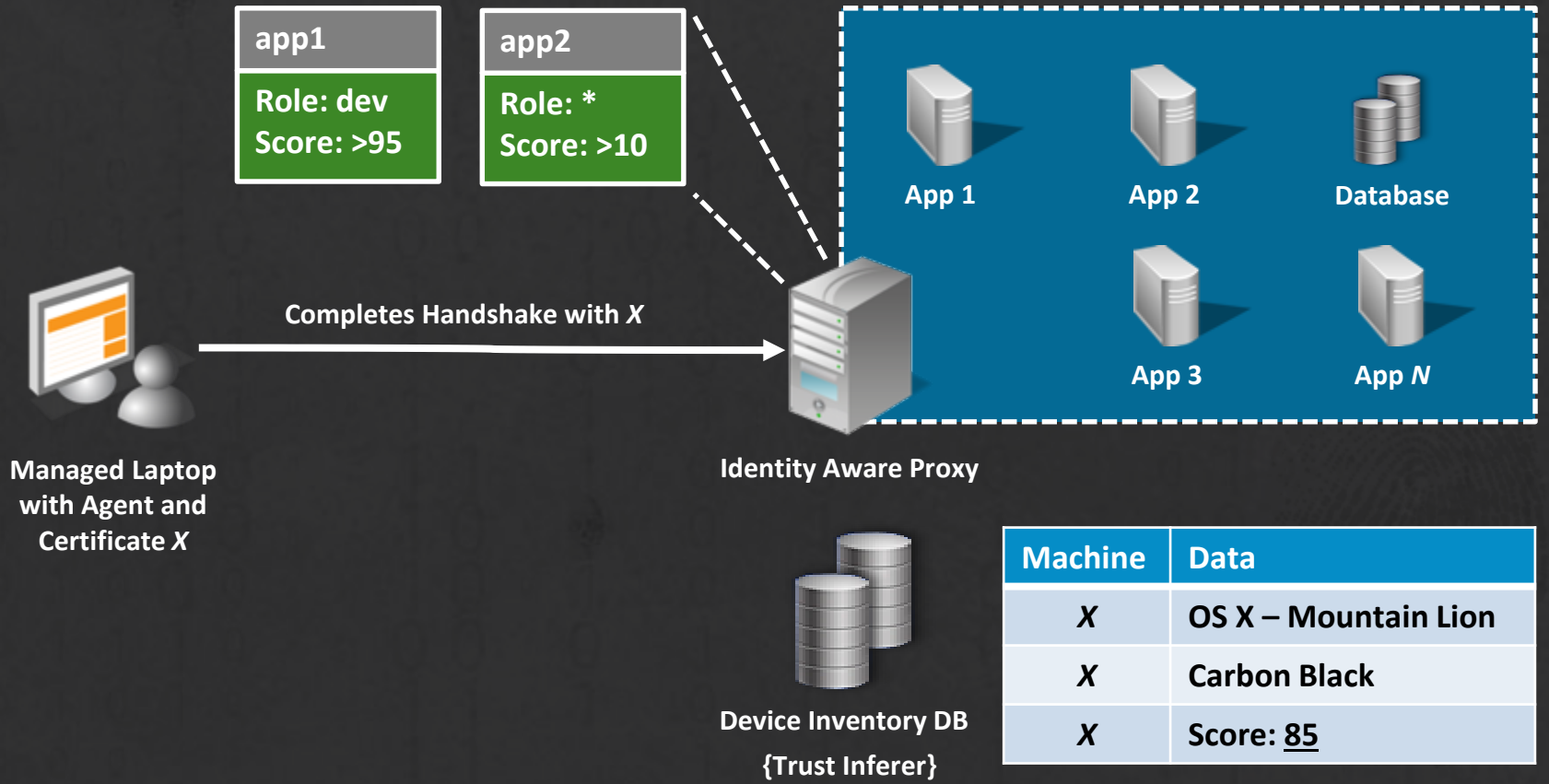
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



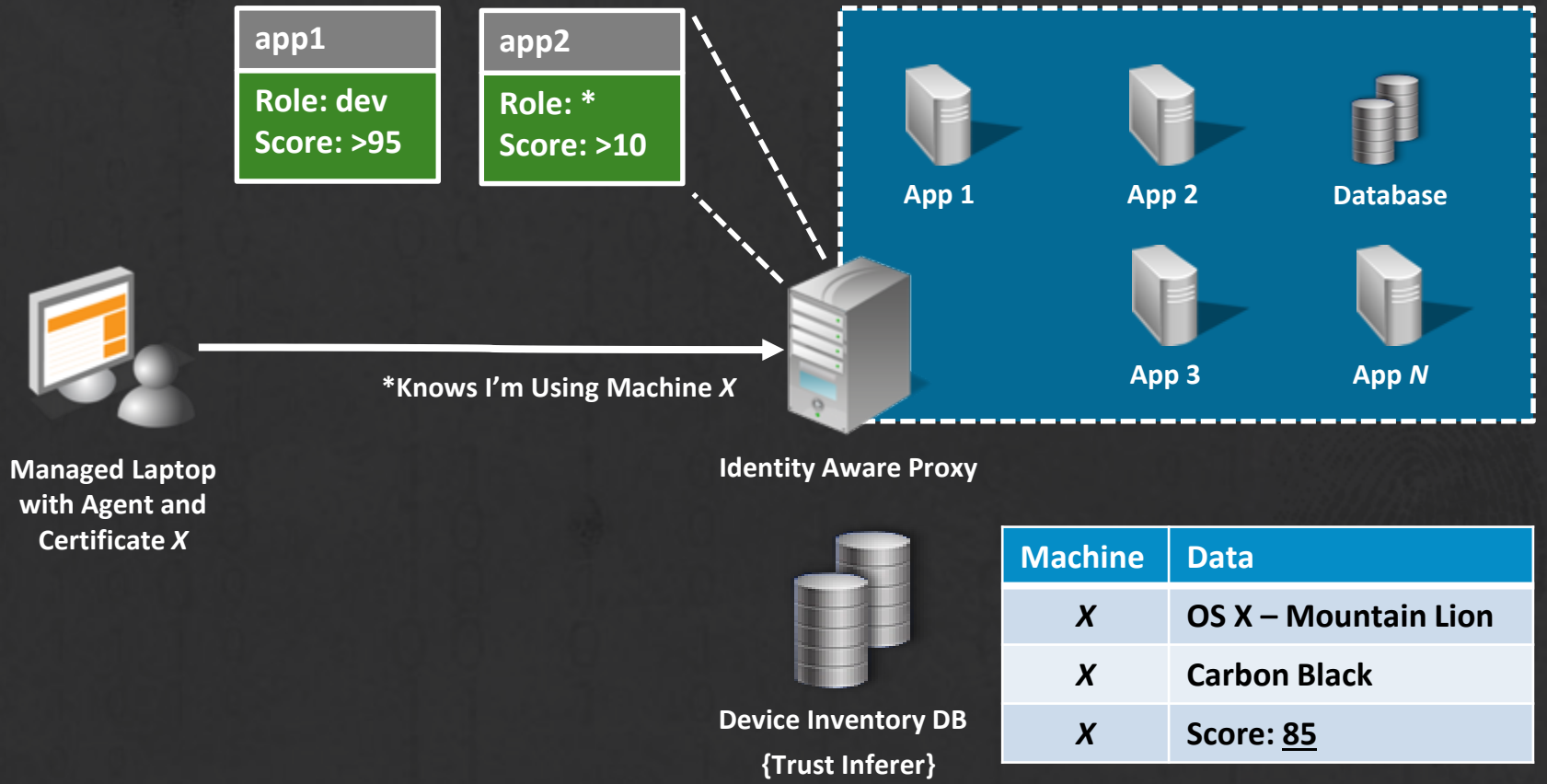
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



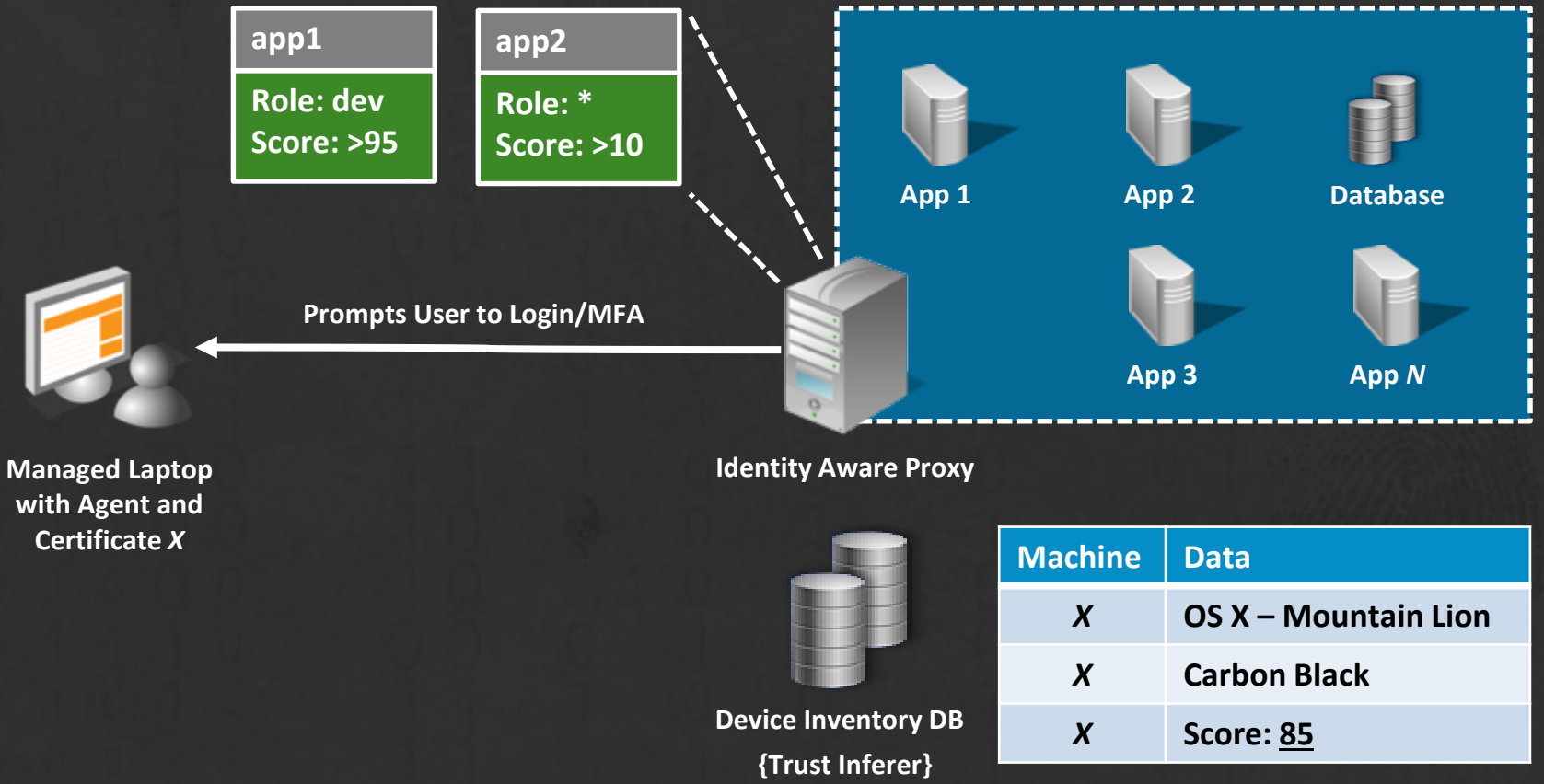
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



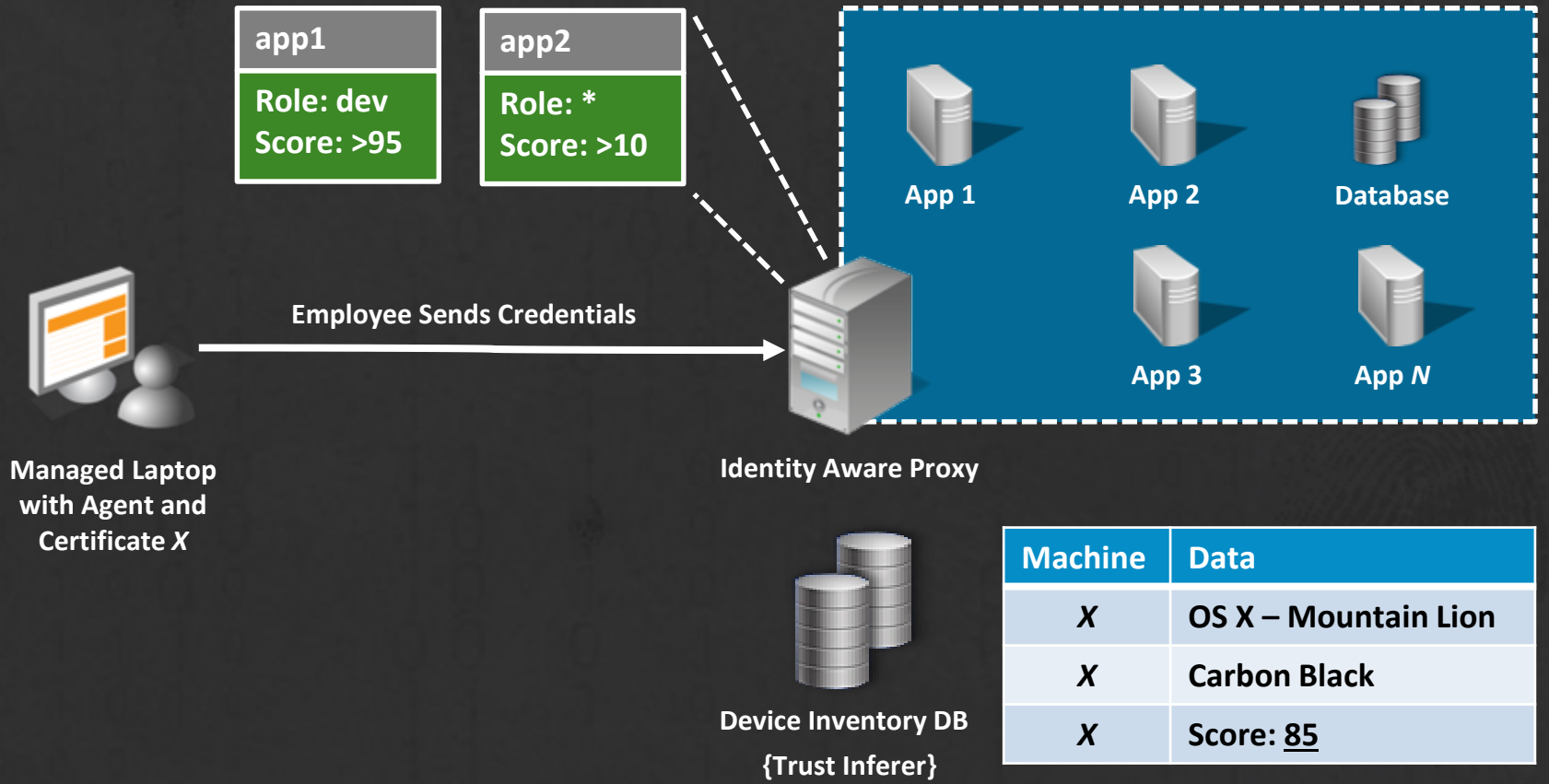
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



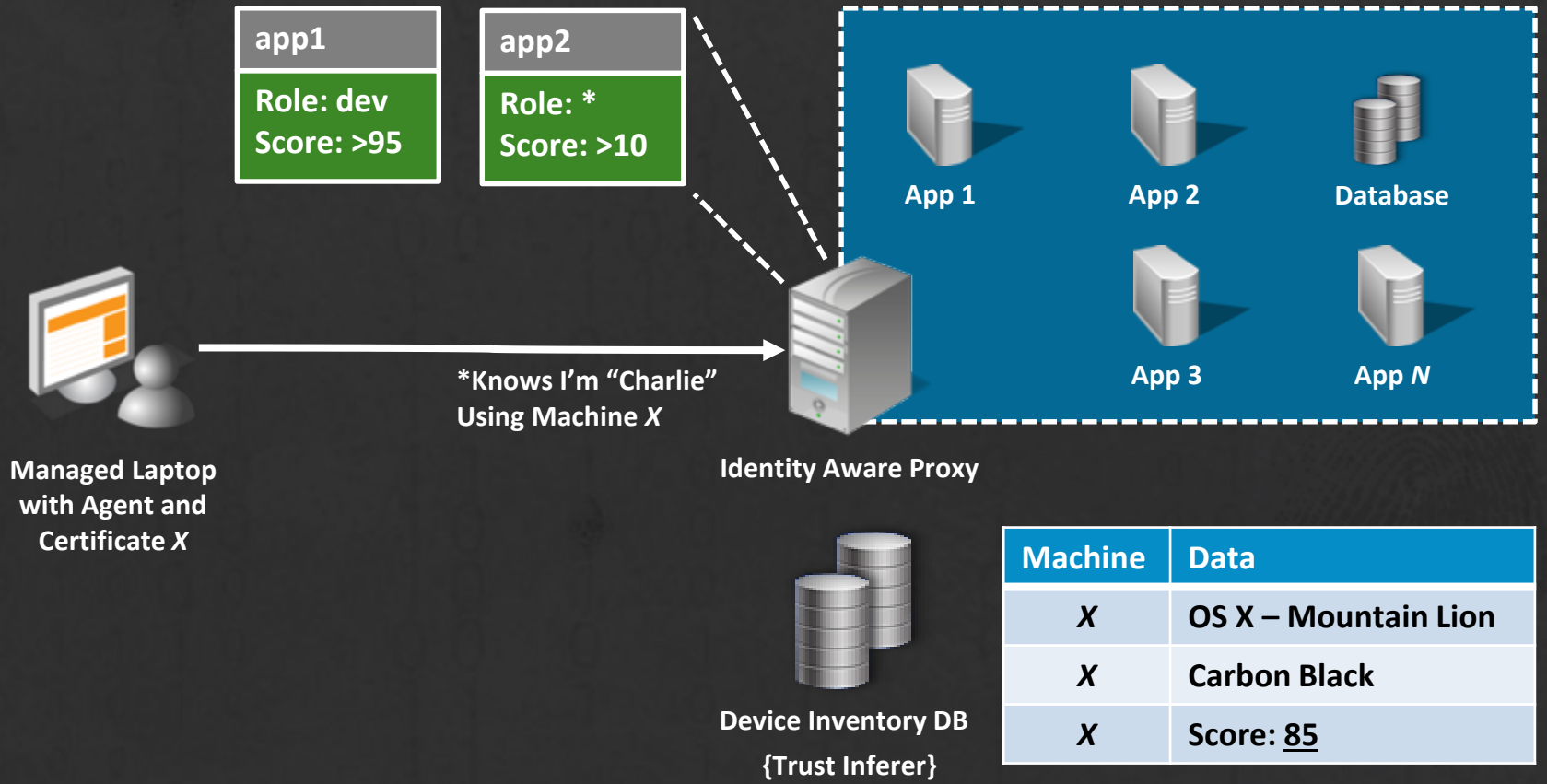
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



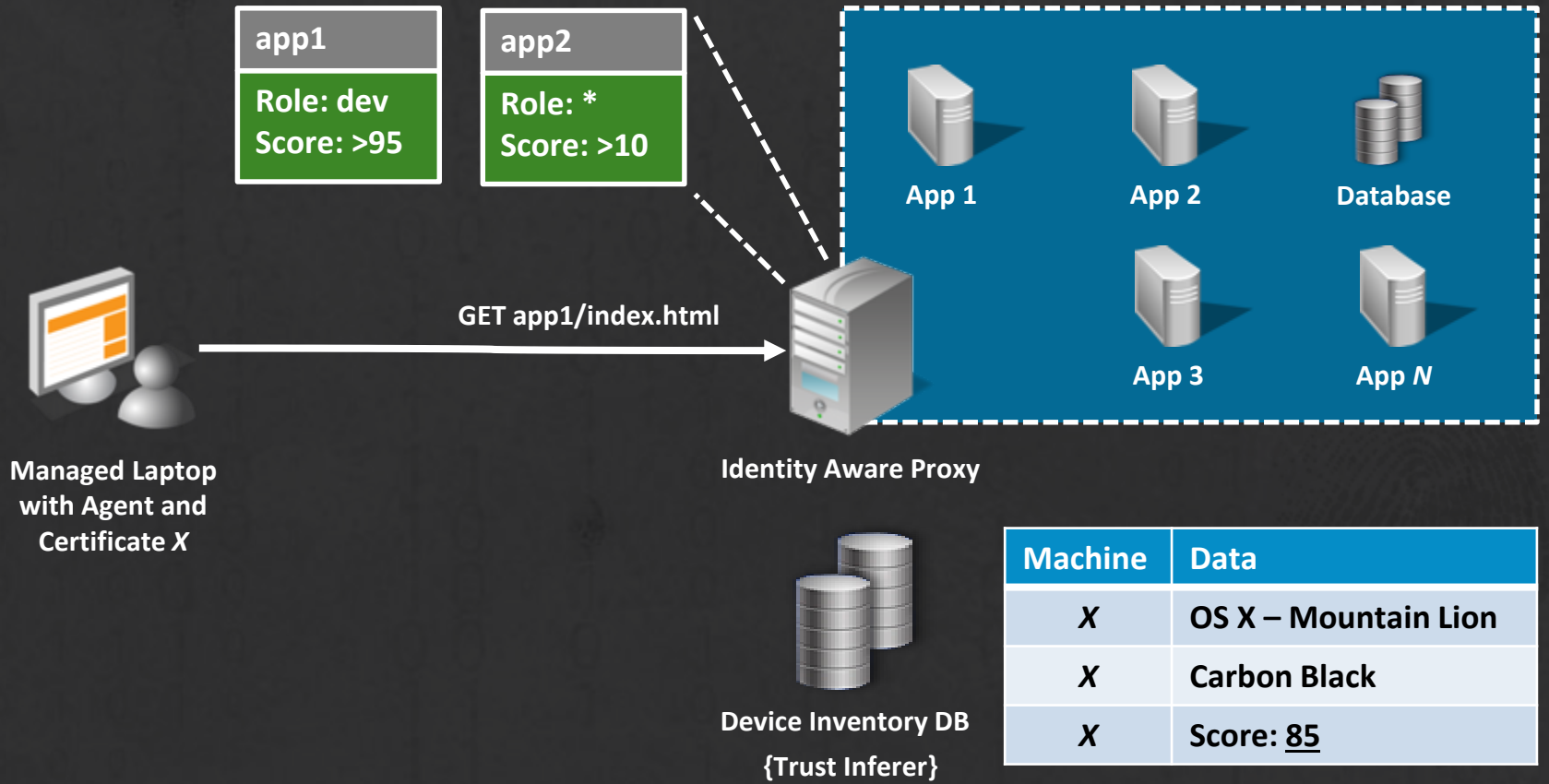
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



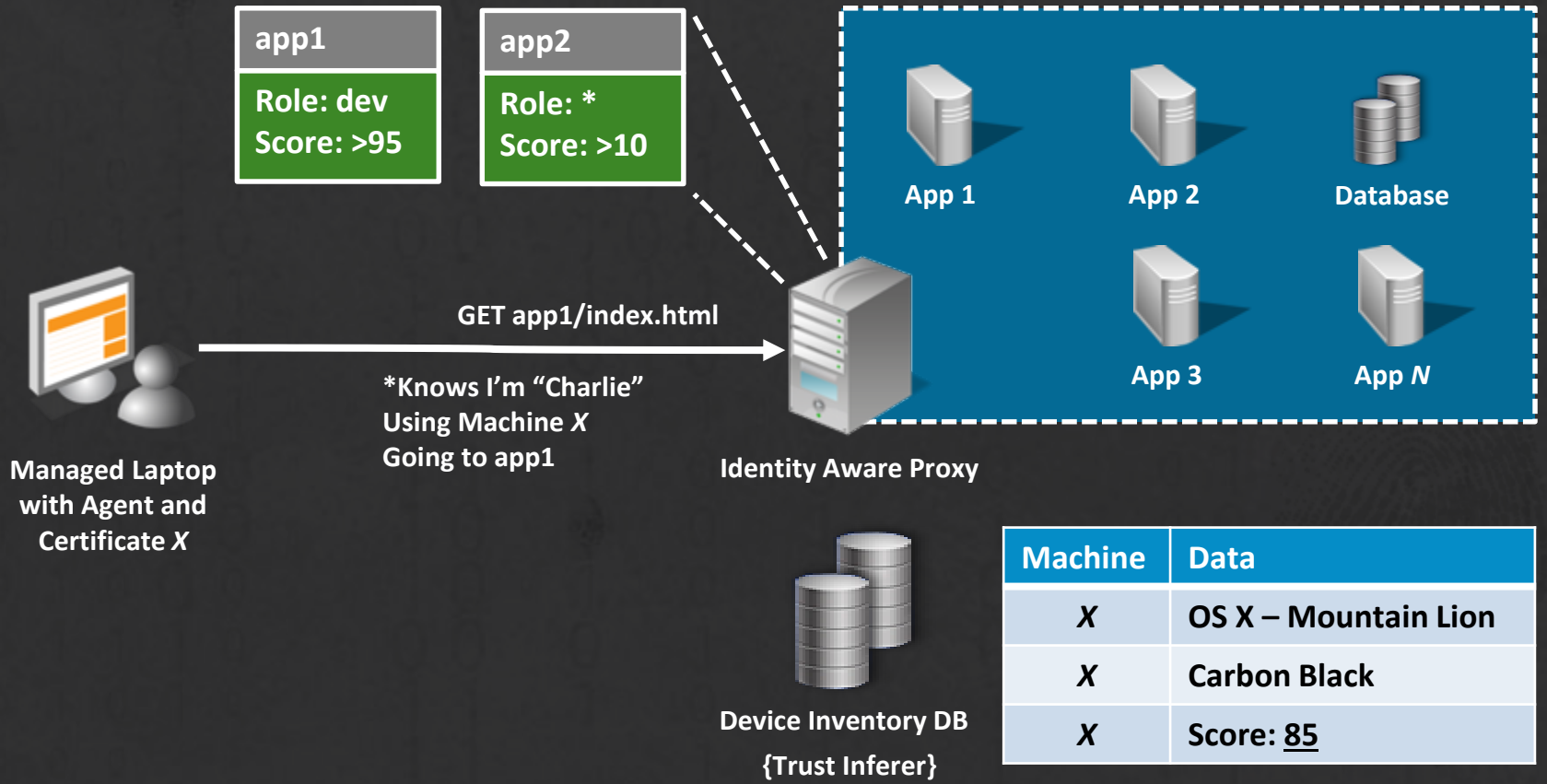
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



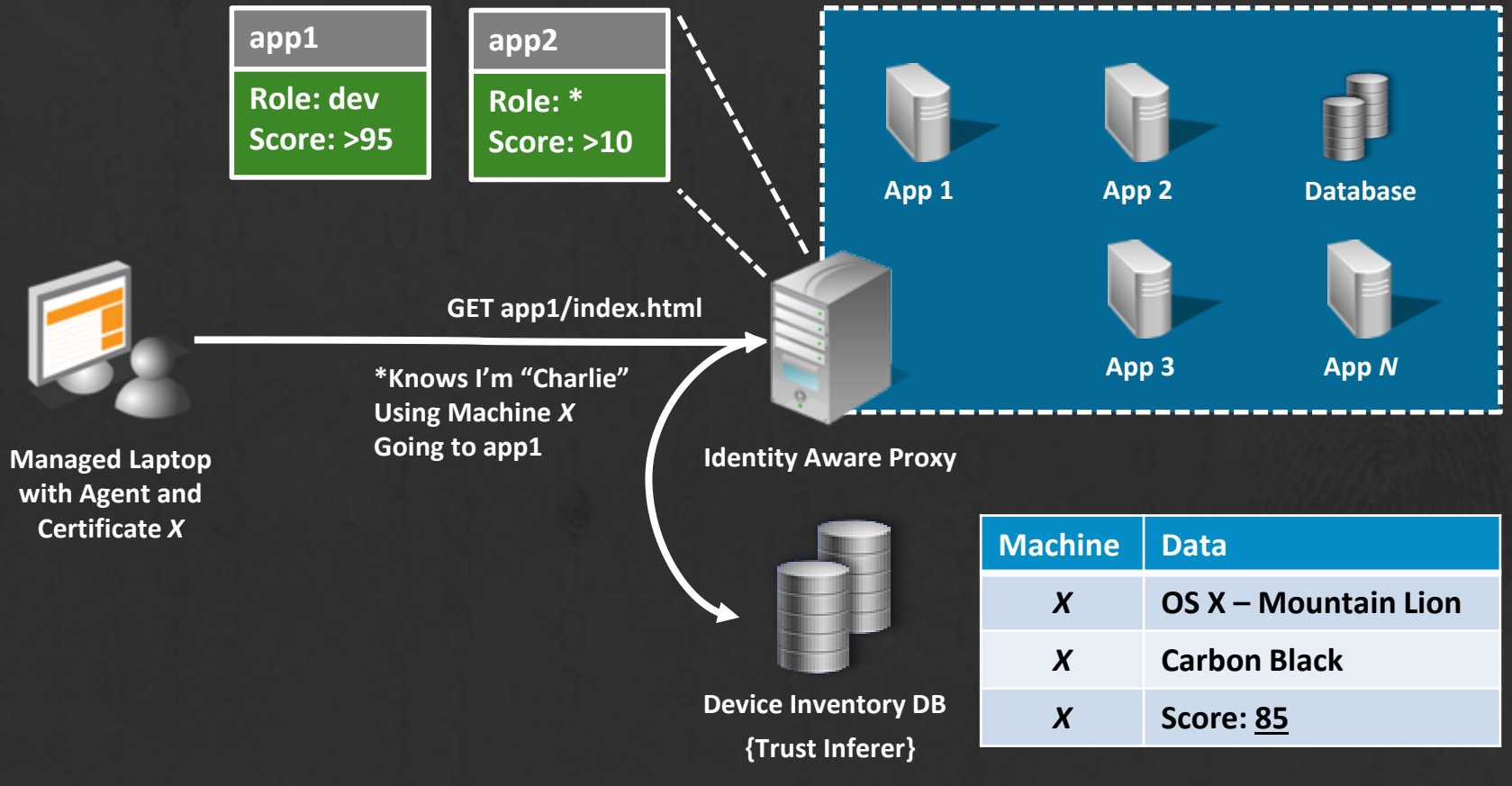
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



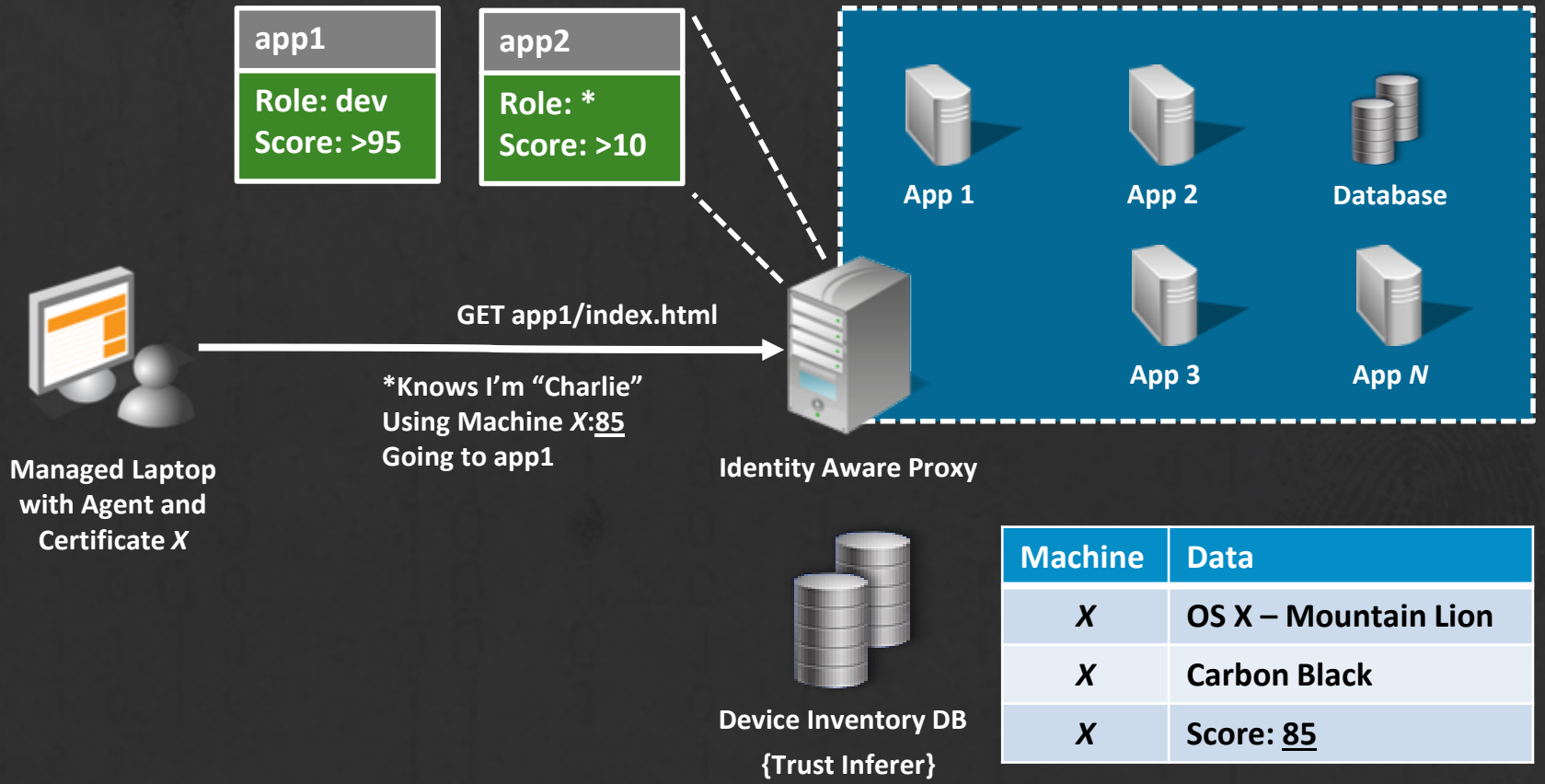
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



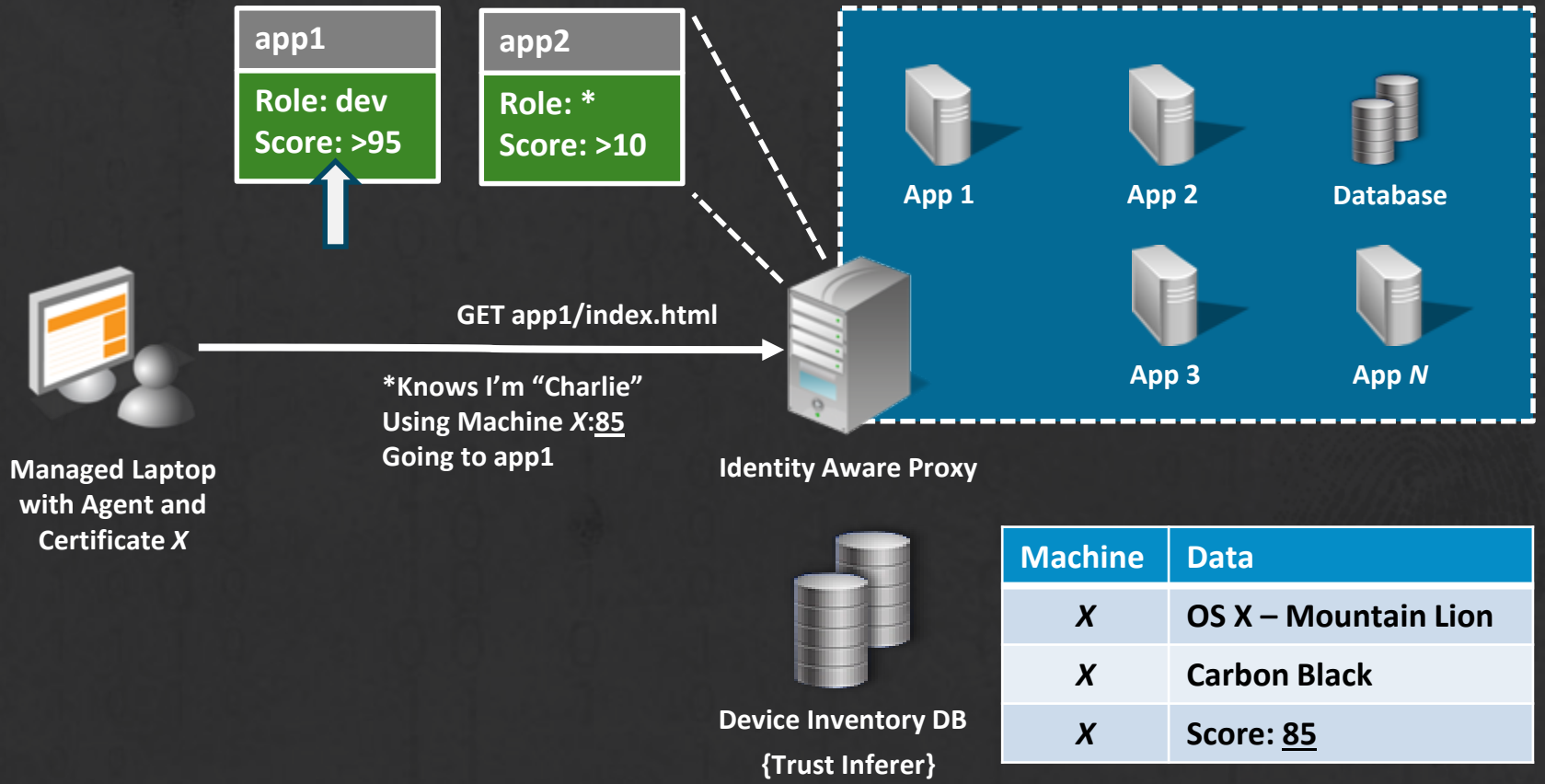
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



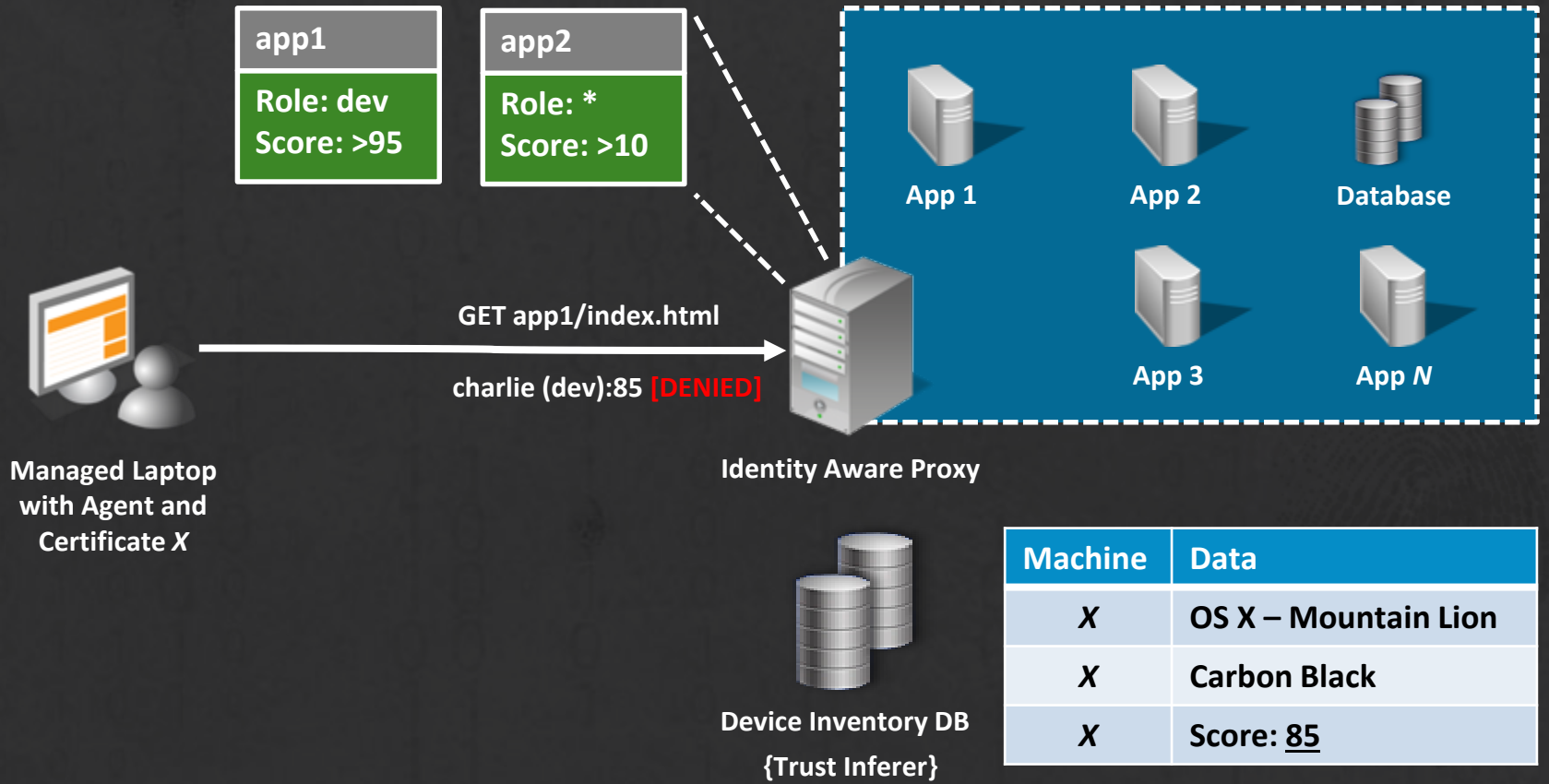
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



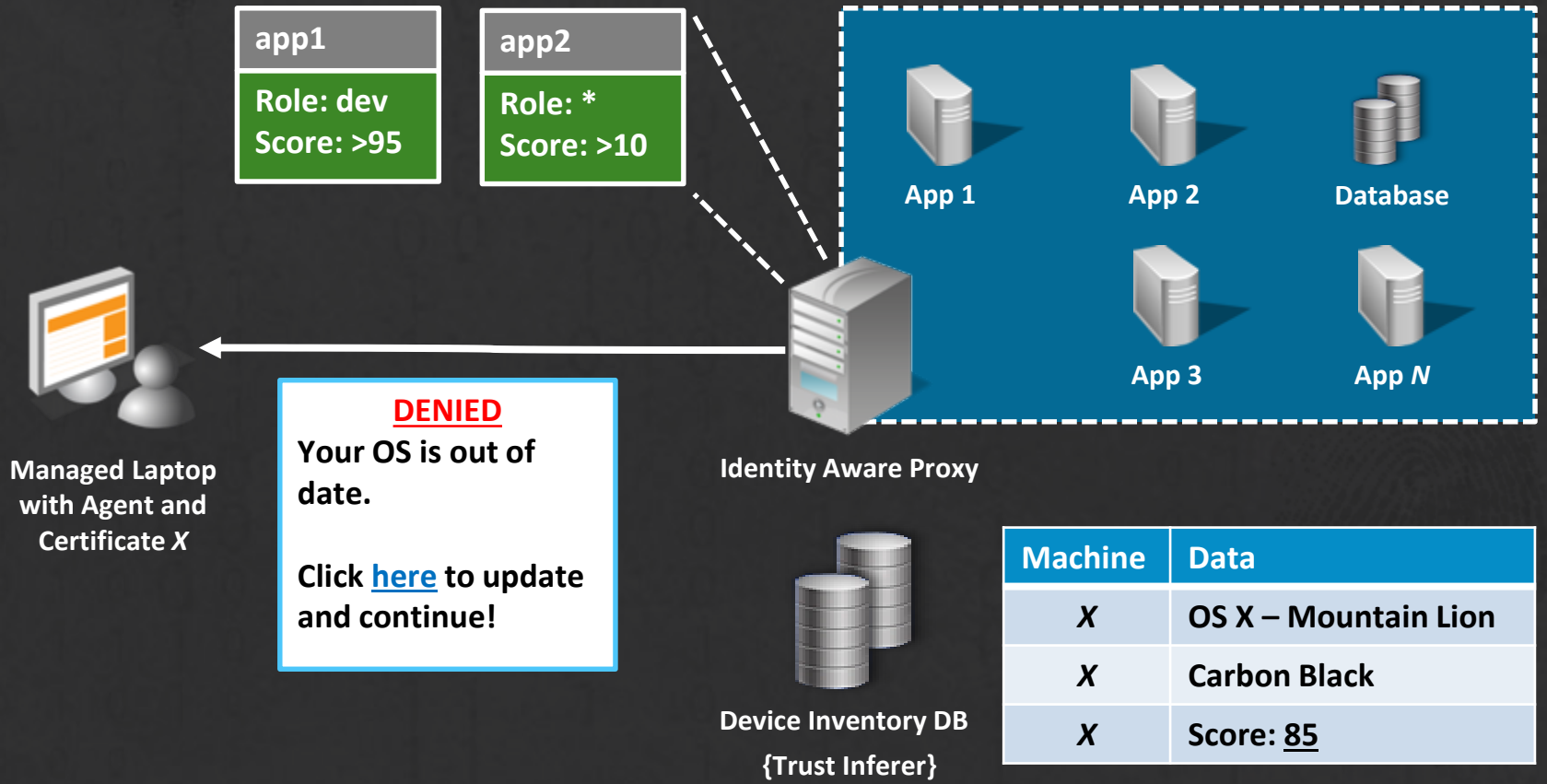
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



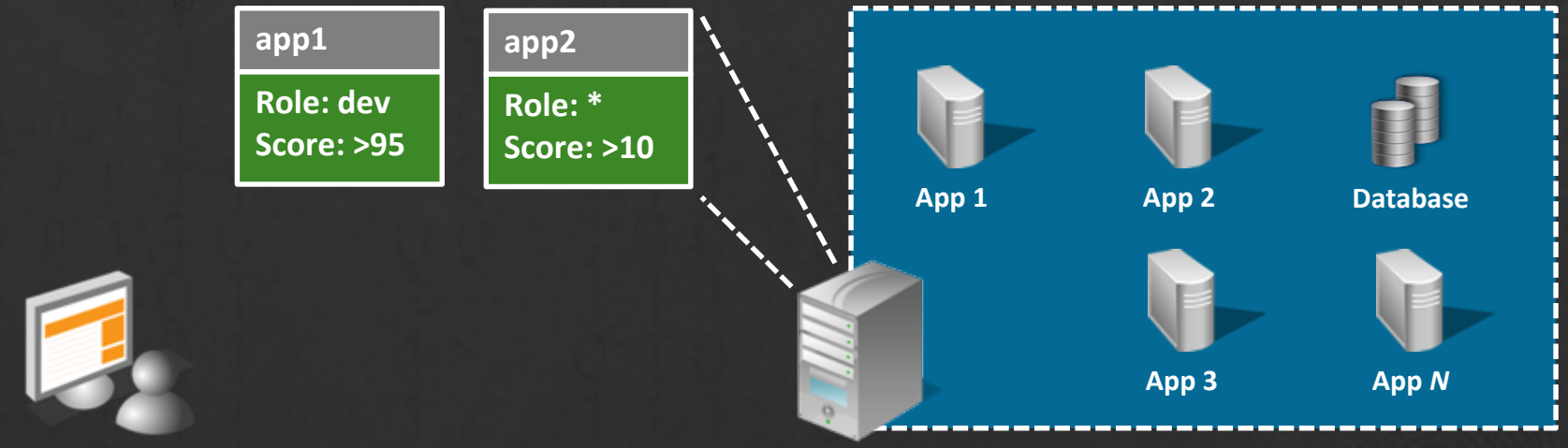
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



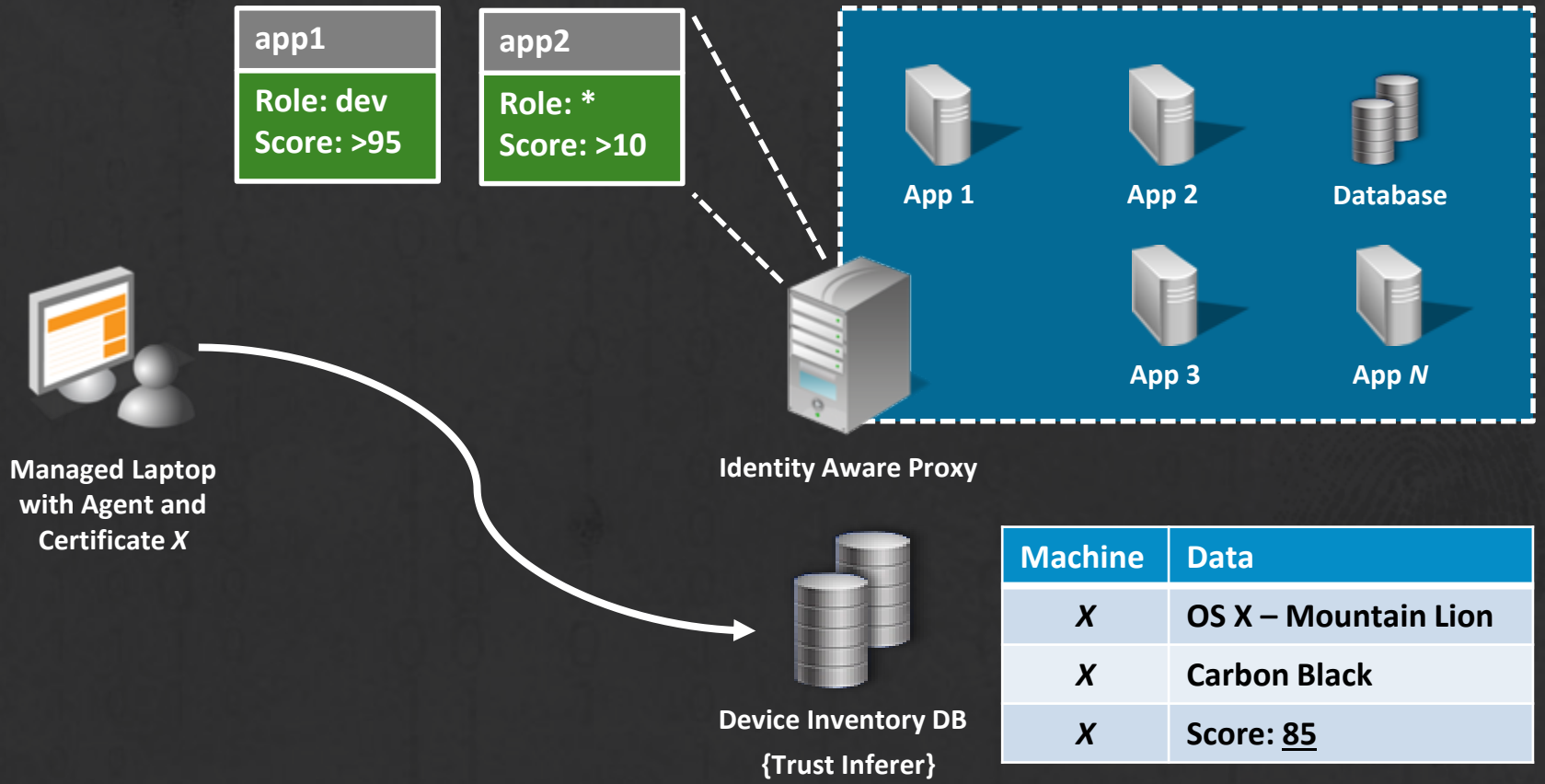
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



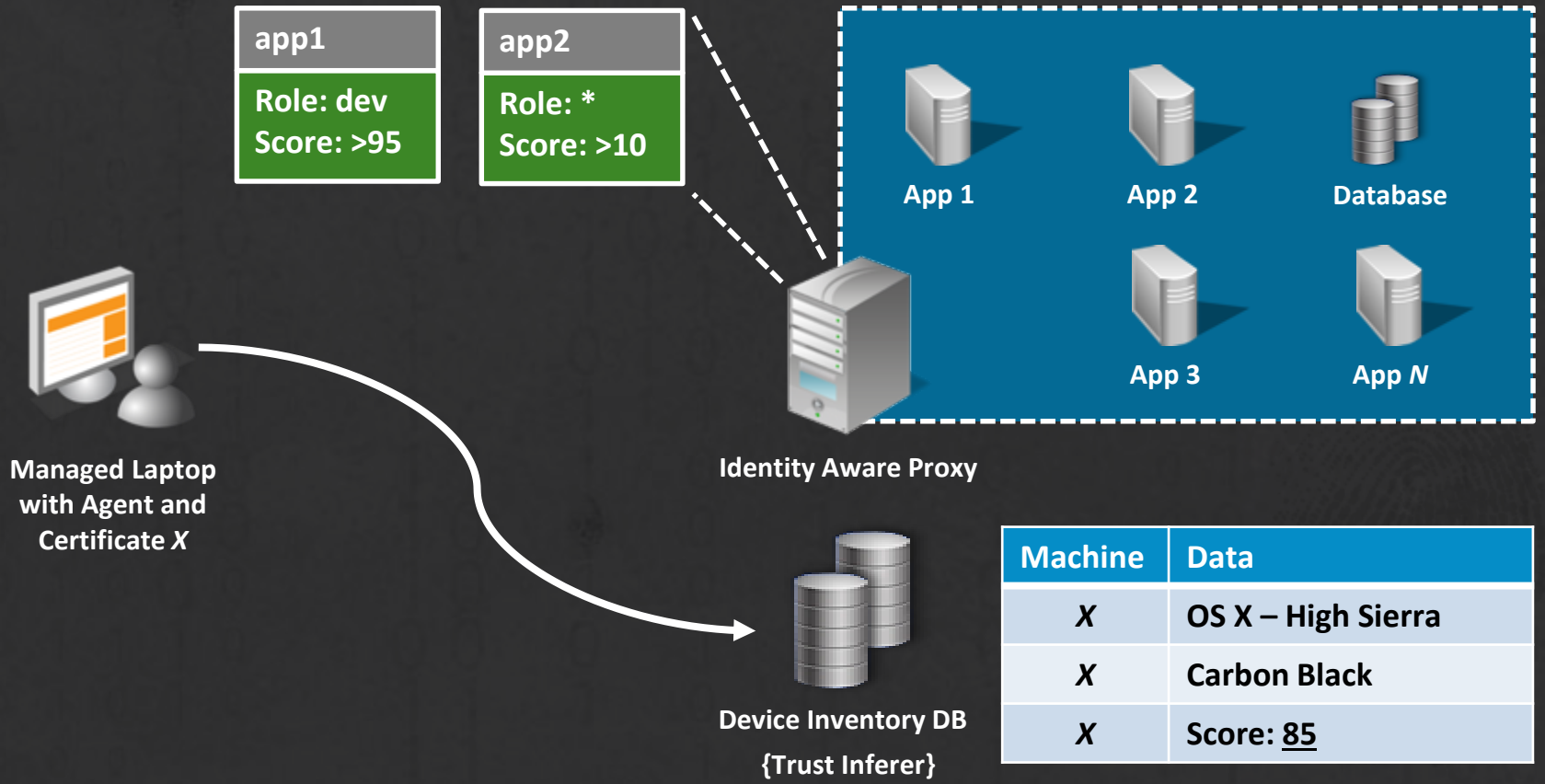
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



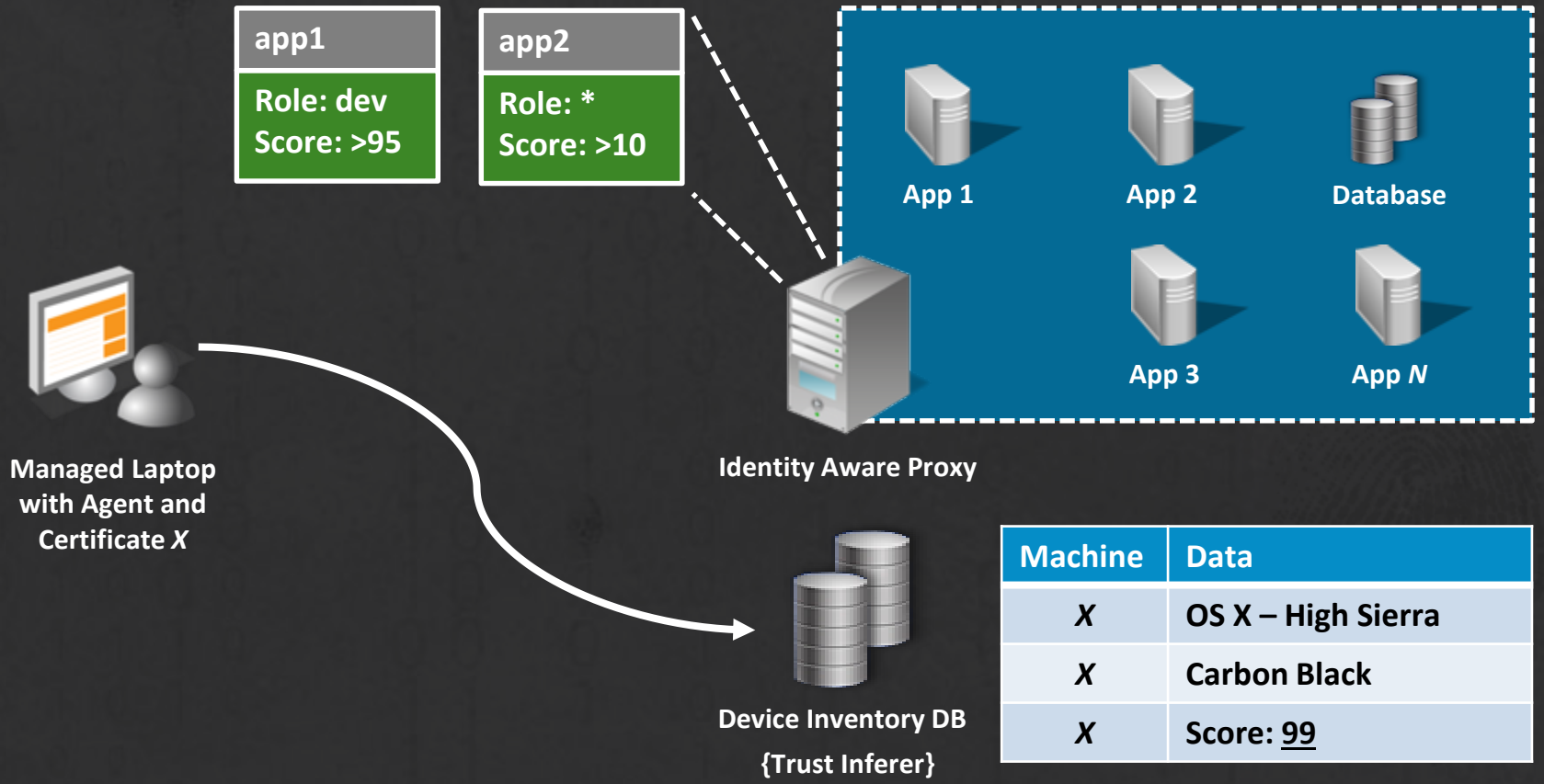
Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 85

Google BeyondCorp



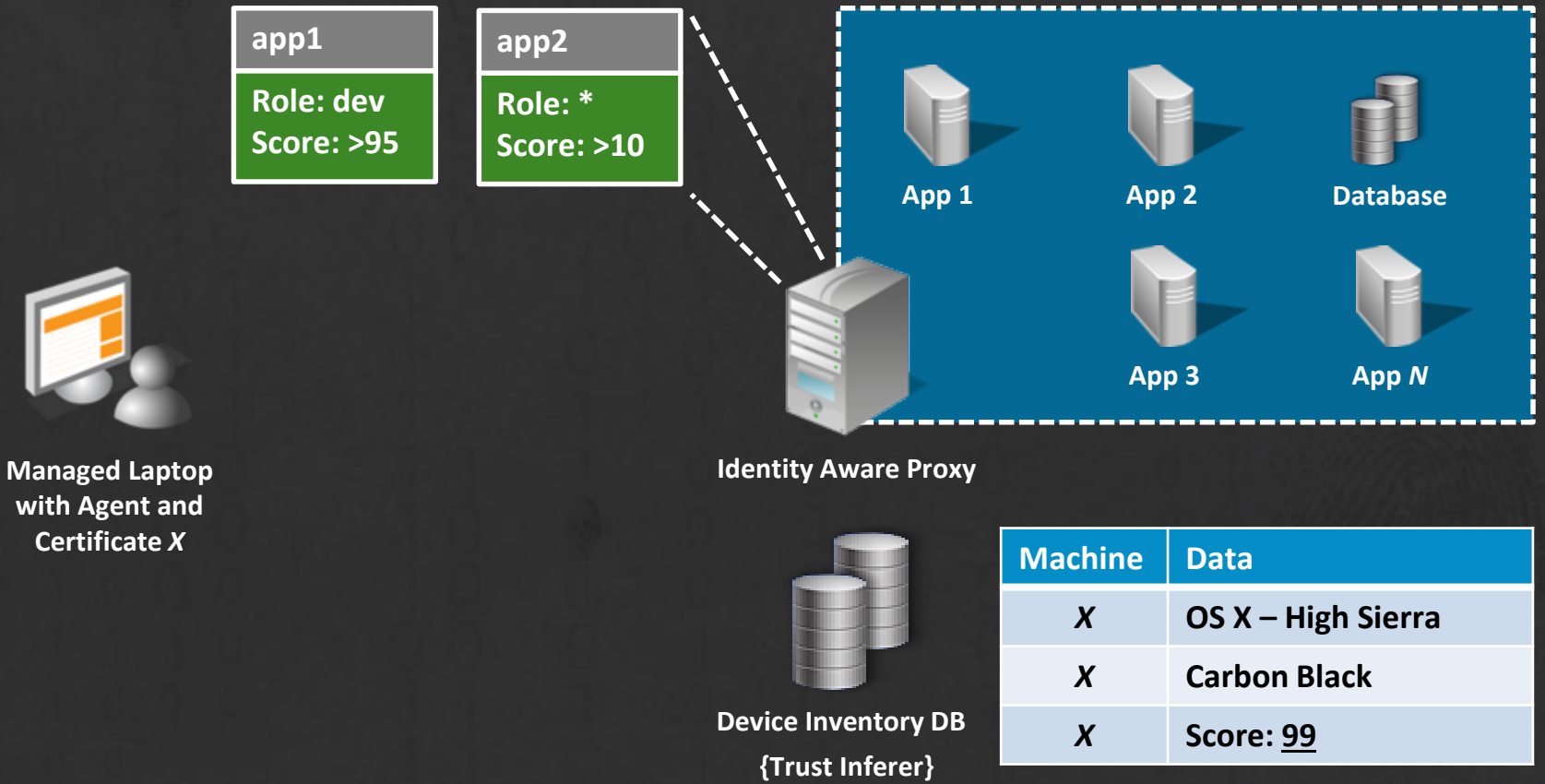
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 85

Google BeyondCorp



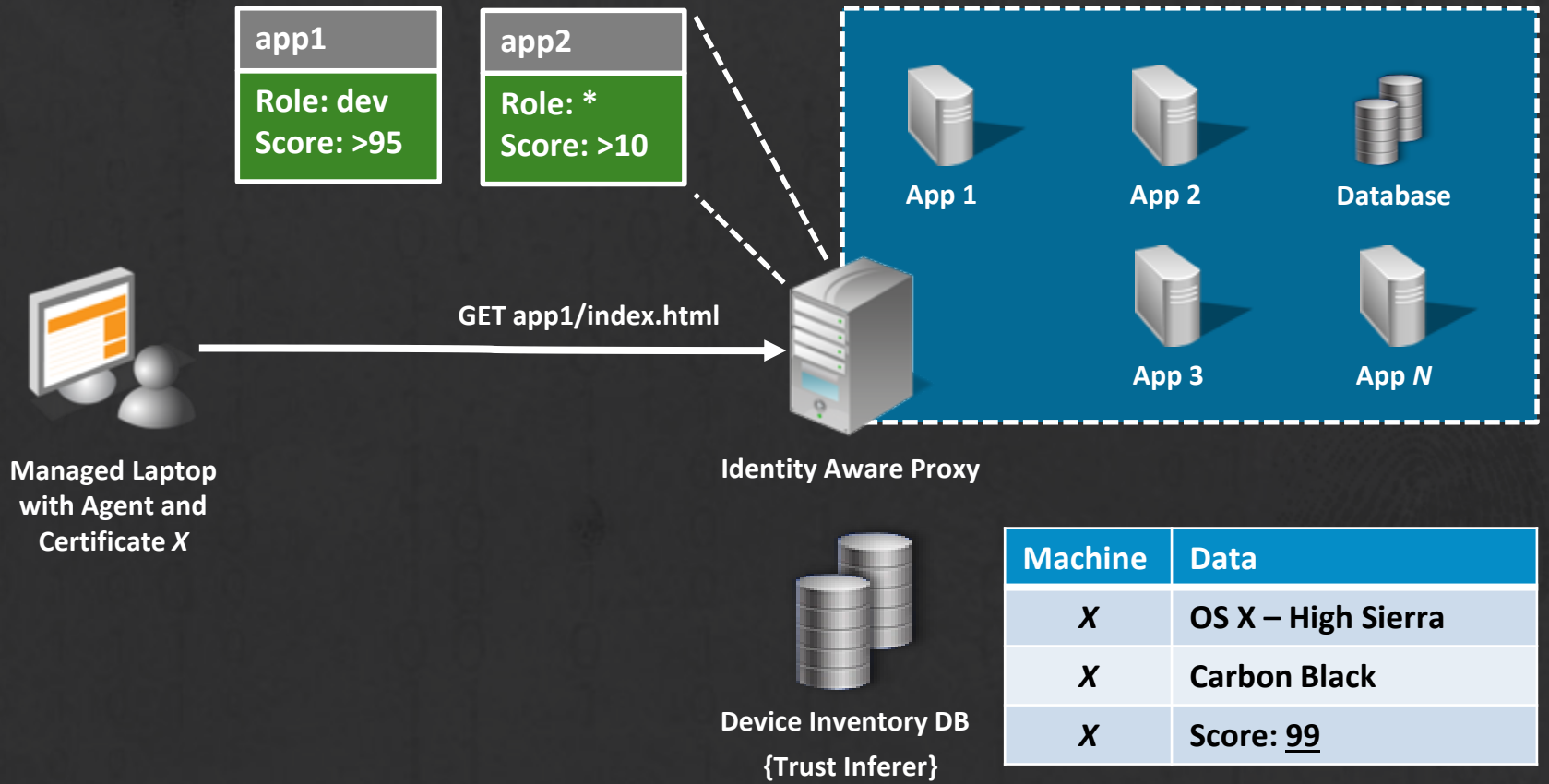
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Google BeyondCorp



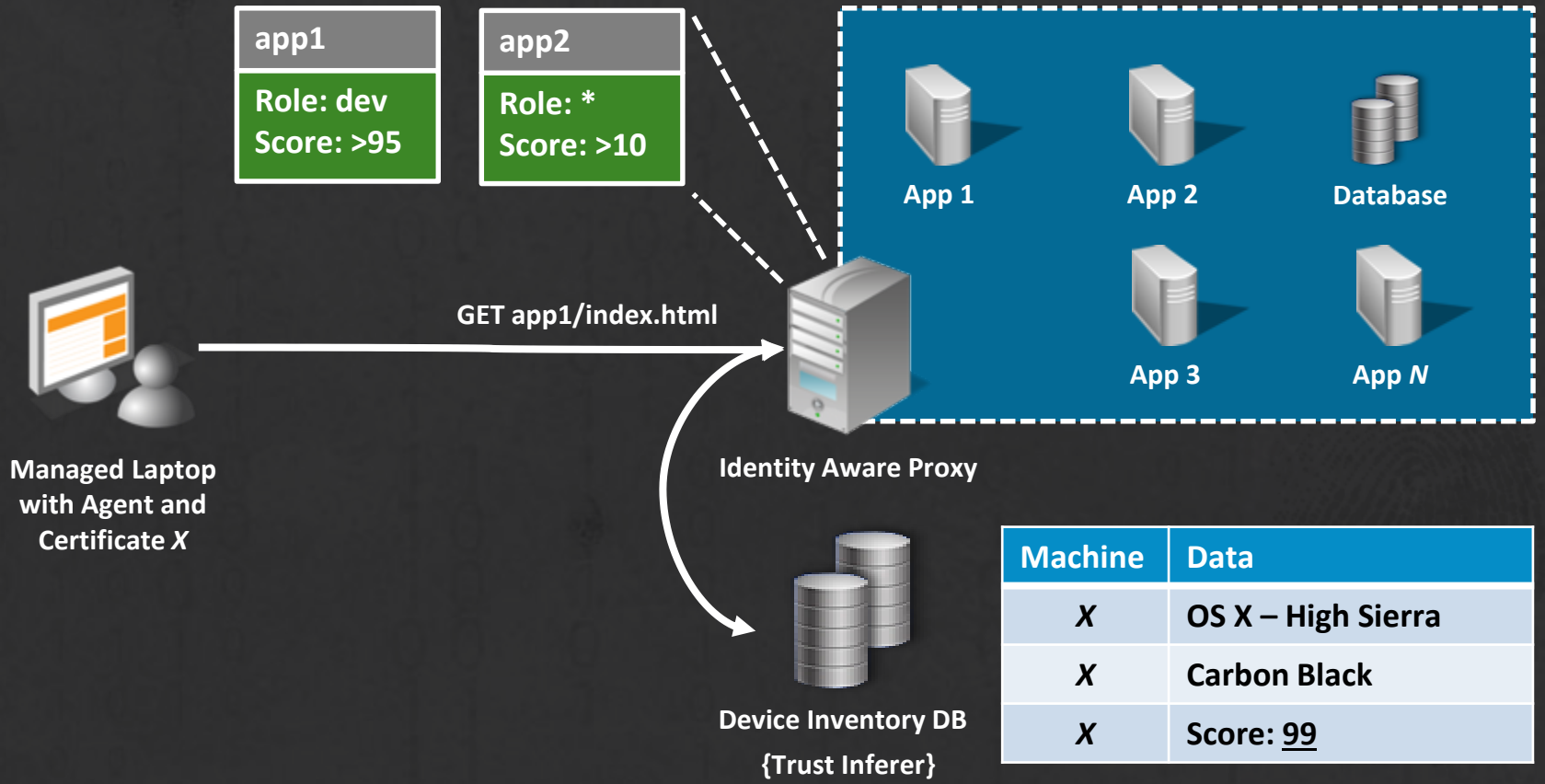
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Google BeyondCorp



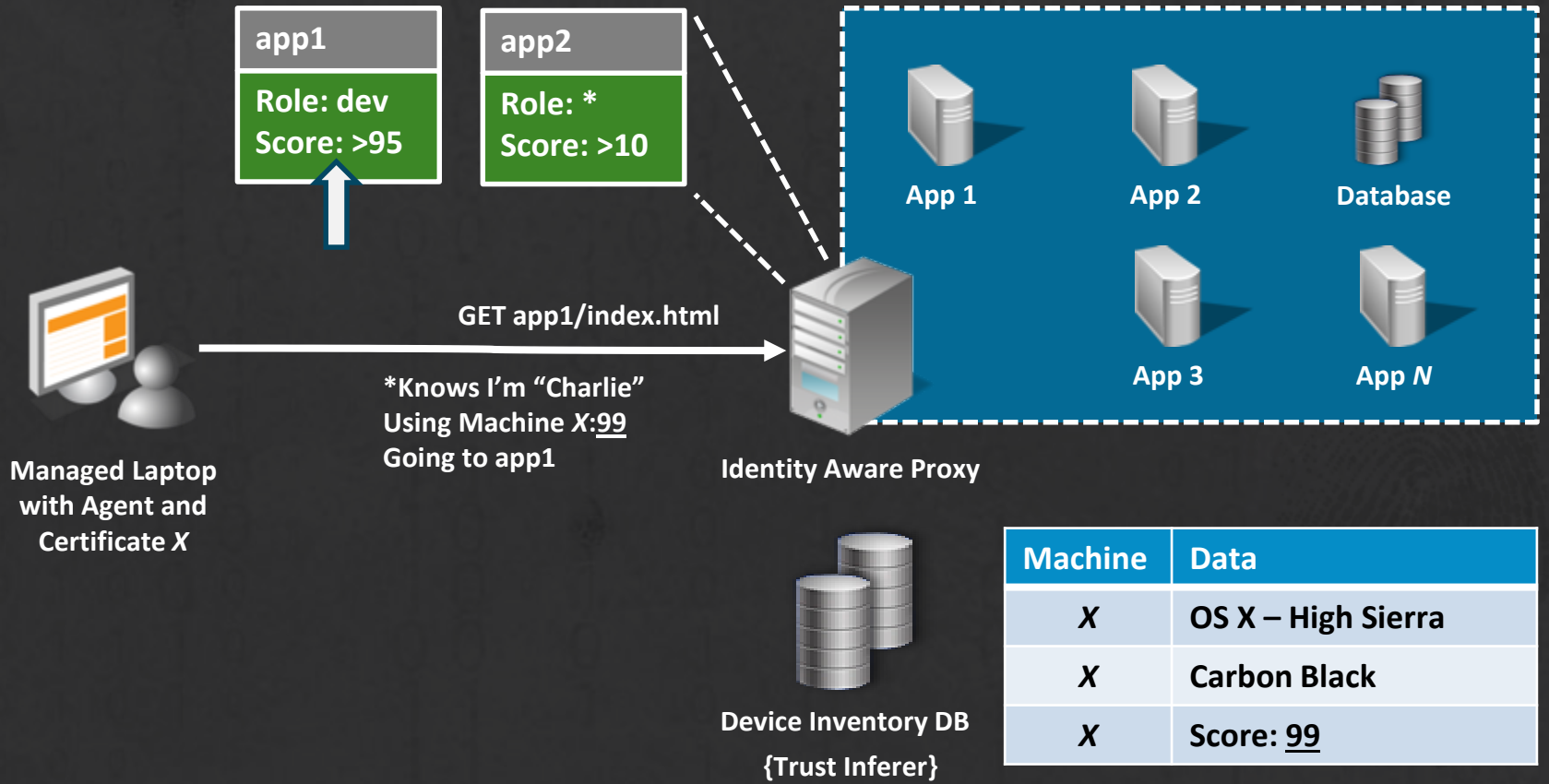
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Google BeyondCorp



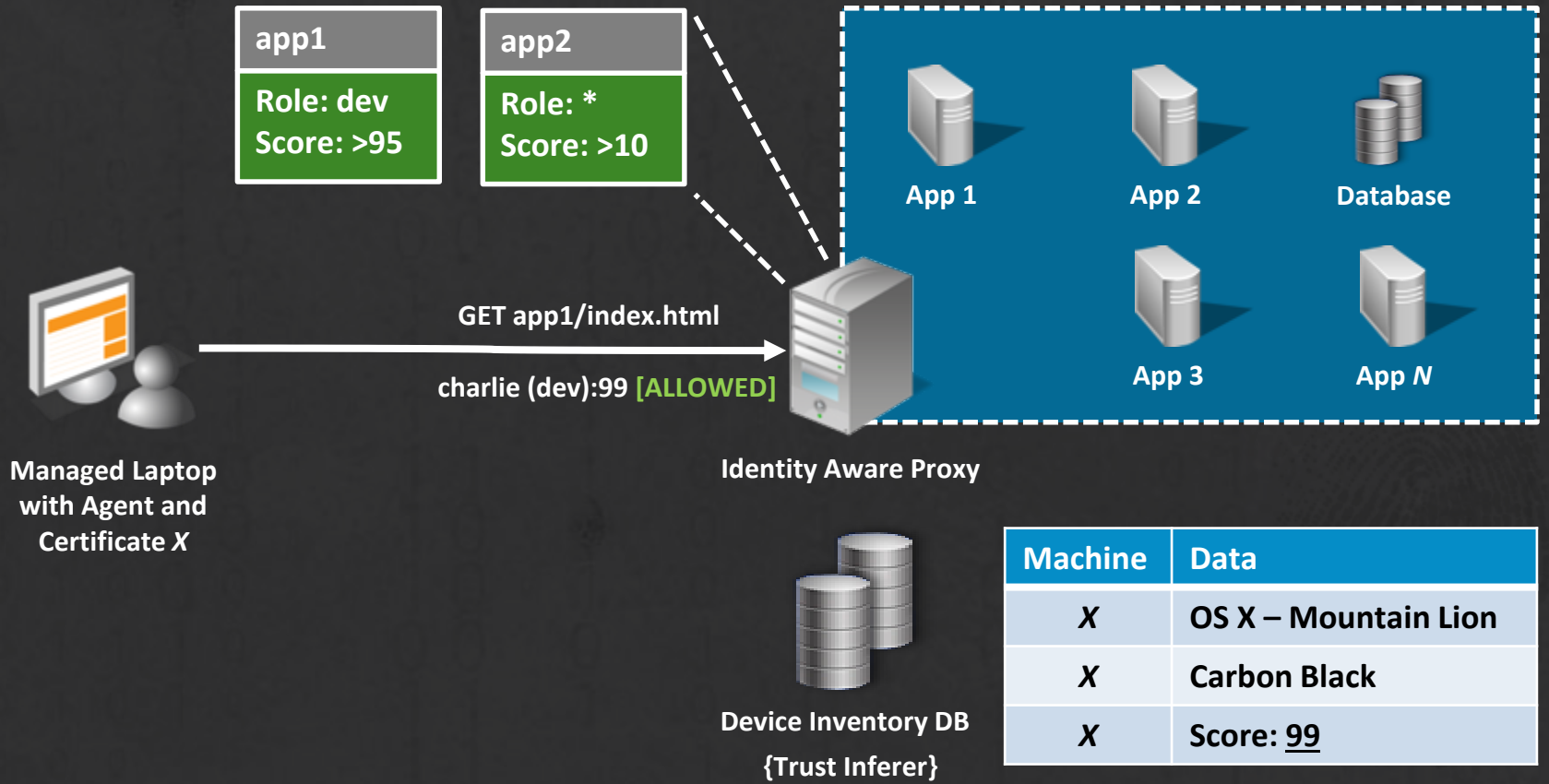
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Google BeyondCorp



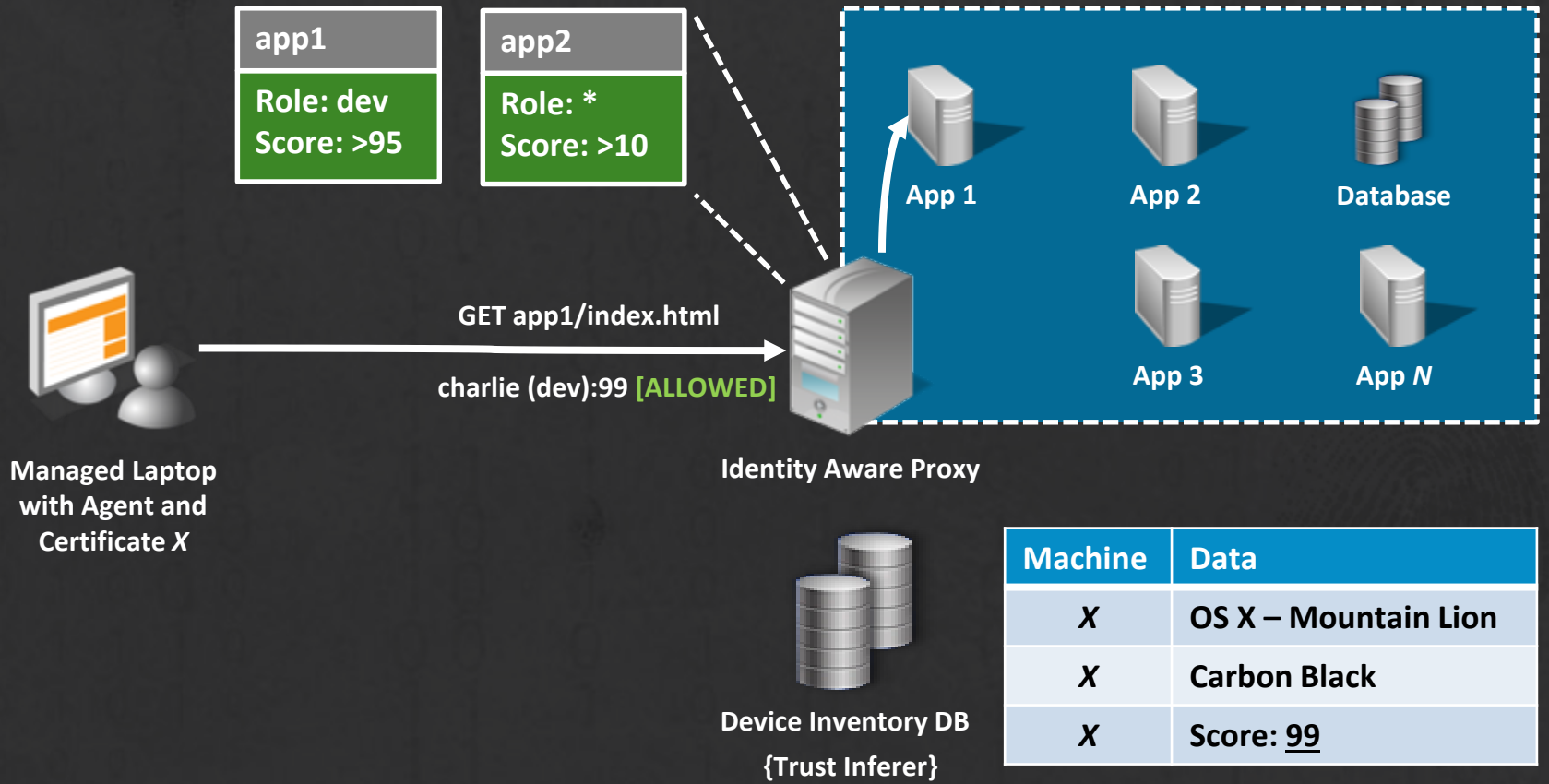
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Google BeyondCorp



Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 99

Google BeyondCorp



Machine	Data
X	OS X – Mountain Lion
X	Carbon Black
X	Score: 99

Google BeyondCorp

BeyondCorp Architecture Accomplishes Set Goals

- **Security Decoupled from Complexity**

  Simply add an app to the micro-perimeter and configure!

- **Application Configuration is Distributed**

  Application owner can set own policies. Less tickets.

- **Self-Remediation is Possible**

  System can inform a user why they were denied and let them repair. Less Helpdesk calls!

Google BeyondCorp

BeyondCorp Also Fulfills Promise of Zero Trust 2.0

- **Identity & Access Occur in the Cloud**
  Easy to scale and users can be anywhere Internet access is.
  Reduces Corporate Networks to Guest Wifi!
- **Strong Authentication and Authorization**
  The proxy must know who you are, your machine posture, and where you are going before you can reach any application.
- **Application Access vs. Network Access**
  Users are granted access to apps *through* the proxy, not through the network!

Google BeyondCorp Downsides

Google is altruistic in its thought leadership.

But not in implementation.

You may only have this for workloads in GCP/GKE.

What about data centers and multi-cloud?

ZERO TRUST 3.0

Posture assessment of the data communications.

Conversion of authentication primitives.

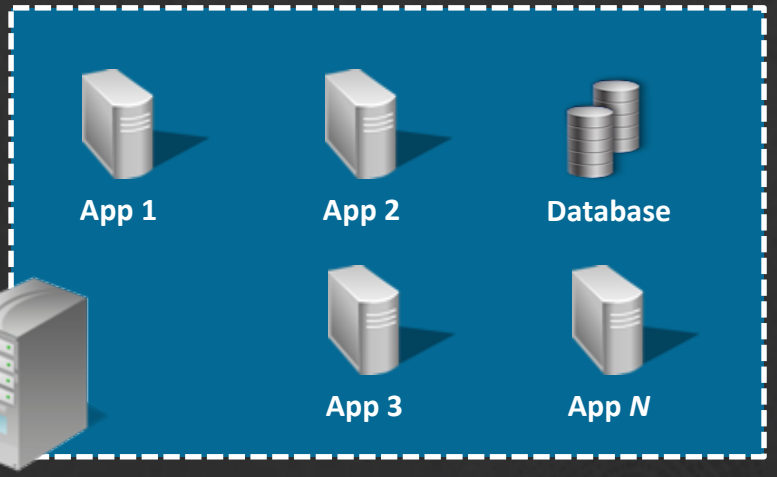
Integration with a security ecosystem.

Support all clouds and private infrastructure.

Zero Trust 3.0

app1
Role: dev Score: >95

app2
Role: * Score: >10



Identity Aware Proxy

Device Inventory DB

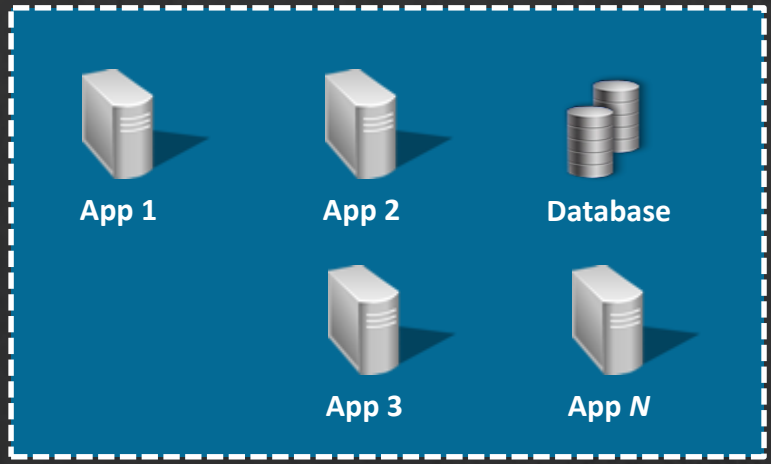
{Trust Inferer}

Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0

app1
Role: dev Score: >95

app2
Role: * Score: >10



Device Inventory DB

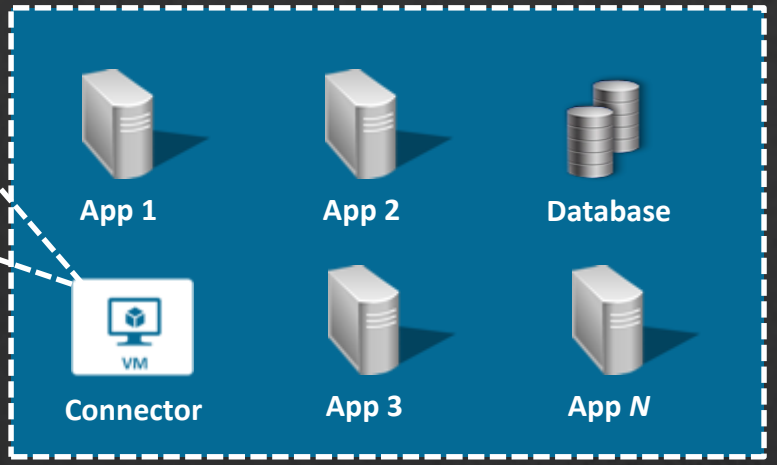
{Trust Inferer}

Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0

app1
Role: dev Score: >95

app2
Role: * Score: >10

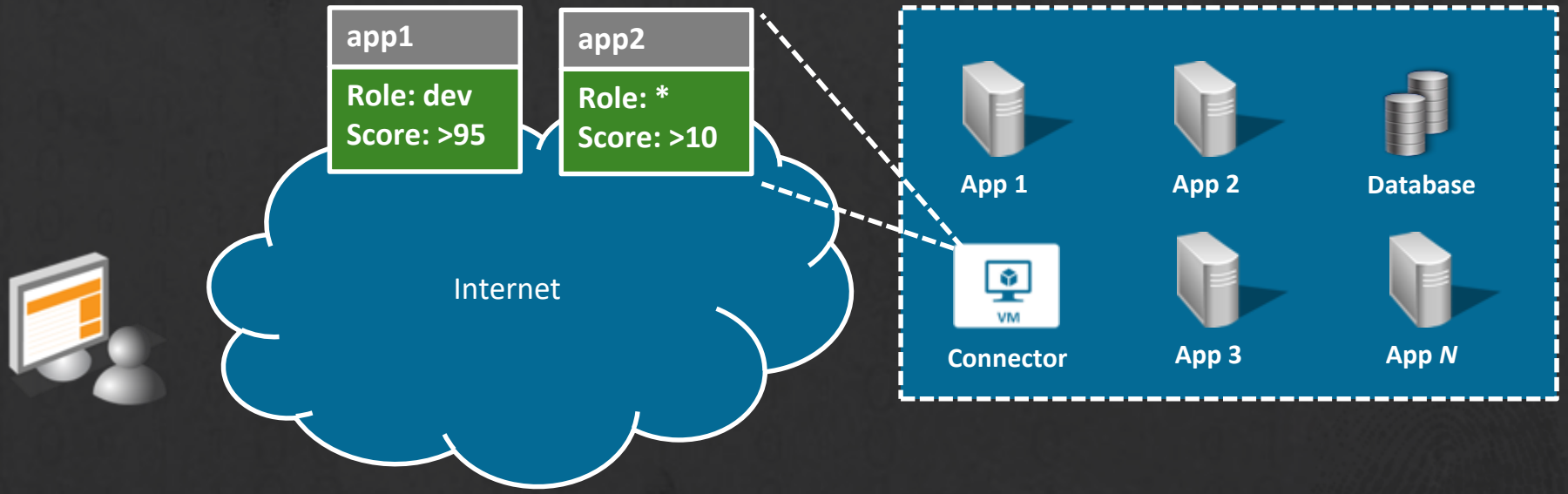


Device Inventory DB

{Trust Inferer}

Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0

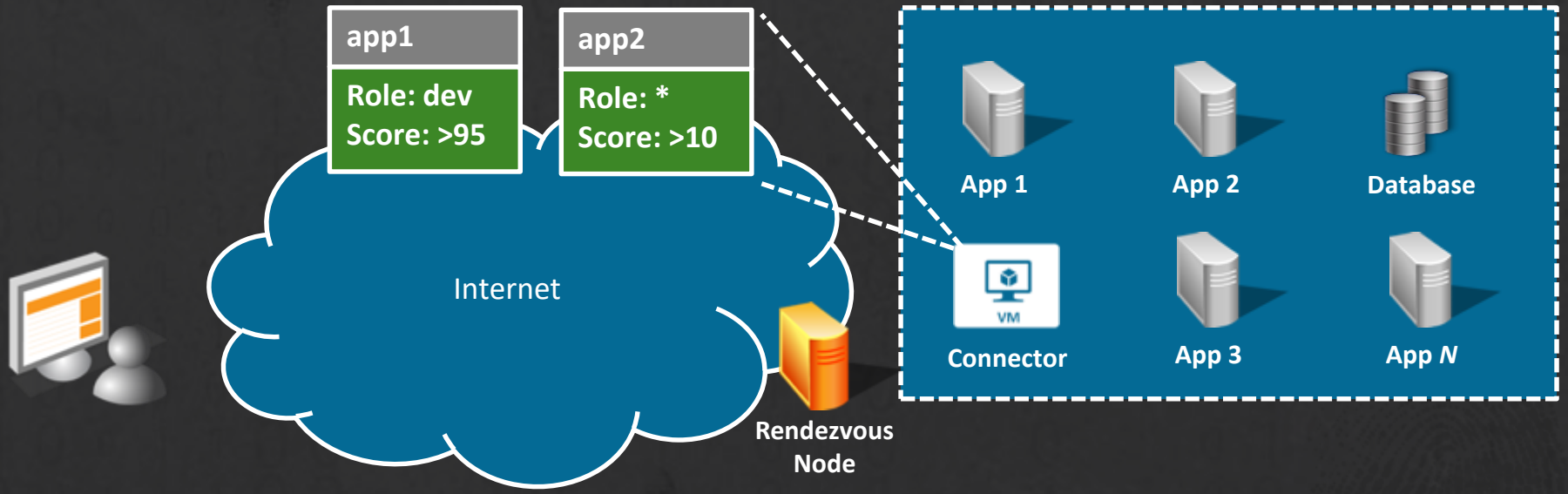


Device Inventory DB

{Trust Inferer}

Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0

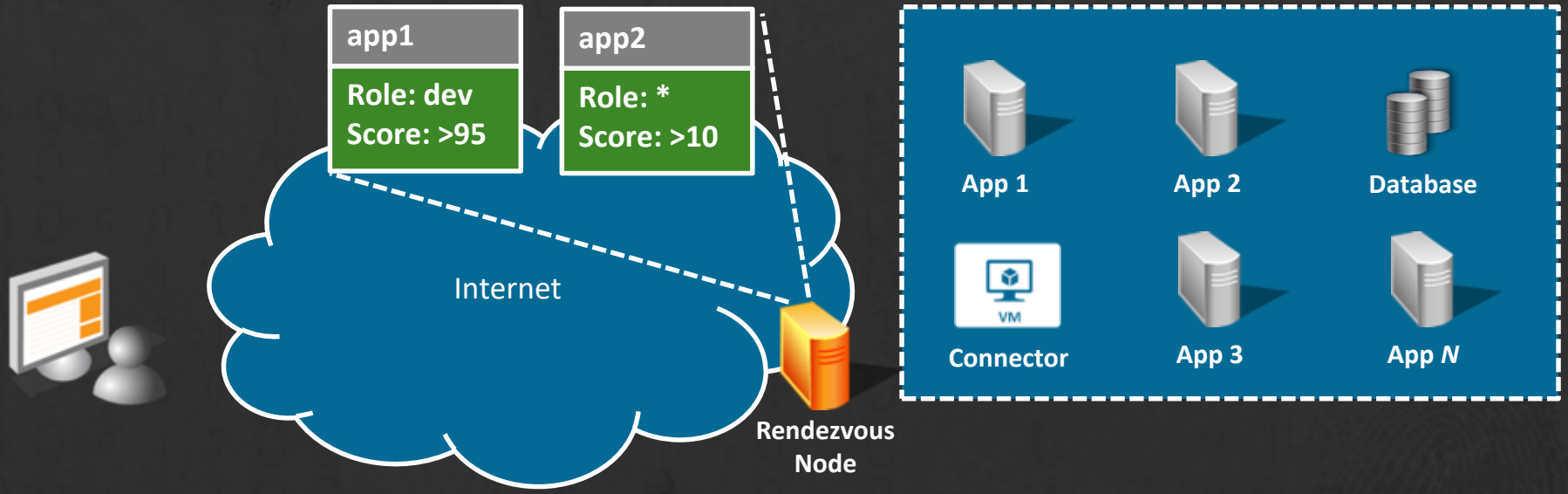


Device Inventory DB

{Trust Inferer}

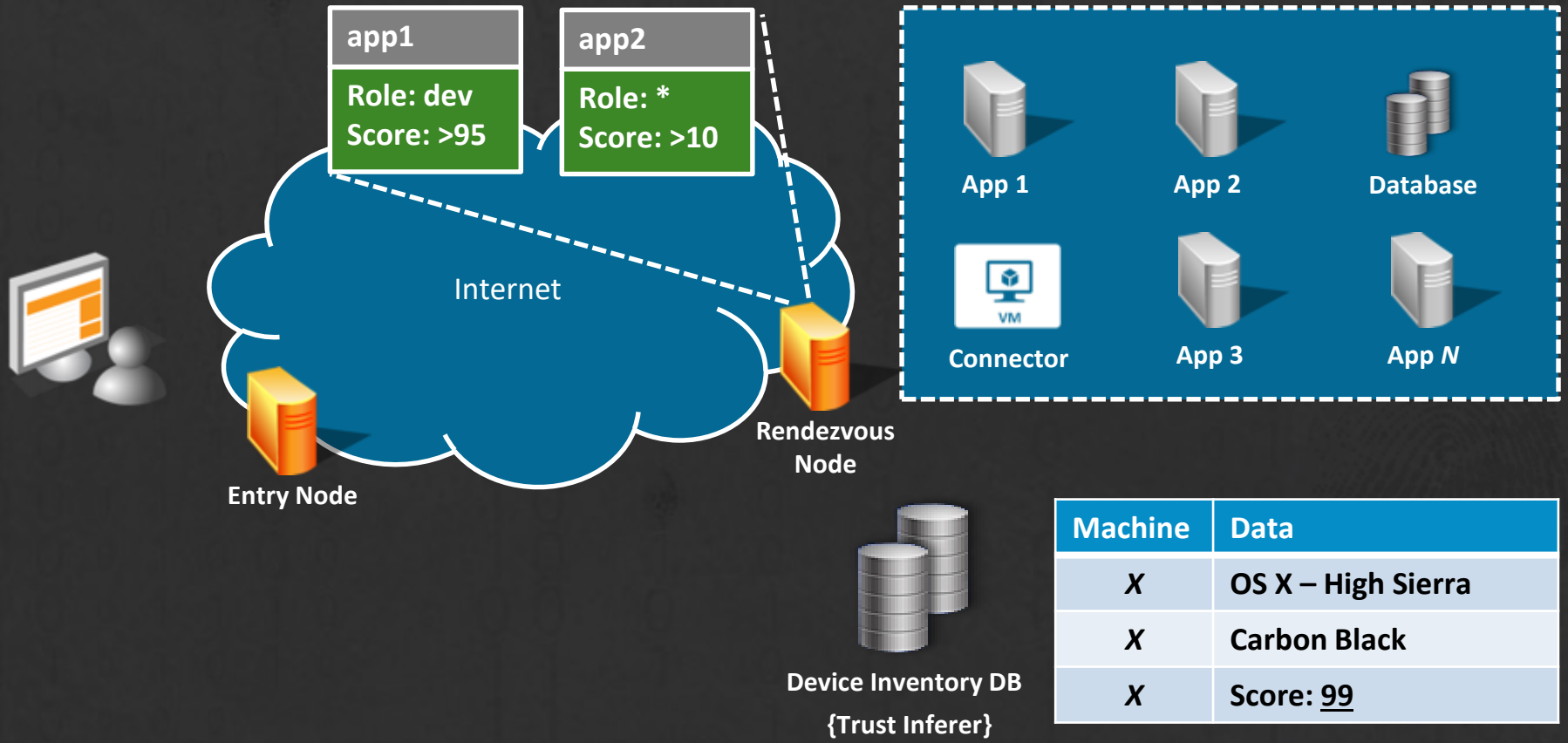
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



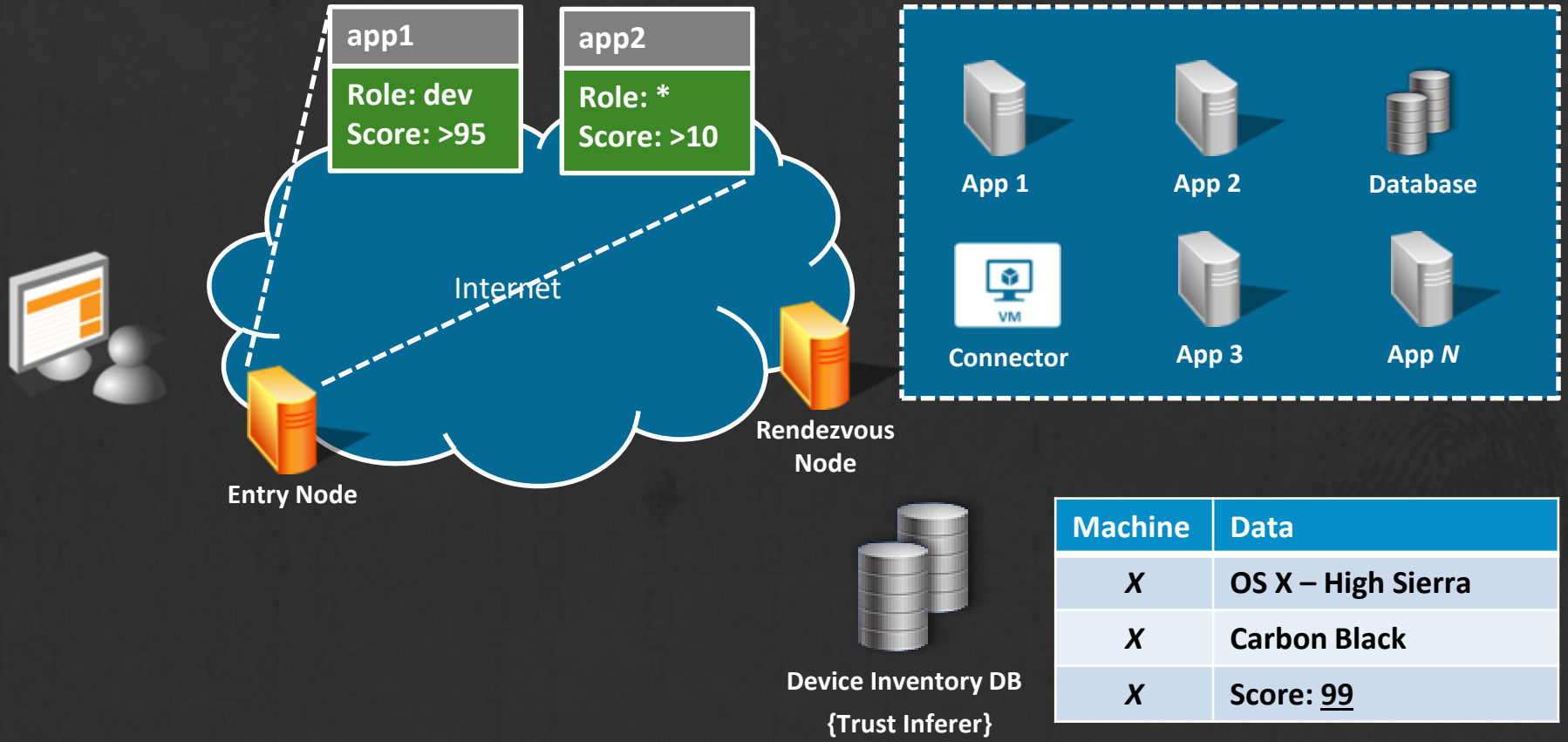
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



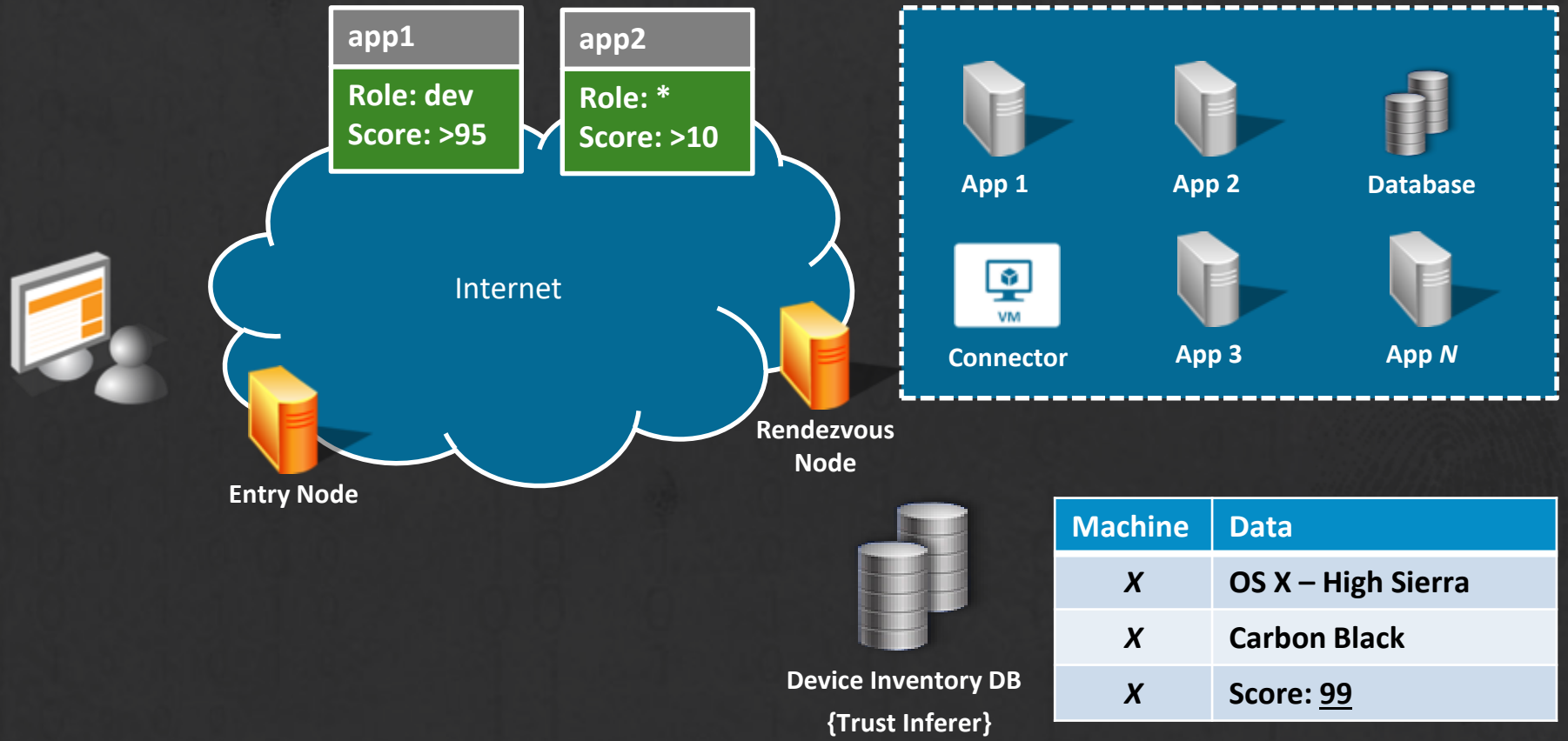
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



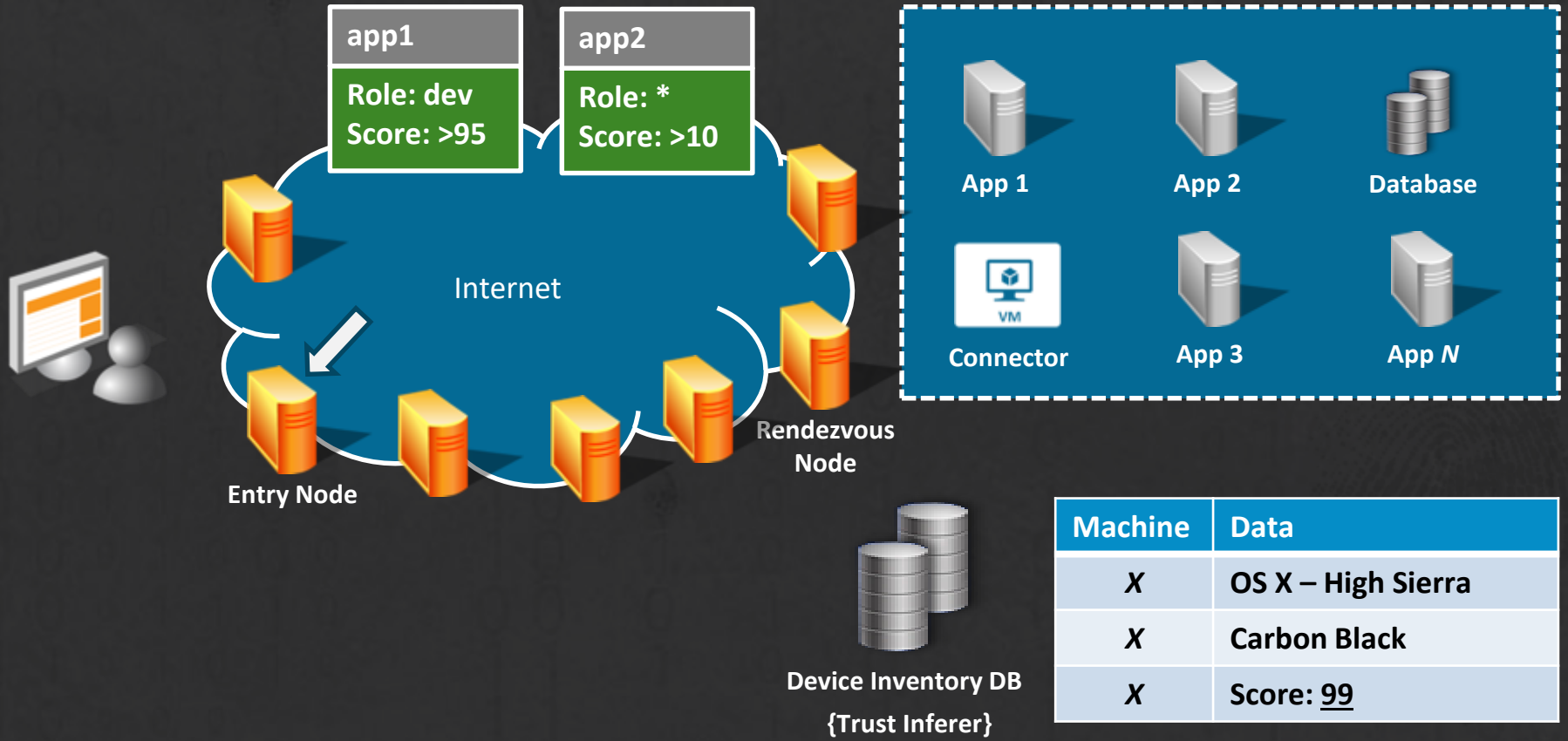
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



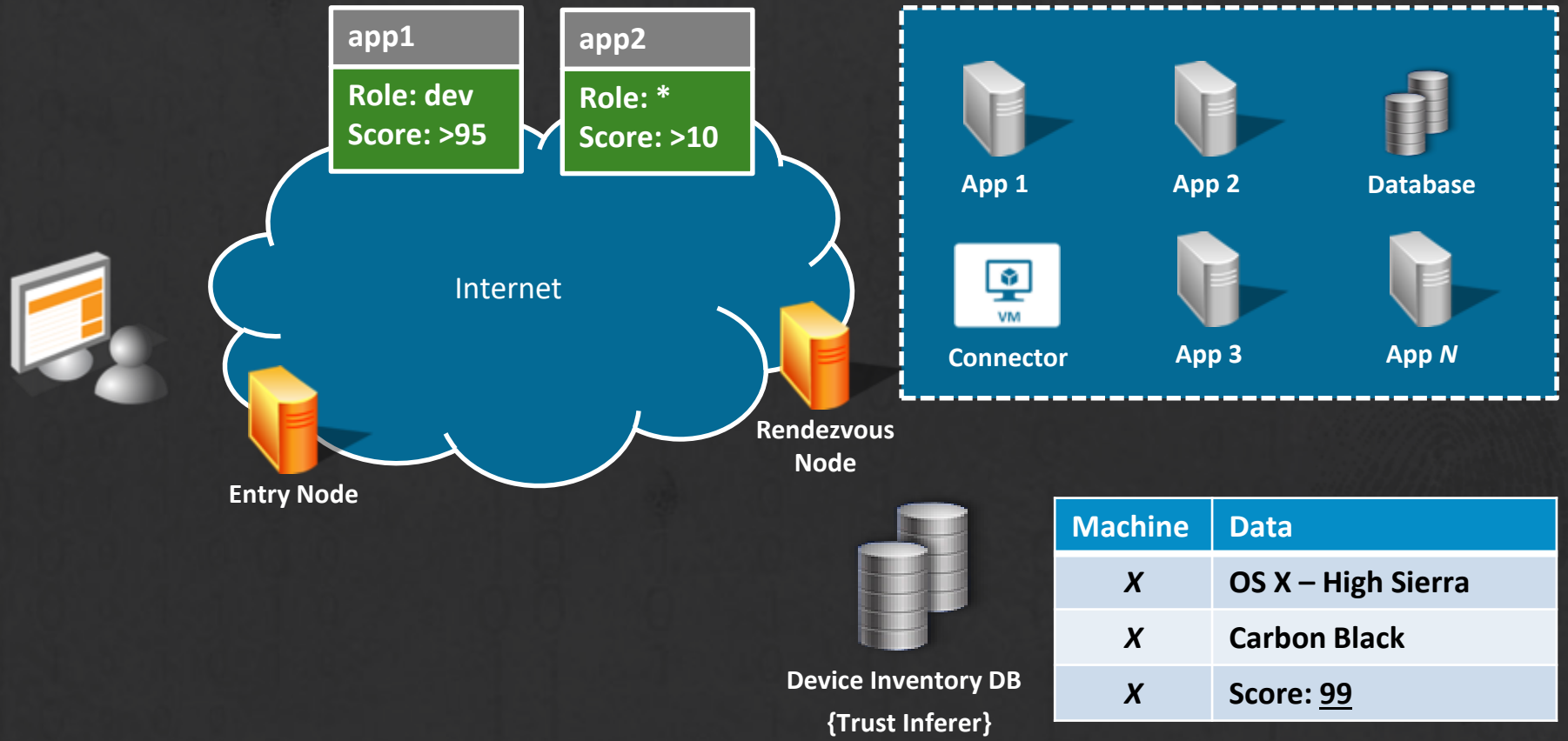
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



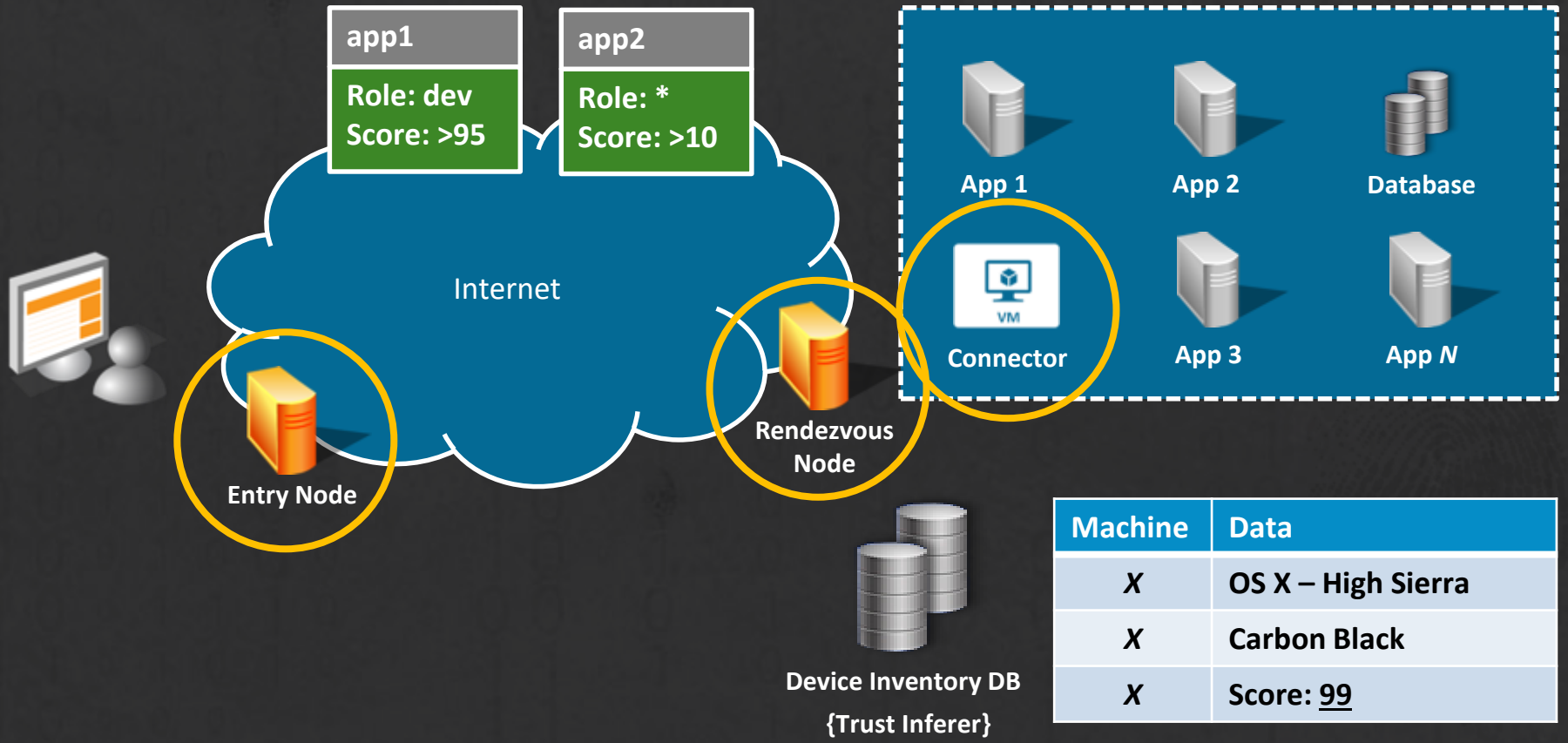
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



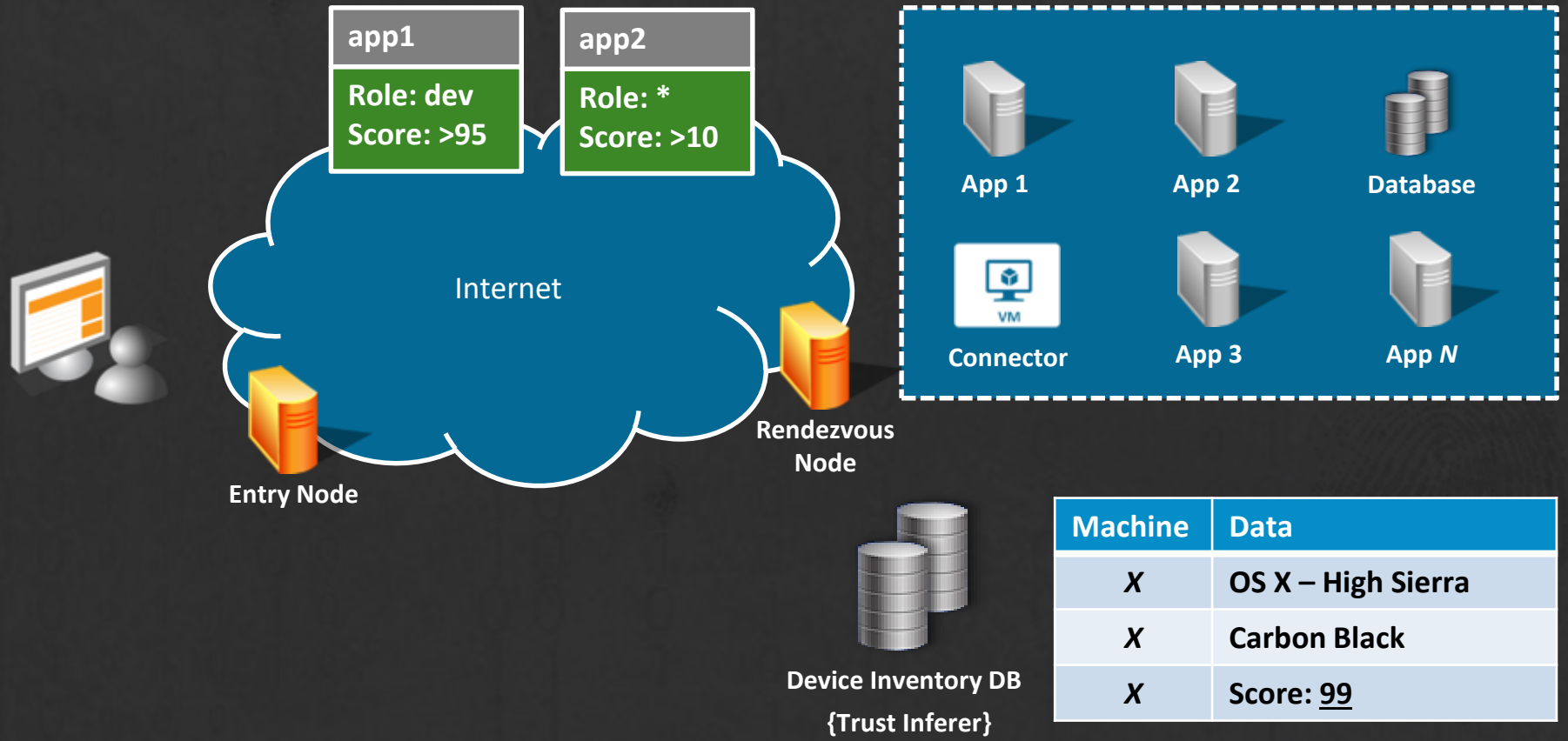
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



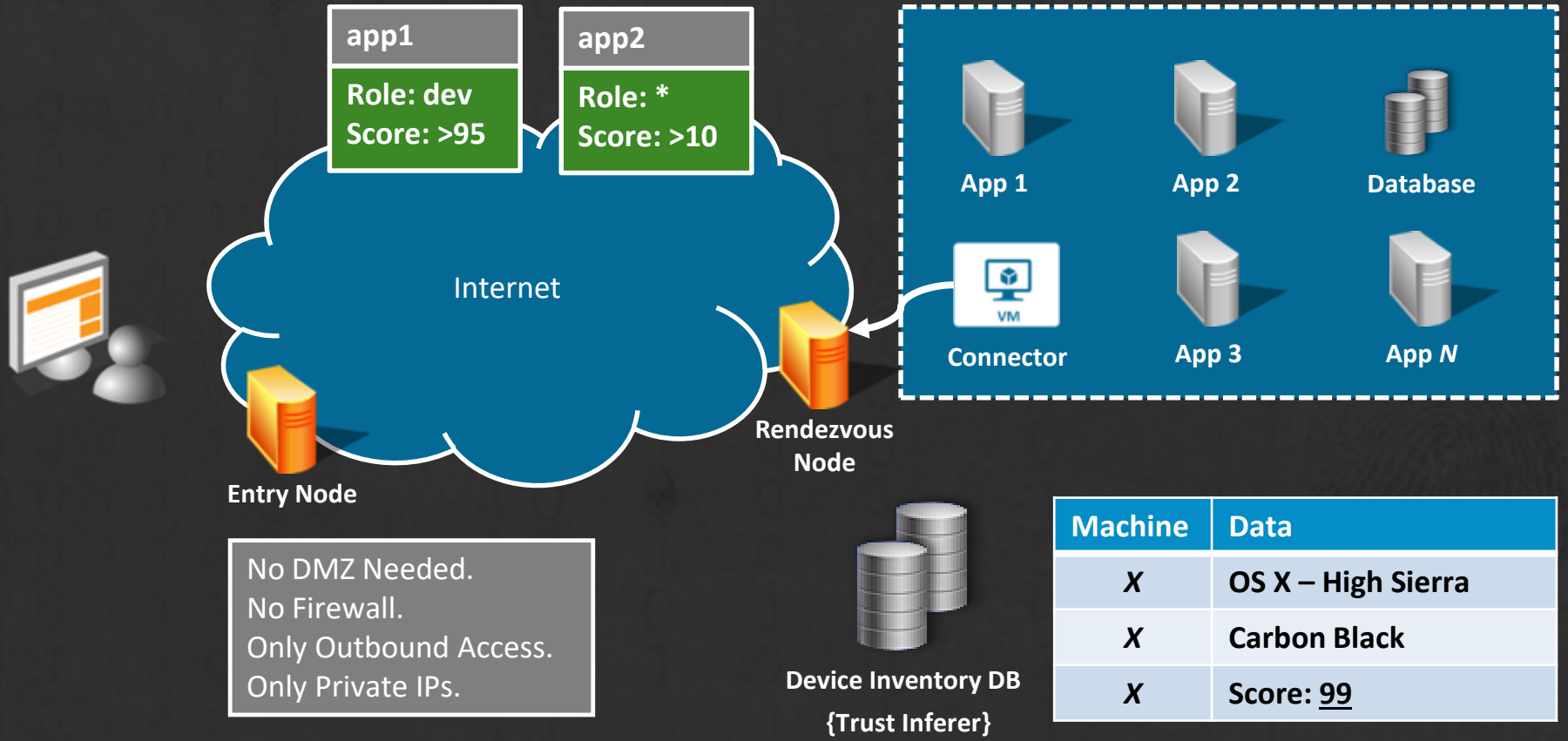
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



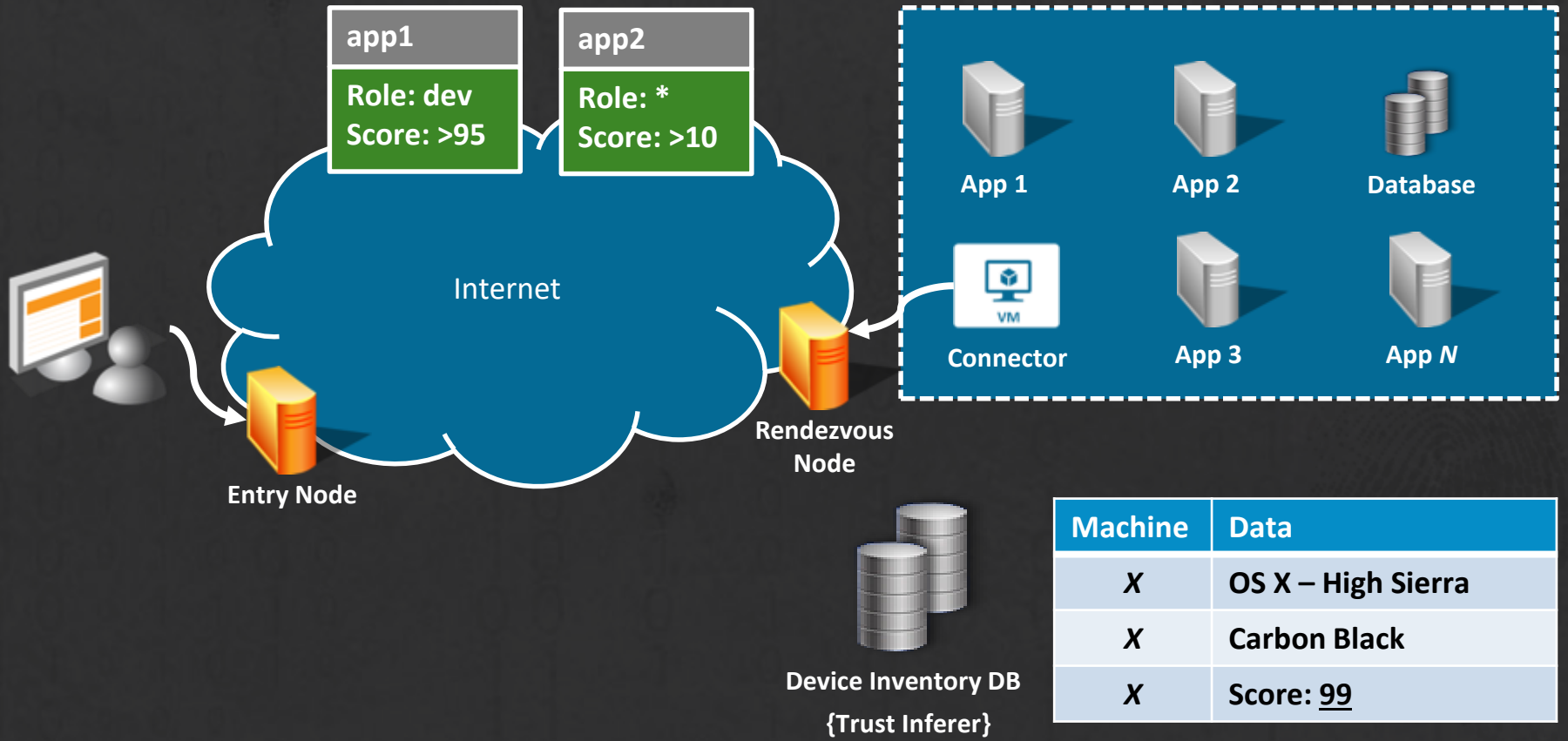
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



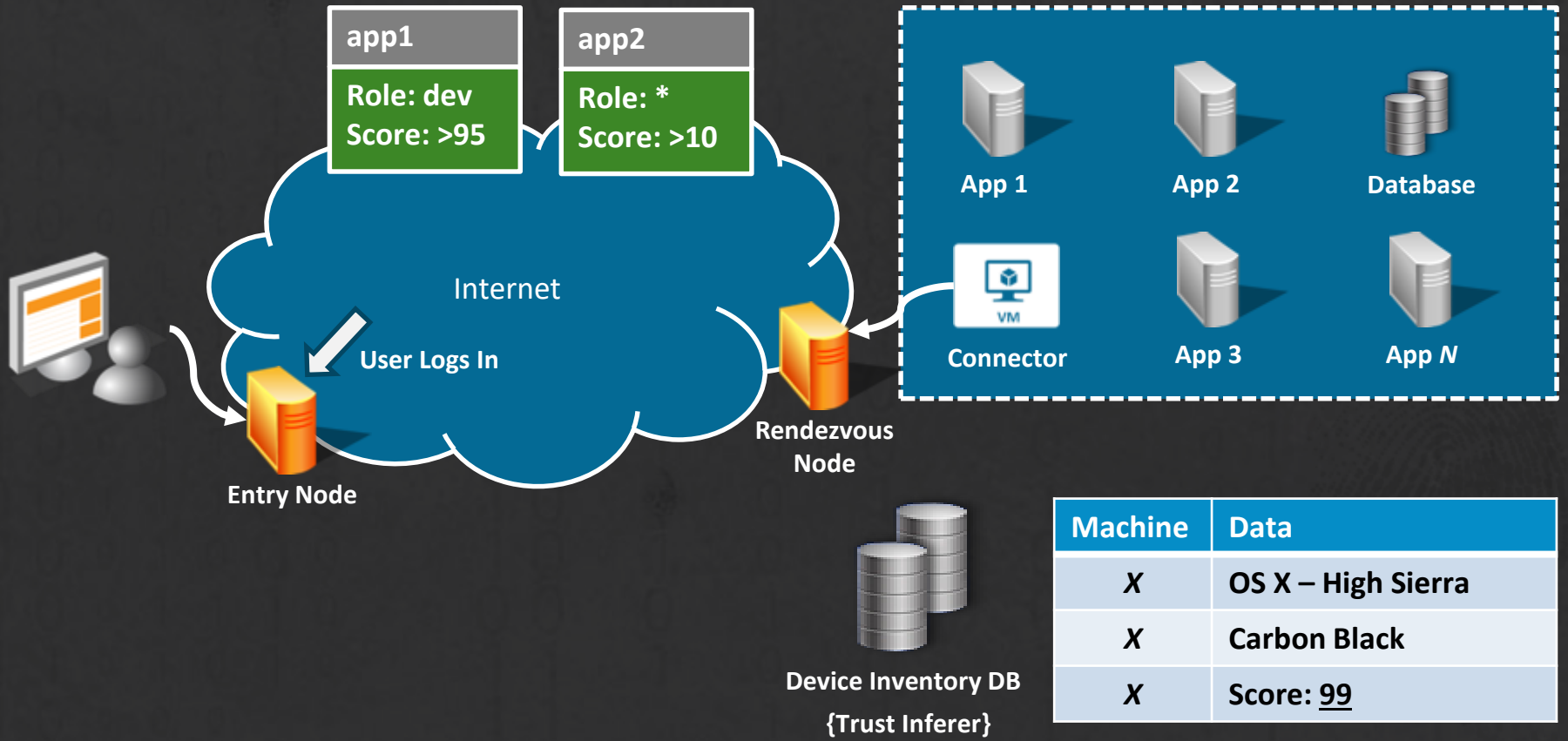
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



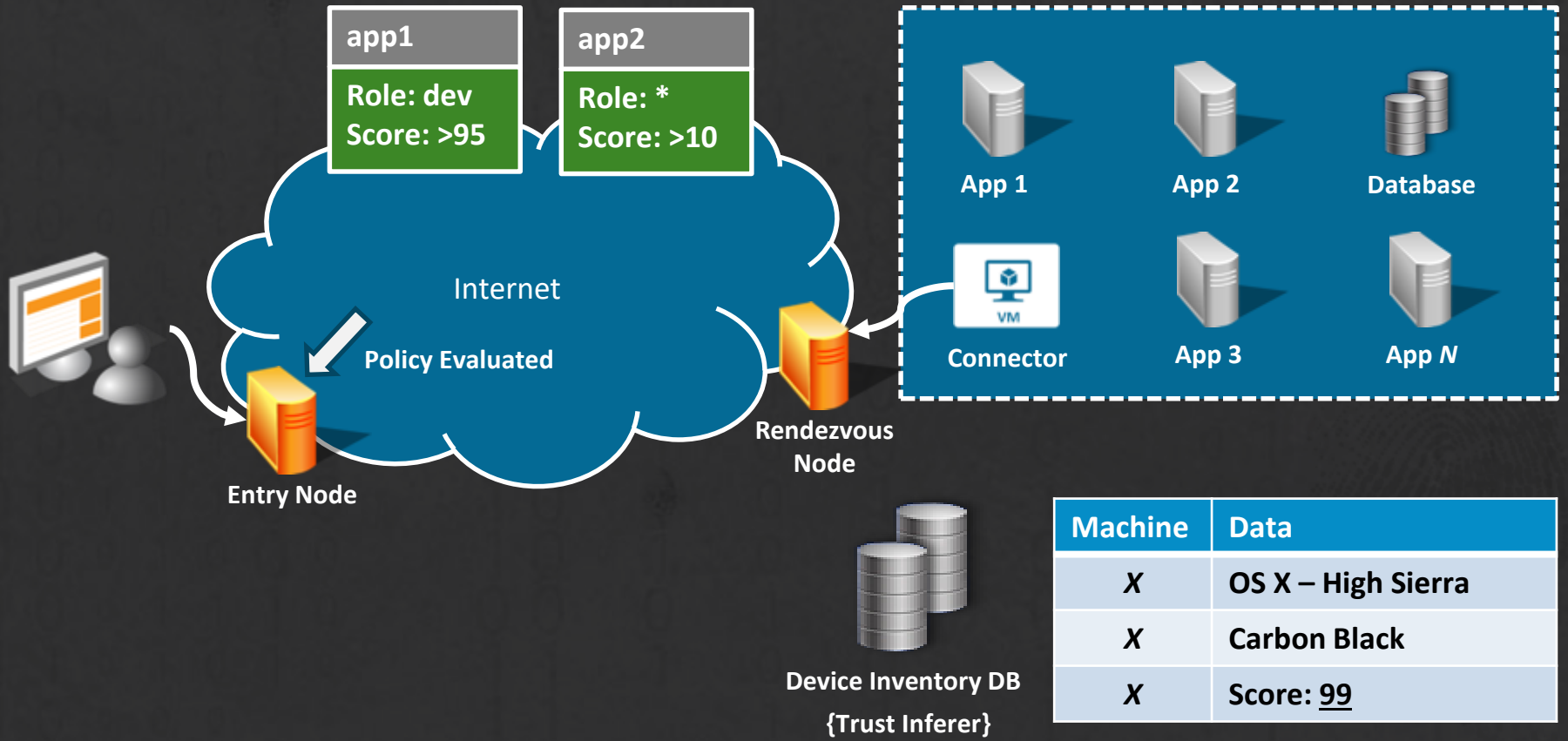
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



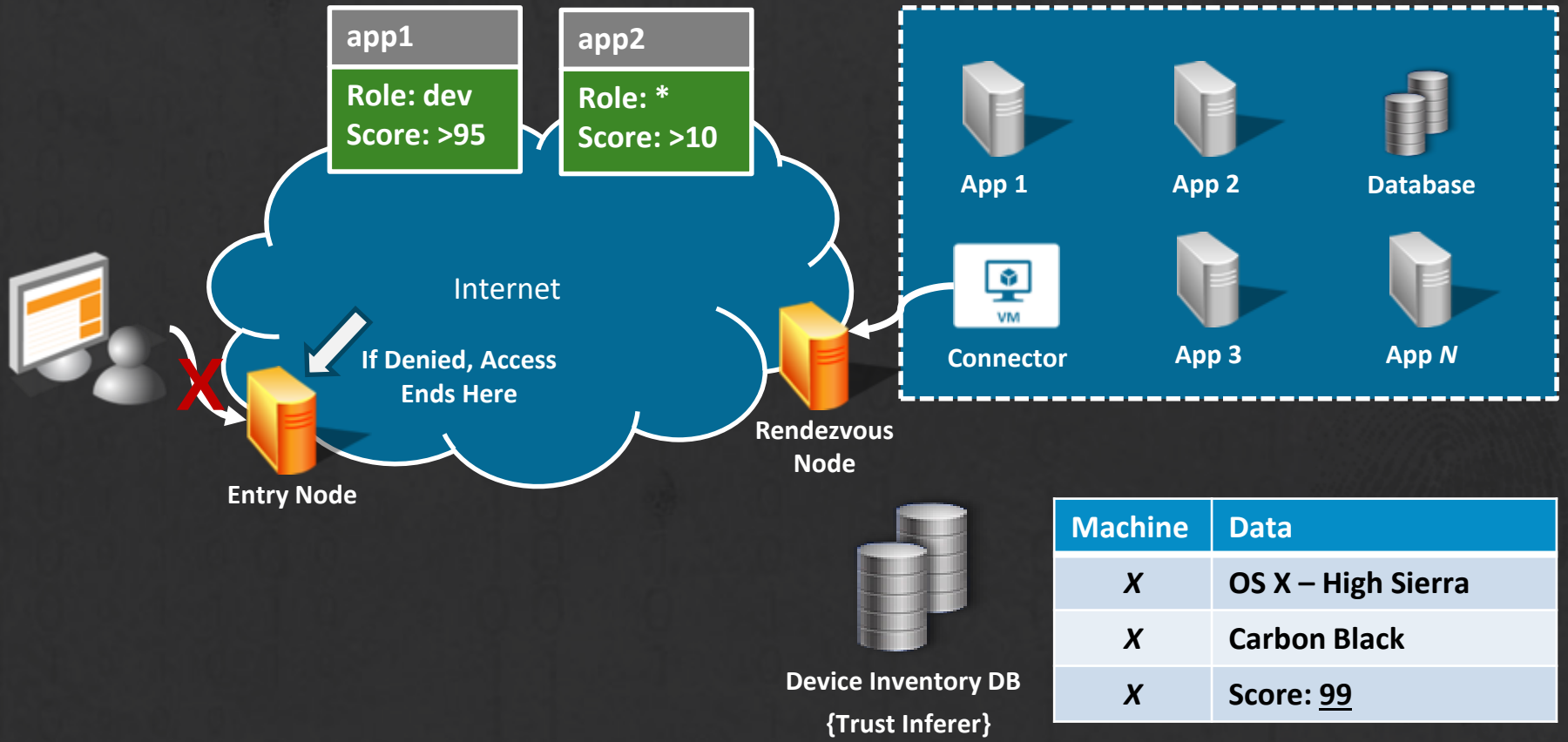
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



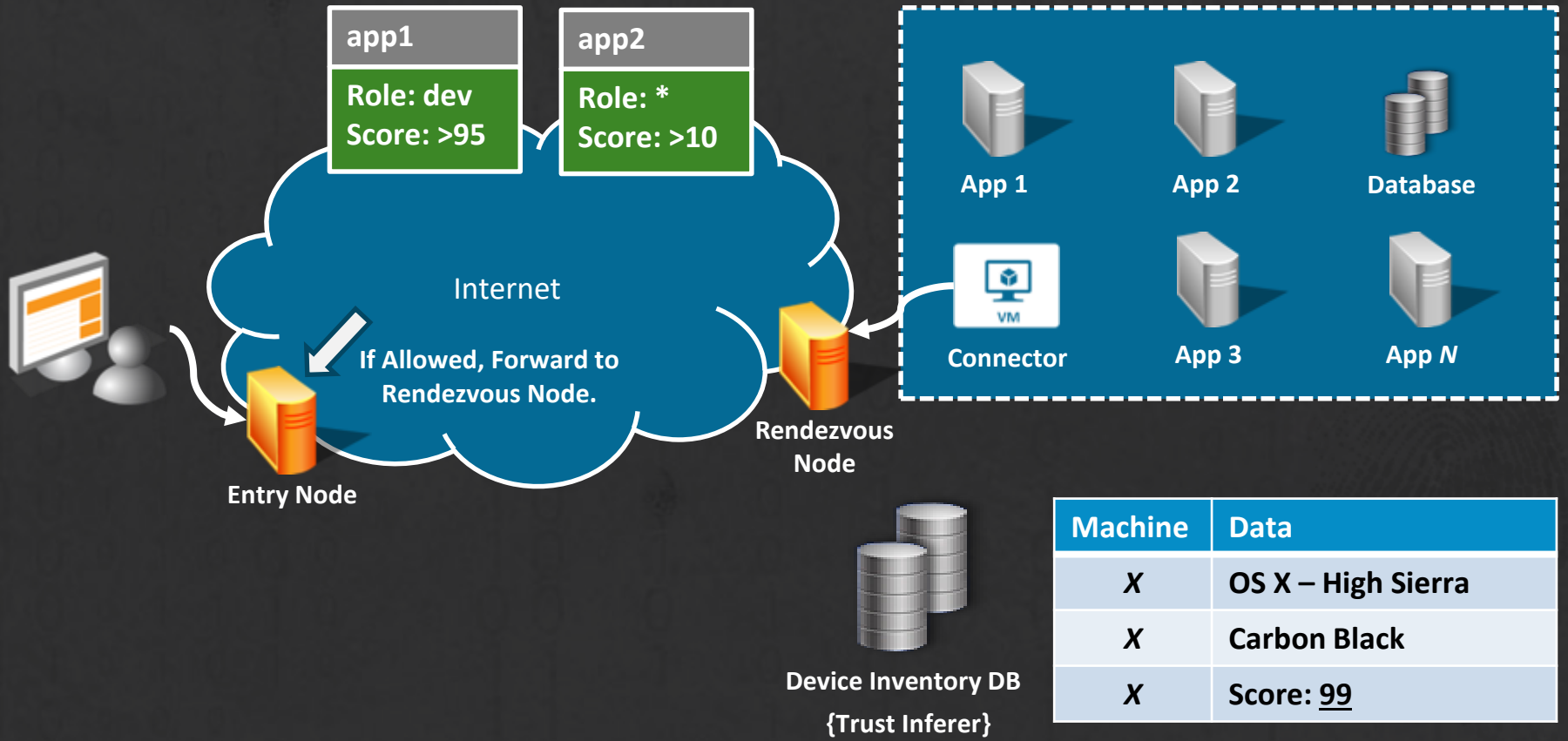
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



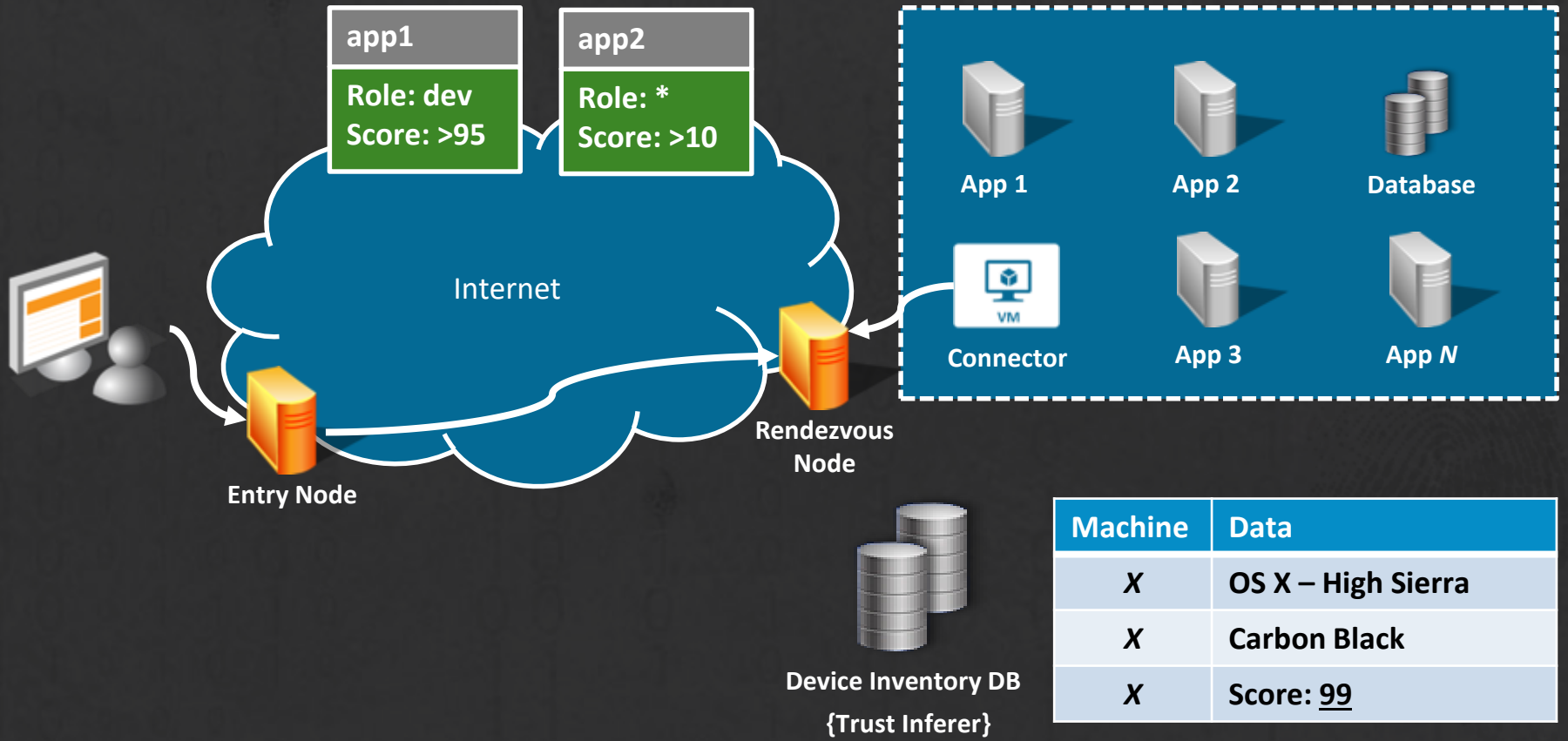
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



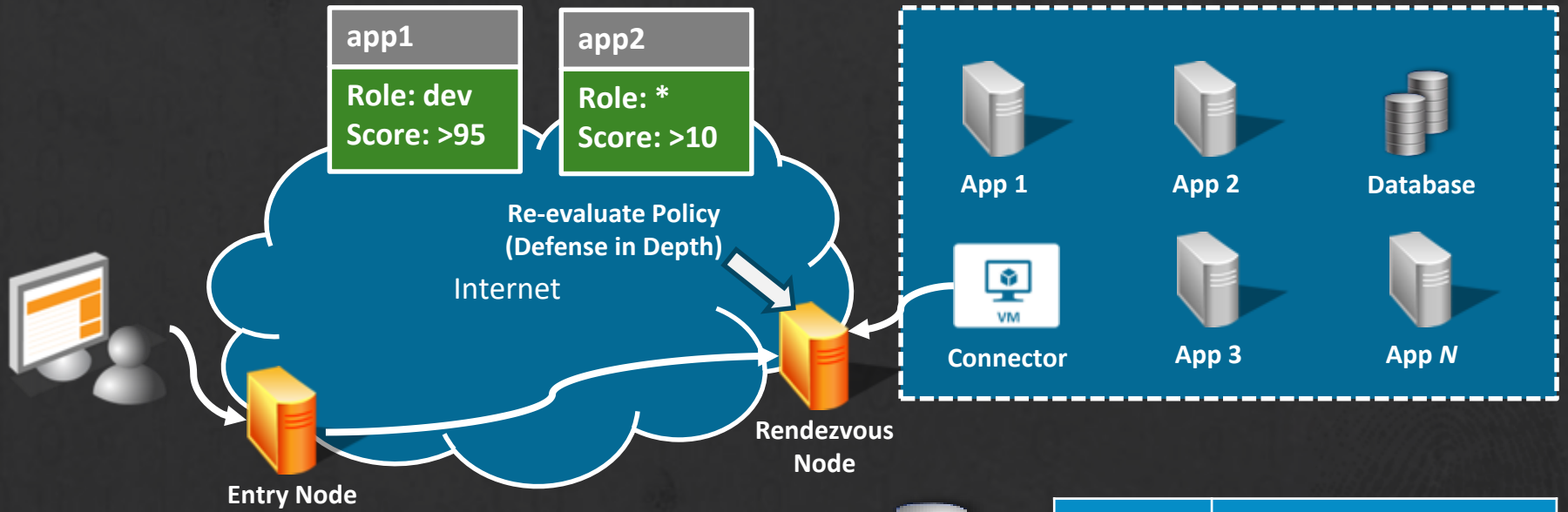
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0

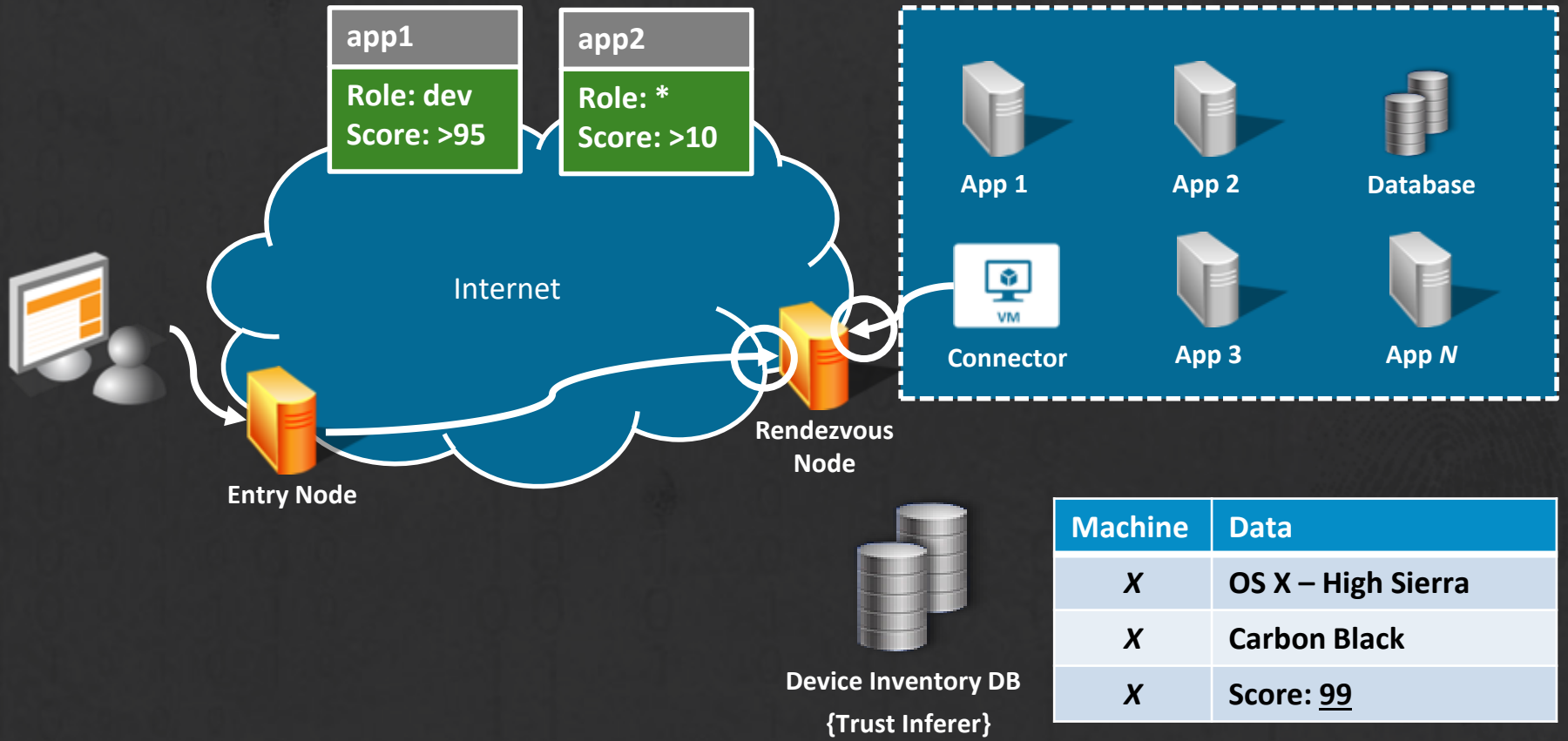


Device Inventory DB

{Trust Inferer}

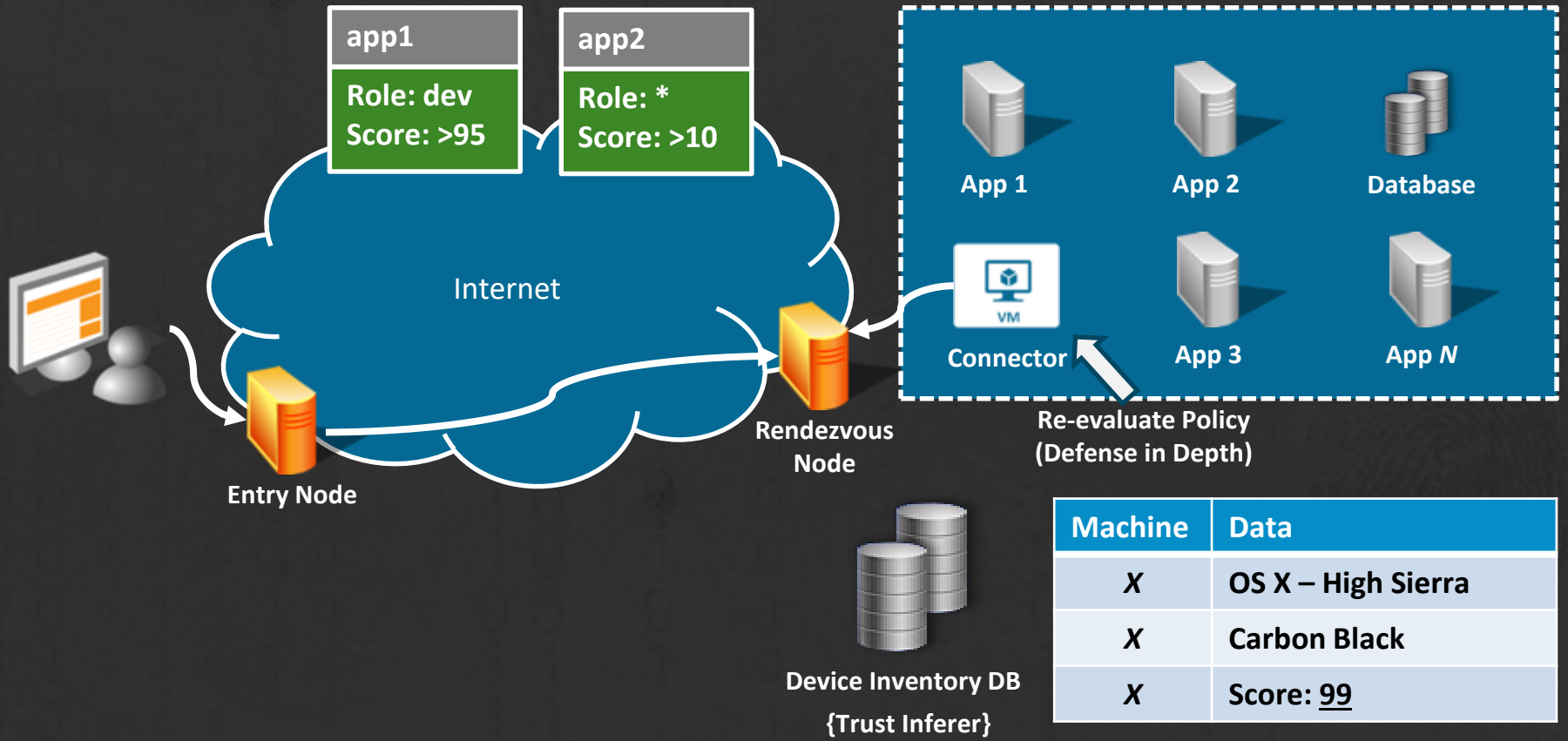
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



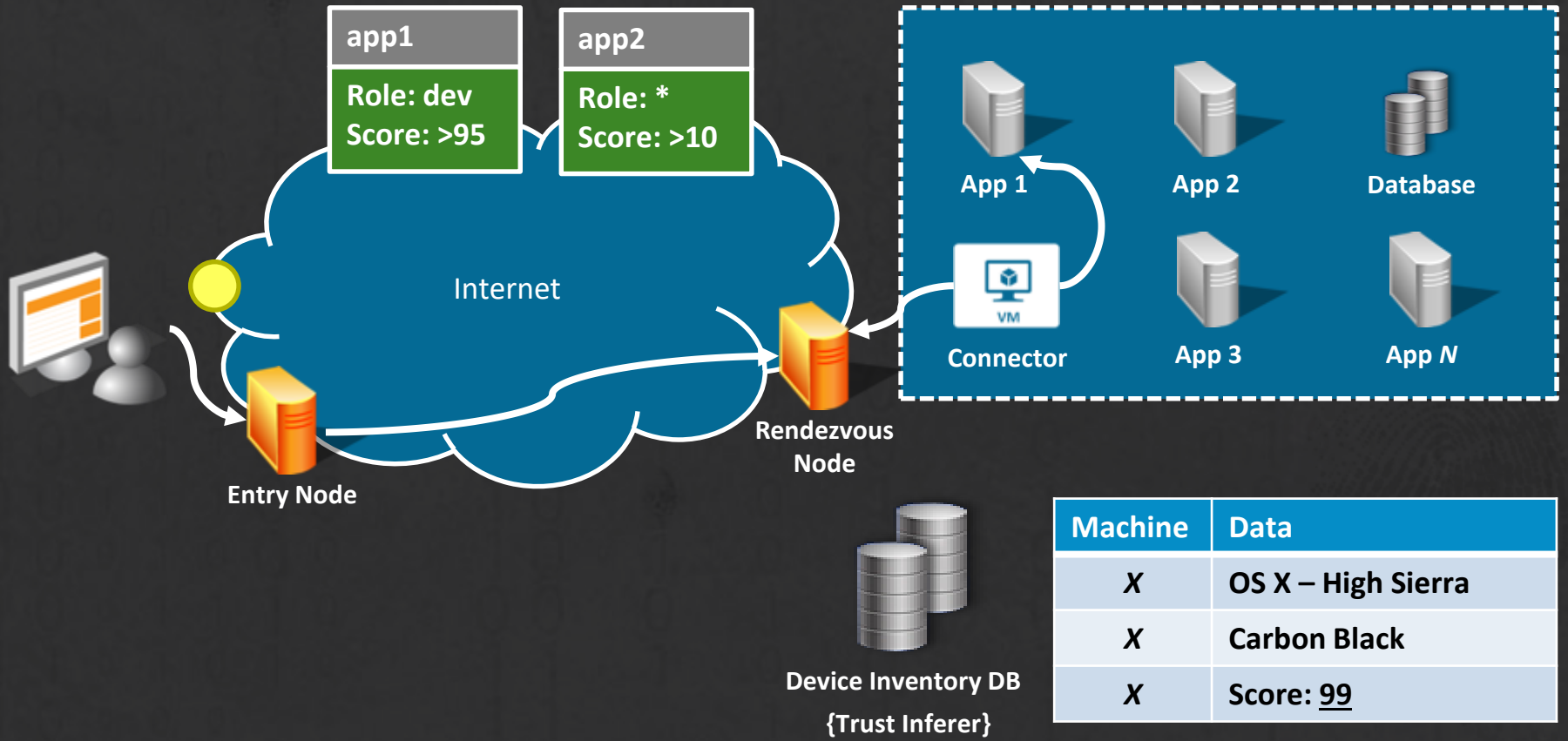
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



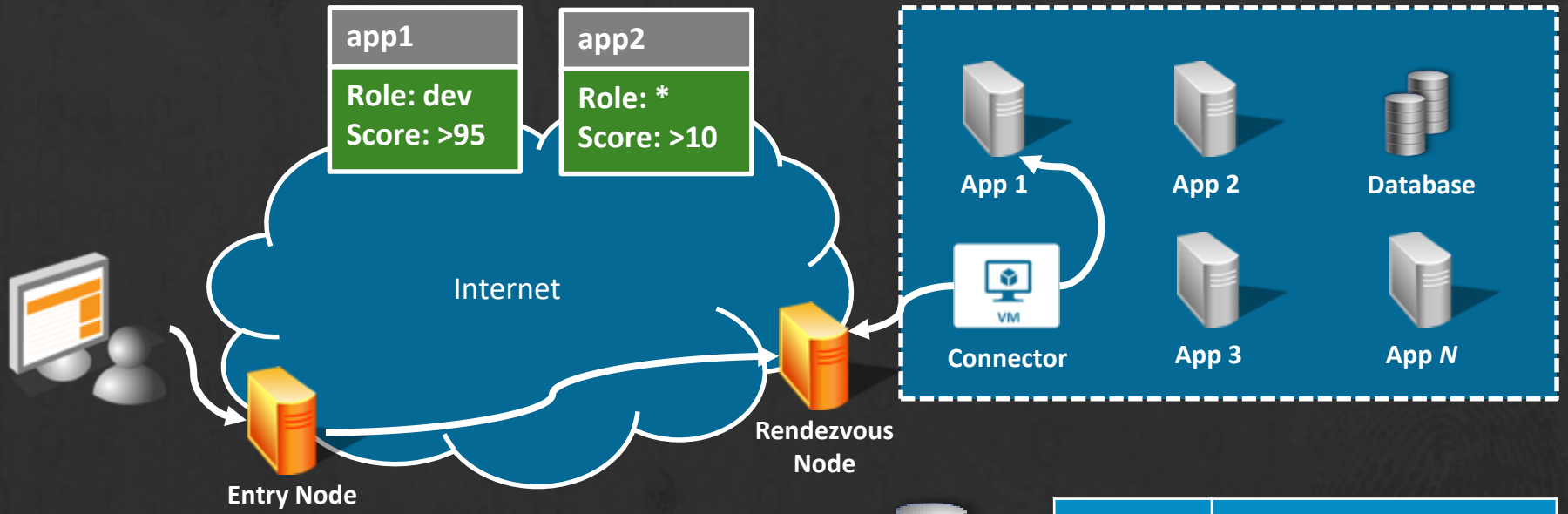
Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0

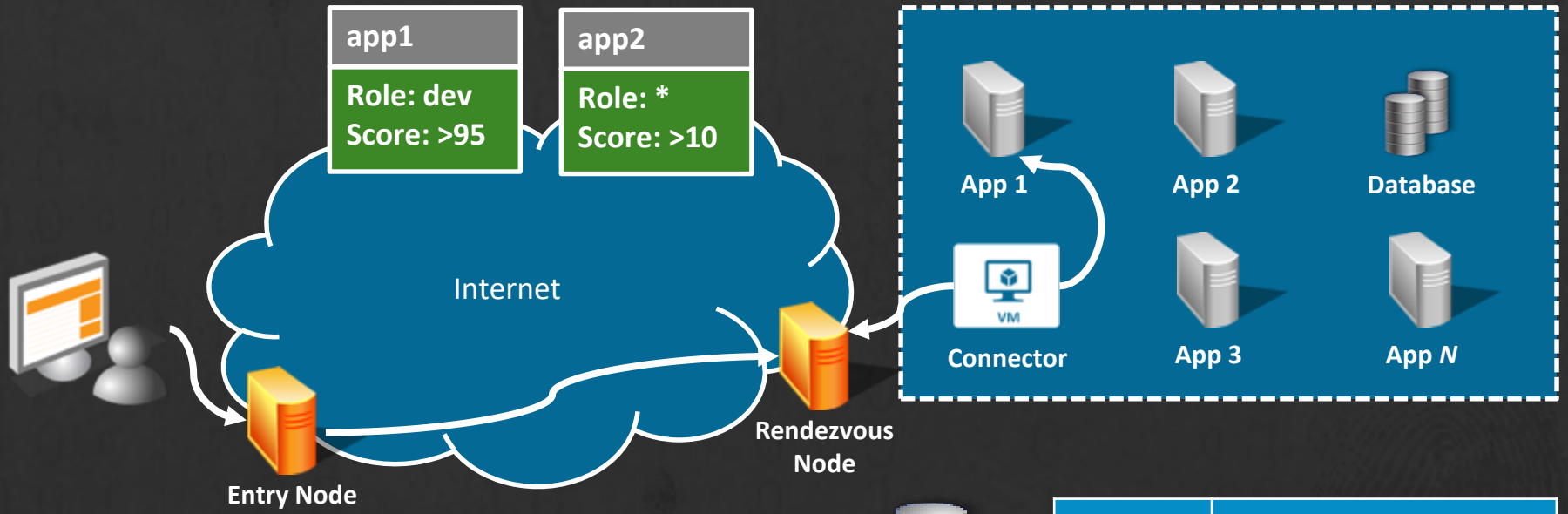


Authorized Users Get Locality Optimizations (Caching).
Attackers Denied Far Away From Assets.
DDOS Can Be Absorbed at Edge of Internet Easier.
Can Be Clientless If Protocol Proxy Friendly.

Device Inventory DB
{Trust Inferer}

Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

Zero Trust 3.0



Split Proxies Give Two Other MAJOR Advantages:

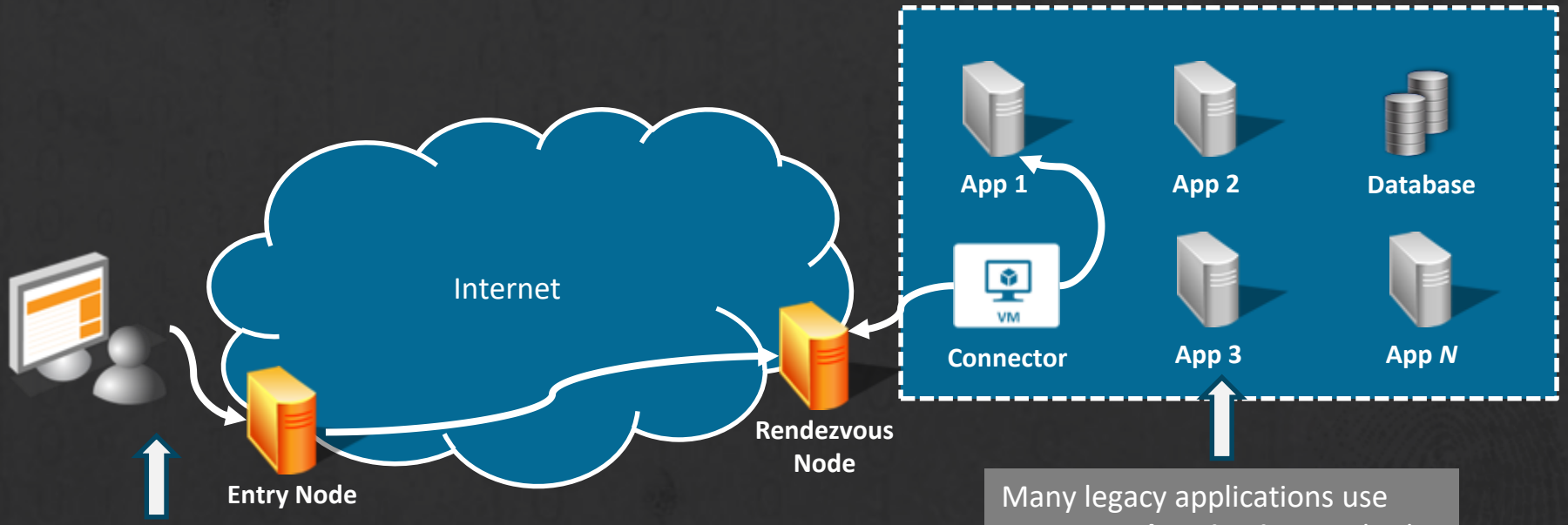
- Legacy Authentication Bridging
- Security Injection

Device Inventory DB

{Trust Inferer}

Machine	Data
X	OS X – High Sierra
X	Carbon Black
X	Score: 99

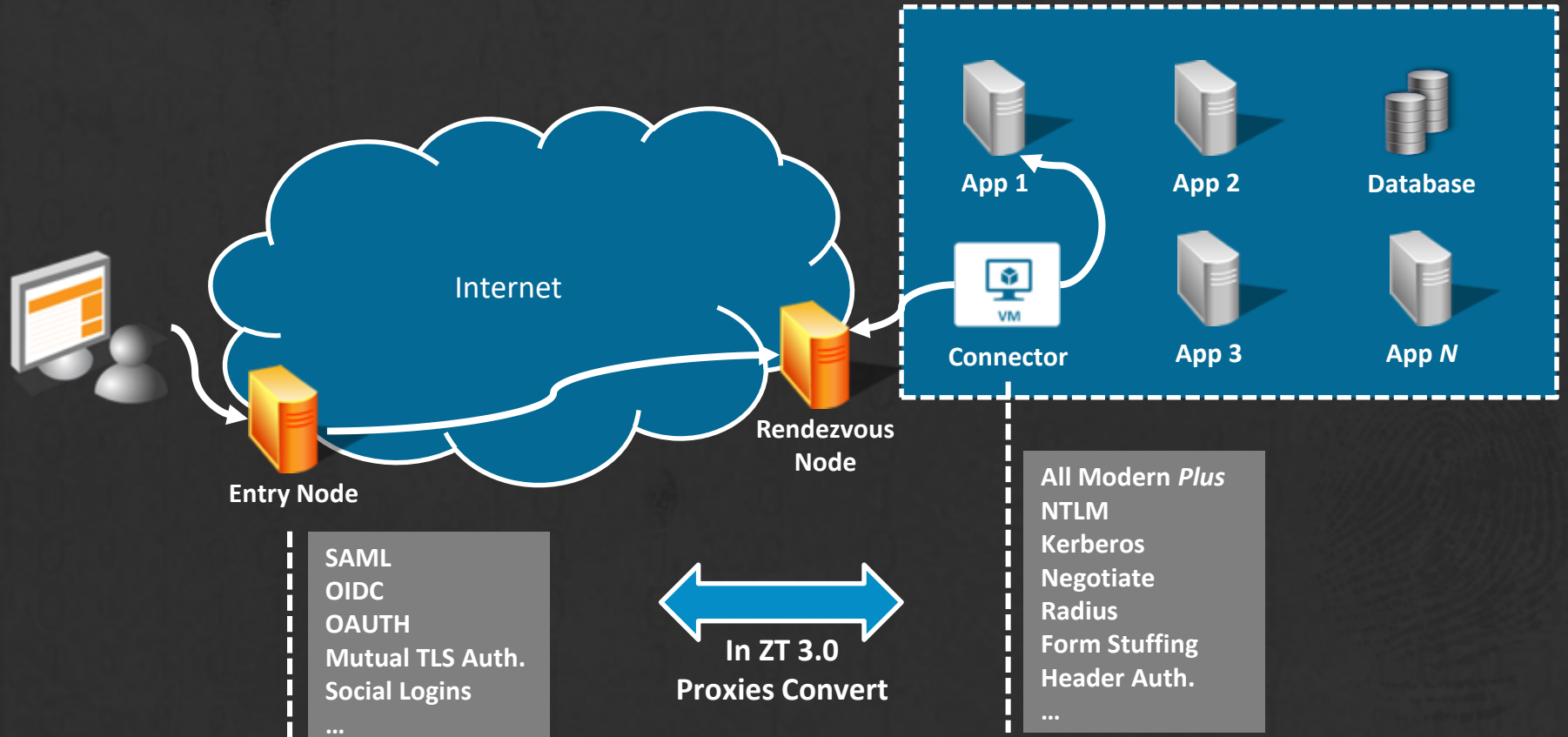
Zero Trust 3.0 :: Legacy Authentication Bridging



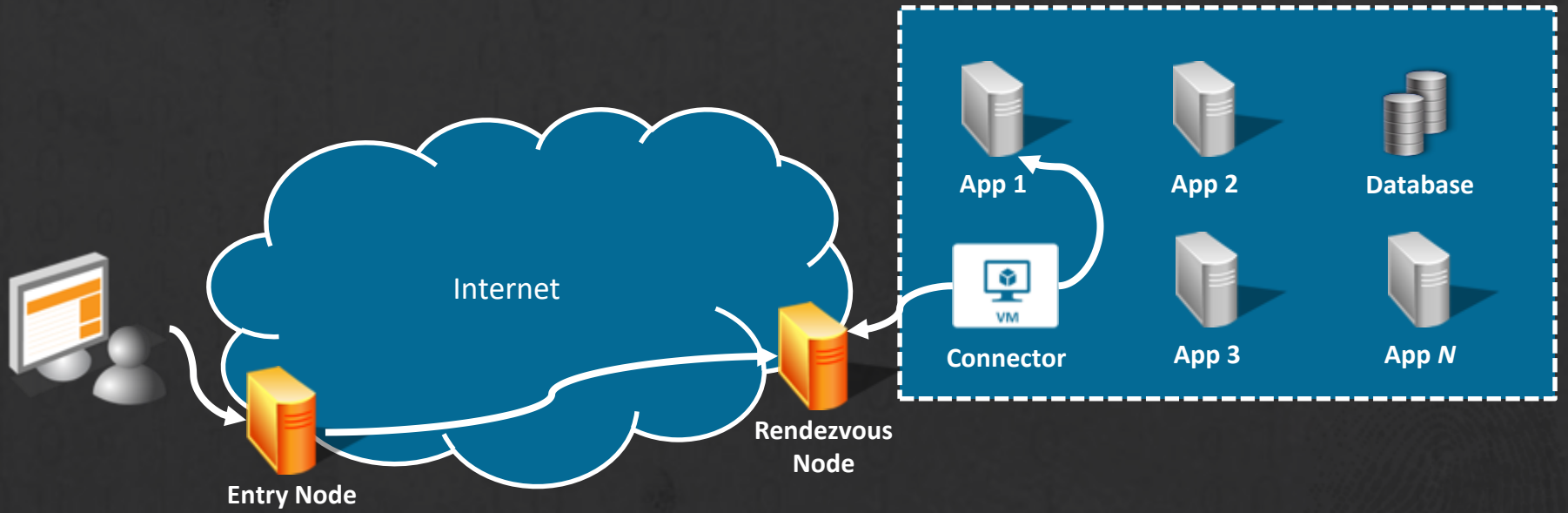
Client outside of any “Perimeter”. Uses modern authentication.

Many legacy applications use **Legacy Authentication** methods like **NTLM, Kerberos, Negotiate, and Radius**. These are **Perimeter Authentication** methods.

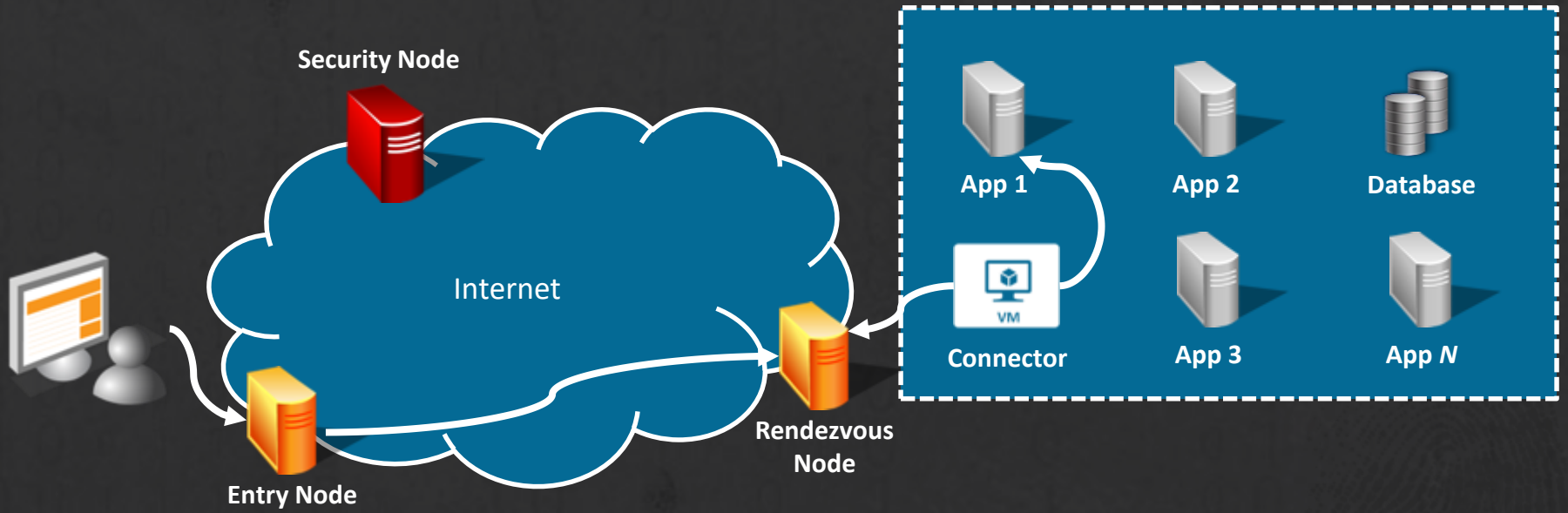
Zero Trust 3.0 :: Legacy Authentication Bridging



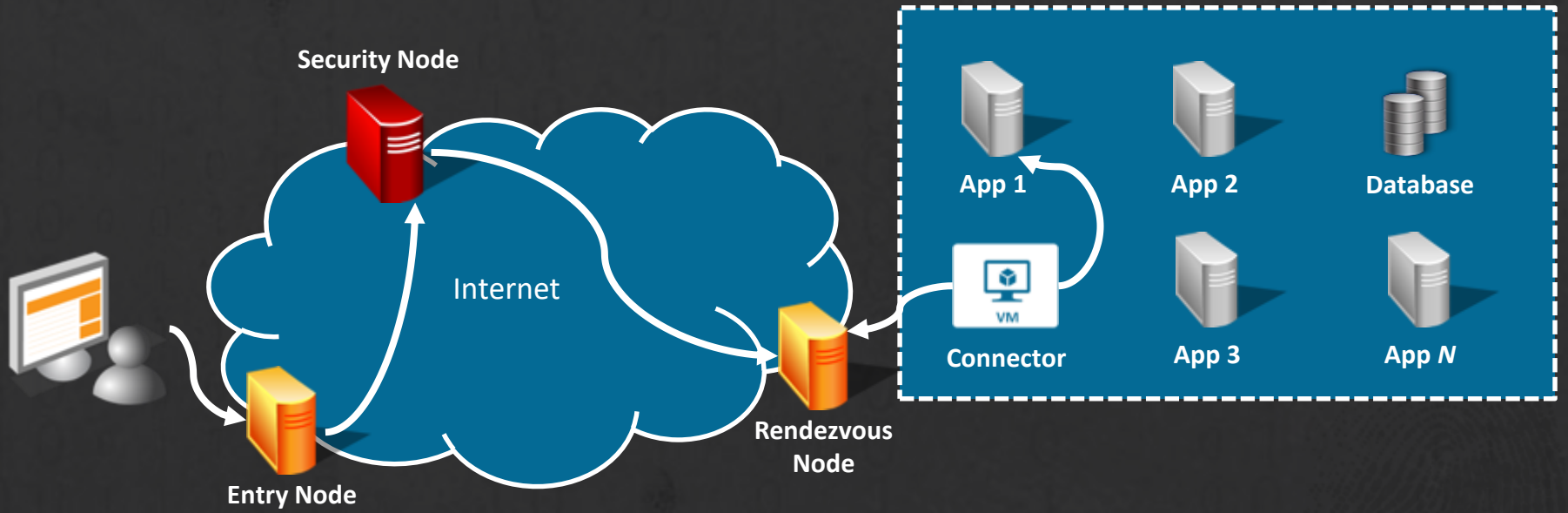
Zero Trust 3.0 :: Security Injection



Zero Trust 3.0 :: Security Injection



Zero Trust 3.0 :: Security Injection



Zero Trust 3.0 :: Security Injection

Security Services

- **Web Application Firewall**

  Studies show your internal sites are much more porous and susceptible to attack. Placing a WAF on all internal sites should be a top priority.

- **Bot Detection**

  The ability to only allow humans to access non-API gateway sites greatly reduces attack surface. Look for providers capable of utilizing AI to discern if you are a human or not based on typematic rate, mouse movements, device orientation, and more.

Zero Trust 3.0 :: Security Injection

Security Services

- **DLP**

  The ability to block protected content from leaving certain applications based on user and group roles is a must in our data economy.

- **Geo/IP/Time Restrictions**

  Look for providers and partners that can restrict access to applications based on geography, Ips and CIDRs, and time of day.

Zero Trust 3.0 Summary

Zero Trust 3.0 Goes *Beyond* BeyondCorp

- **Split Proxies**
  Allows the network to keep attackers far away from critical resources and provide locality and caching to authorized users.

- **Legacy Authentication Bridging**
  Allows conversion of authentication methods from modern protocols such as SAML and OIDC to legacy perimeter methods such as NTLM and RADIUS.*

  **WARNING: Tunnels cannot do this.*

Zero Trust 3.0 Goes *Beyond* BeyondCorp

- **Security Injection and Data Comms. Posture Assessment**

  Allows inspection, blocking, and modification of application streams. Many providers will have built-in primitives. Look for someone with a thick internal ecosystem and the ability to *service chain* to third parties.

  **WARNING: Tunnels cannot do this.*

- **Multi-Cloud Support**

  Zero Trust 3.0 treats Data Centers, IaaS VPCs, etc. all the same. Simply create a perimeter that houses your applications and data, give everything private IP addresses, and install a connector!

Summary

Zero Trust is a journey.

Managed services and partnerships will be key.

Your partners, plans, and integrators must be able to *phase* this in.

Mixing of strategies can have value. For example, Micro-Segmentation *within* a Zero Trust 3.0 Micro-Perimeter can prevent lateral movement.

Moving Beyond Perimeter Security

A comprehensive & achievable roadmap to less risk

8 Steps To Zero Trust

1. App Precheck
2. Access Proxy Prep
3. Test Lab Enrollment
4. Security Upgrade
5. Performance Upgrade
6. External User Enrollment
7. Internal User Enrollment
8. VLAN Migration

8 Steps To Zero Trust

A comprehensive guide & roadmap to Zero Trust by Akamai CTO Charlie Gero

Zero Trust Ref. Architecture

Simple visual guide on how to apply Zero Trust across common environments

akamai.com/zerotrust


THANK YOU