Endace

Rapid Fault Resolution
and Threat Response

Endace: Protecting Reputations

15 years in business

100% Network History

Protecting the world's biggest networks

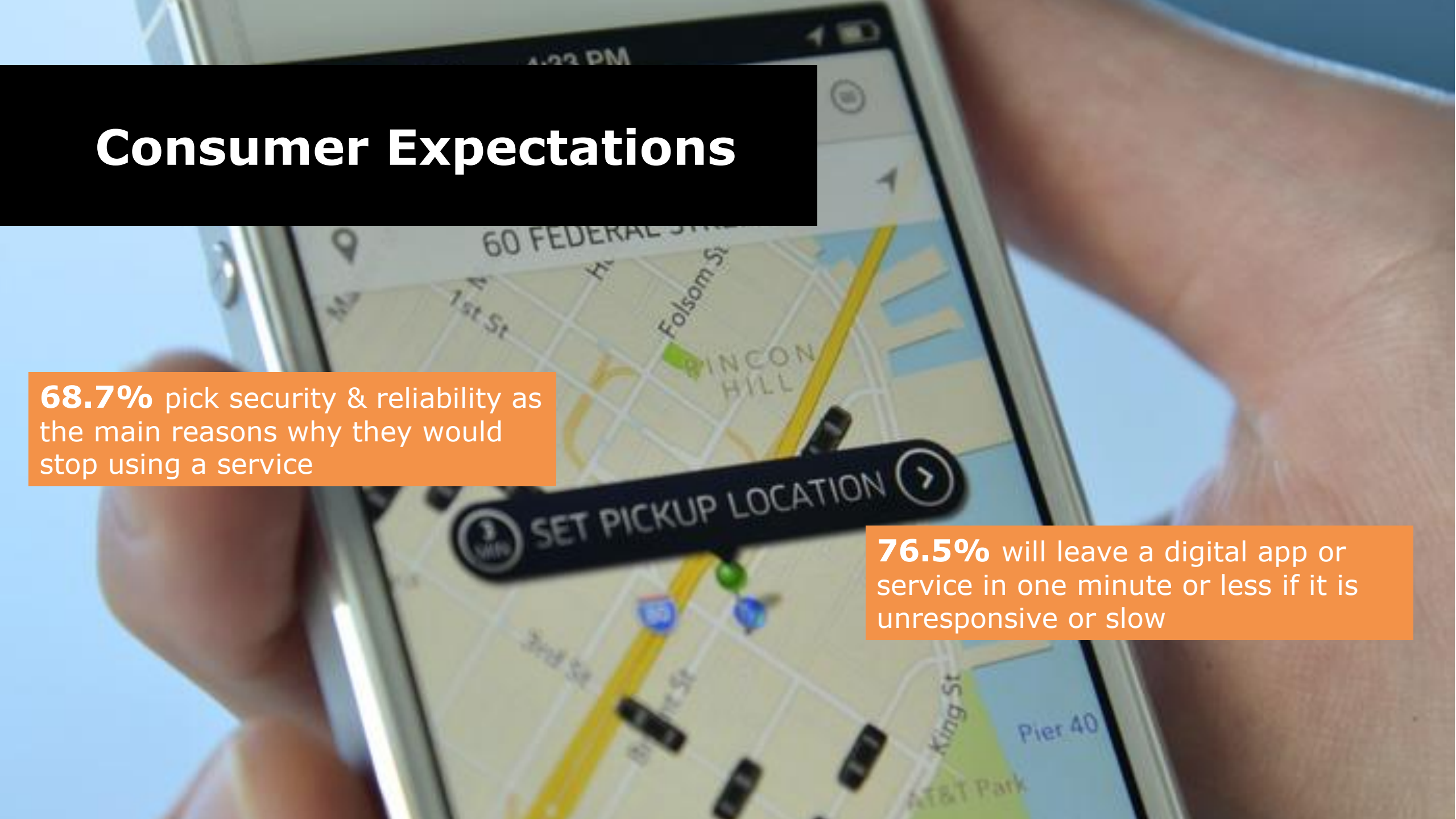
Renowned for reliability and innovation

We Serve

- 5 of the Top 10 Global Telcos
- 5 of the Top 10 US Commercial Banks
- 2 of the world's 3 largest Exchanges
- 4 of the Top 10 Fortune 50
- Trusted supplier to Government and Military

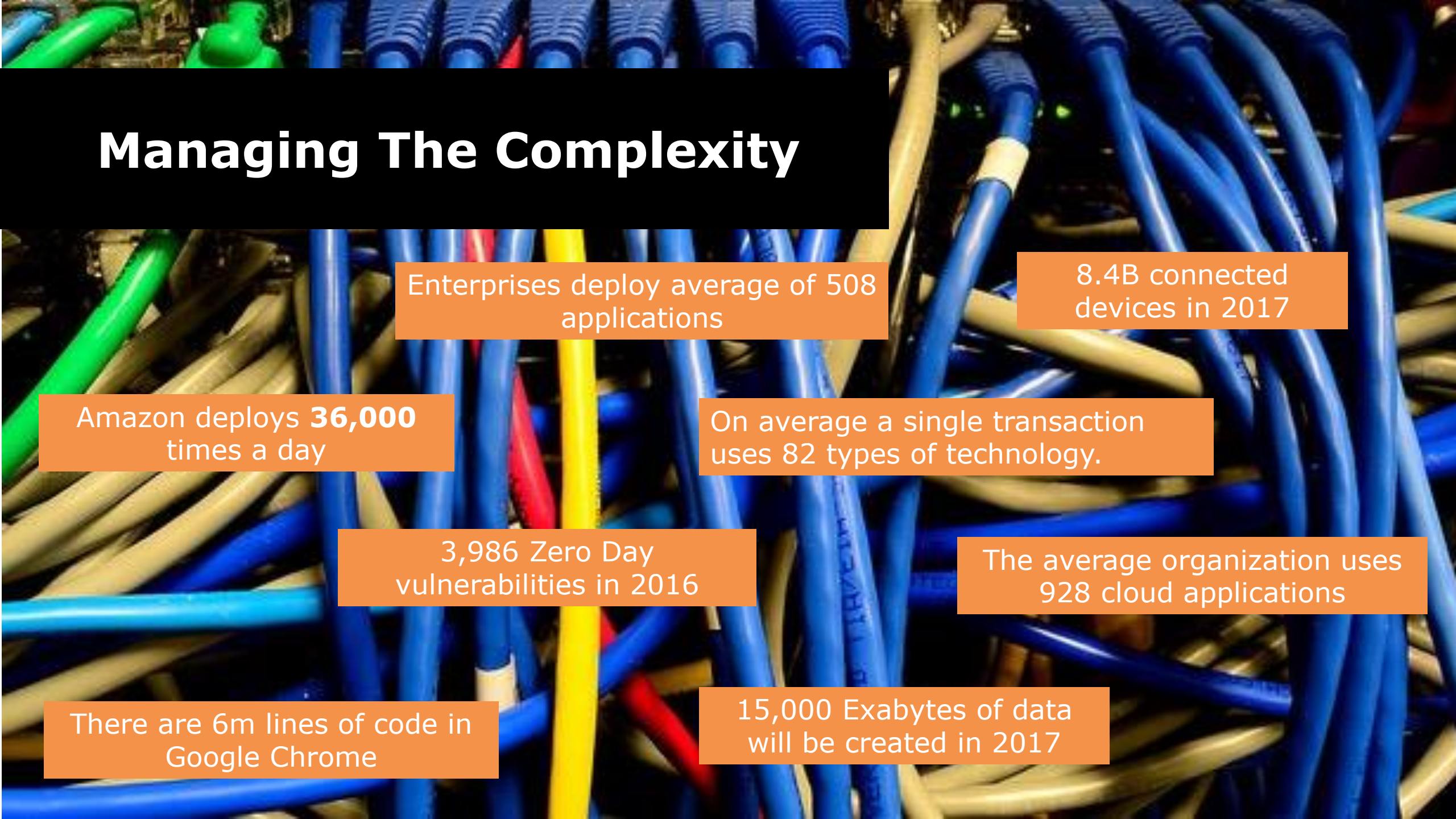

The Bottom Line
Average security breach costs
$7.35M
$5,600 per minute
average downtime cost
1 second slower = $1.6B
less revenue at Amazon.com
Fortune 1000 companies average total
downtime cost $1.3B~$2.5B
Cybercrime cost global economy
$450B in 2016

Consumer Expectations



68.7% pick security & reliability as the main reasons why they would stop using a service

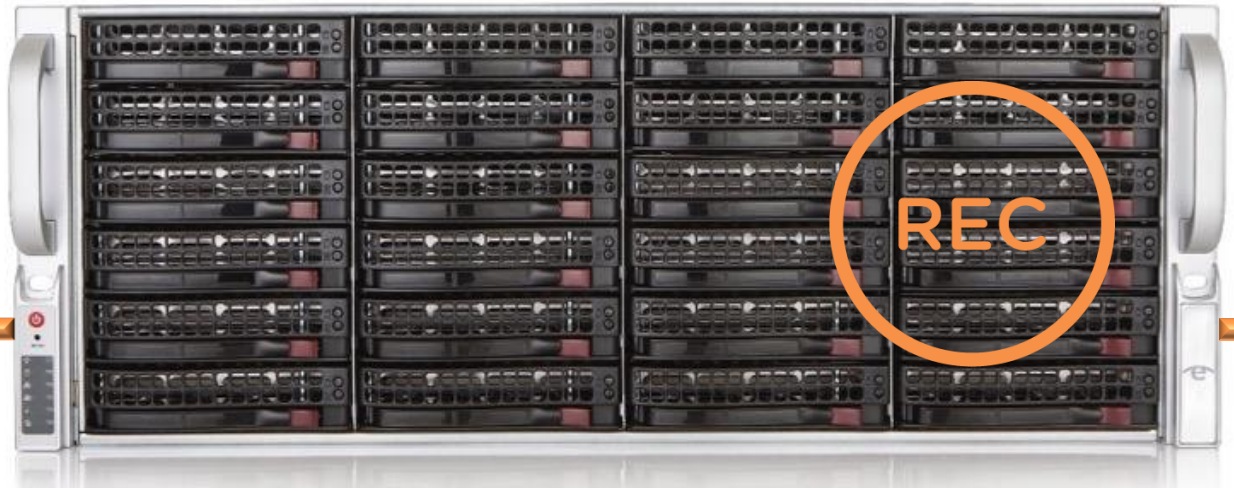
76.5% will leave a digital app or service in one minute or less if it is unresponsive or slow


Managing The Complexity
Enterprises deploy average of 508 applications
8.4B connected devices in 2017
Amazon deploys **36,000** times a day
On average a single transaction uses 82 types of technology.
3,986 Zero Day vulnerabilities in 2016
The average organization uses 928 cloud applications
There are 6m lines of code in Google Chrome
15,000 Exabytes of data will be created in 2017

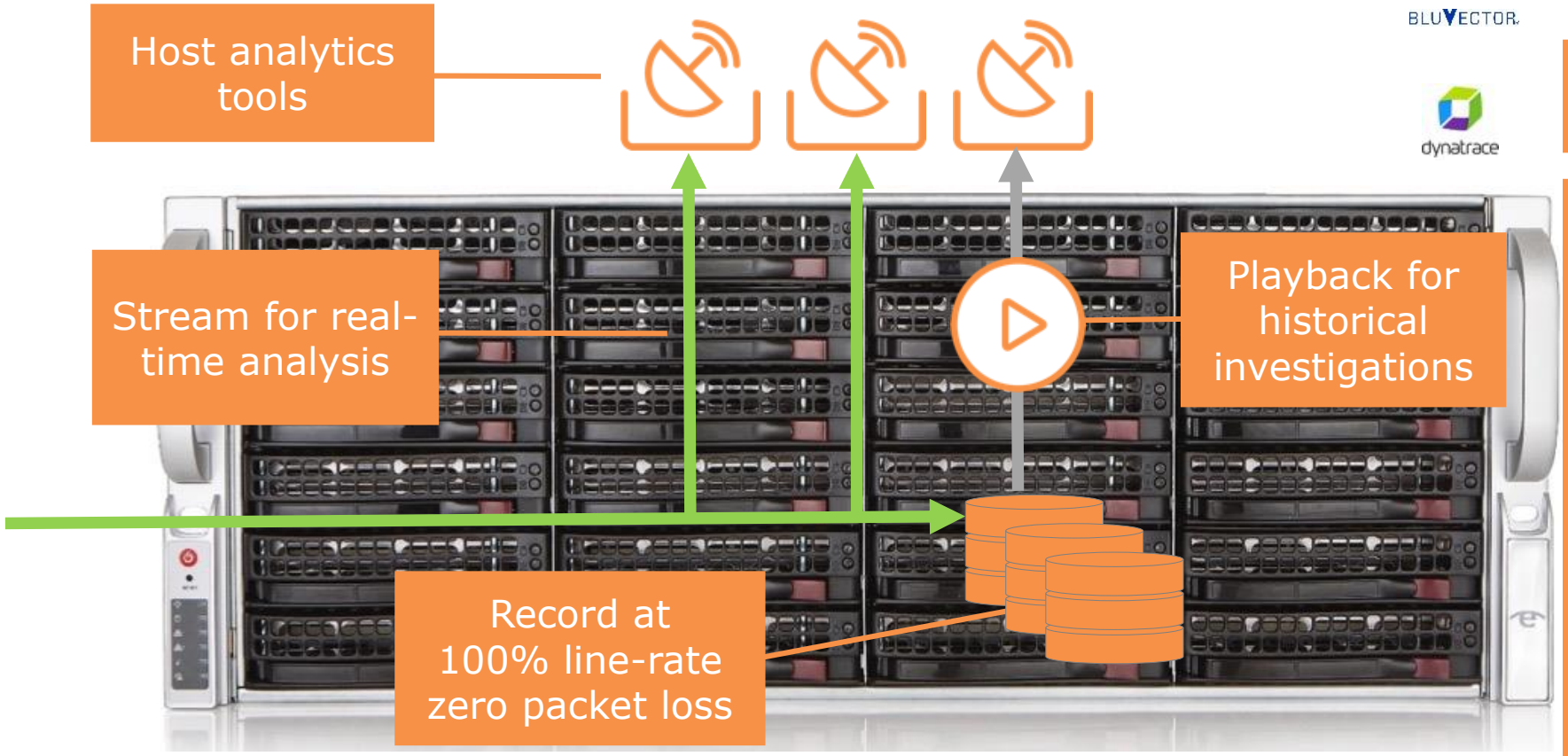
It All Happens On The Network

The evidence is in the network traffic

If you record it, you can **definitively see** what happened



EndaceProbe Analytics Platform



Integrated with your chosen tools

API

splunk>
cisco Solution Partner
STEALTHWATCH
idappcom
Gigamon
plixer
paloalto NETWORKS
dynatrace
TRACE
ixia A Keysight Business
IBM Security
BLUVECTOR

Custom and Open-Source Tools

The Traditional Approach

Dedicated Appliances

Endace Network Analytics Platform

splunk> · plixer · paloalto NETWORKS · dynatrace

Cisco Solution Partner · Gigamon · IBM QRadar · SNORT

ArcSight An HP Company · STEALTHWATCH · SURICATA · argus

idappcom · BLUVECTOR · ixia A Keysight Business

DARKTRACE

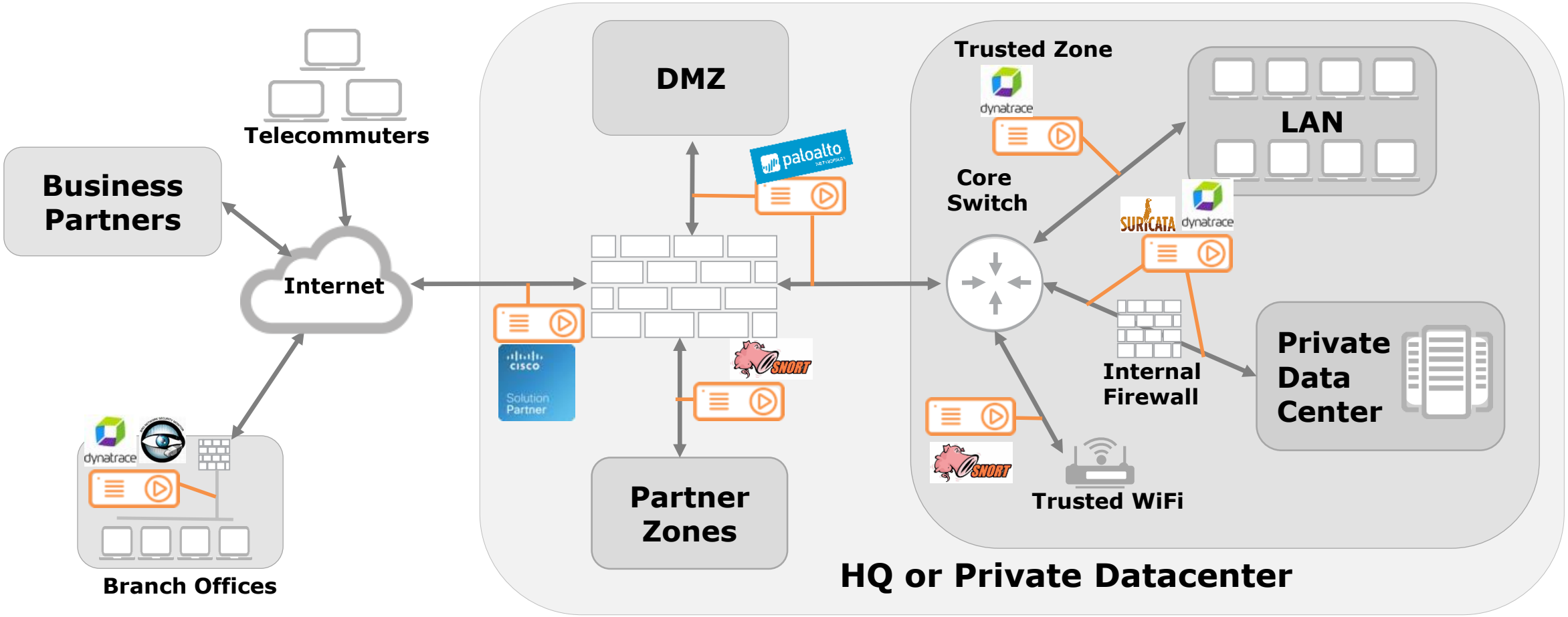
Fusion Partners

Flexible, Scalable, Low TCO

EndaceProbe, Single Source of Truth For All

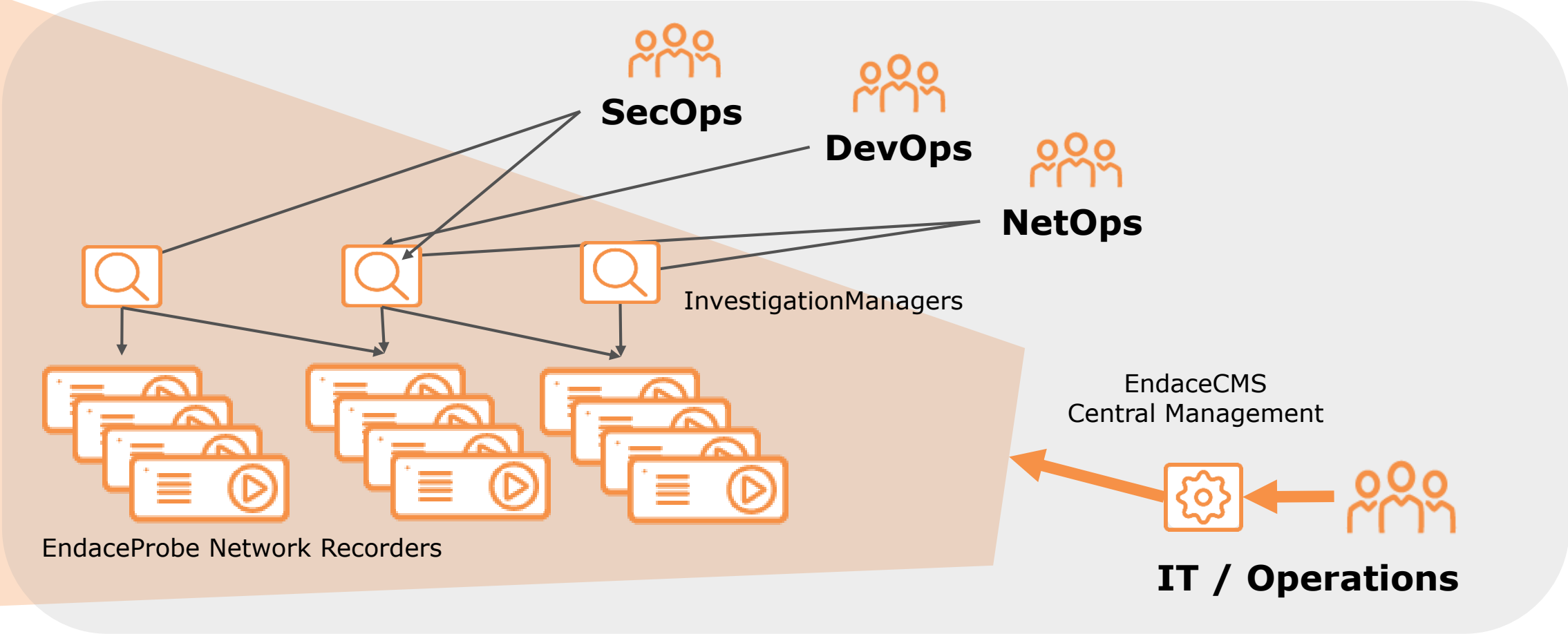
Security, Application Performance and Network Health

Deploying Endace Open Platform



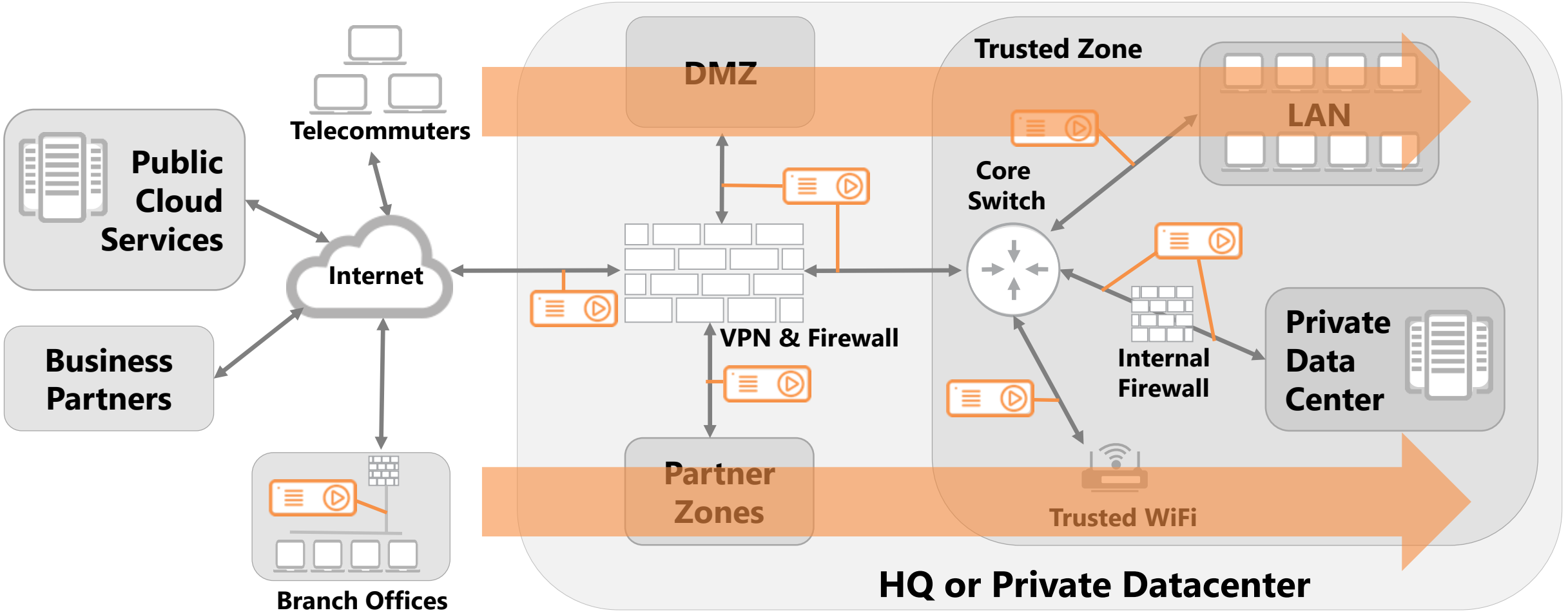
Deploy Tools on EndaceProbe Open Platform.

EndaceFabric Scalable Architecture



Rapid Fault Resolution for DevOps

An End-To-End View Of Transactions



Example – Resolving A DevOps Release Failure

1 REC → 2 → 3 → 4

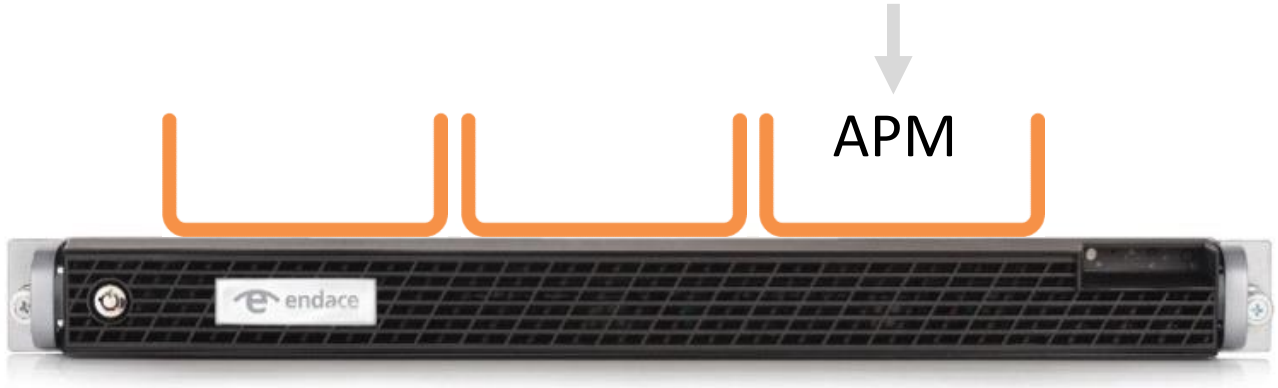
Record your Network Traffic

New E-Commerce application version deployed

Issue reported, rollback done

Playback to hosted APM tool for deep analysis.

What broke the release this morning?



Rapid Investigation for SecOps

The Security Landscape

Firewalls
IPS
Antivirus
Antimalware

IDS
AI based Analytics
NBAD
Threat Intelligence

Largely
Manual

Investigation: The Traditional Approach

The Process

Review and Correlate:

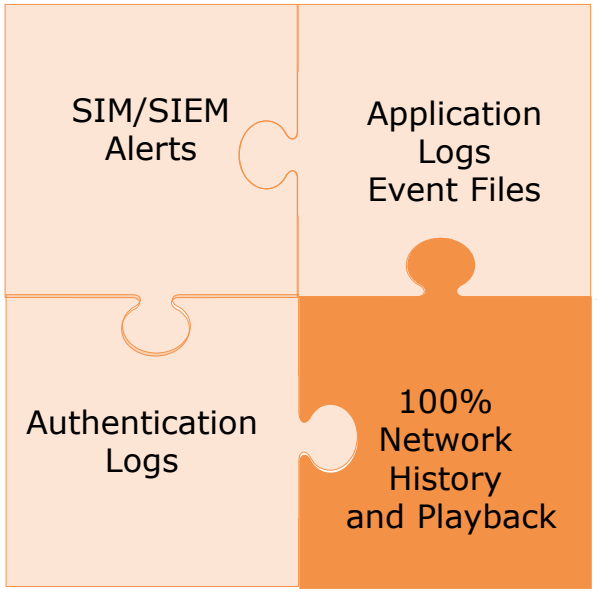
- SIM/SIEM events
- System logs
- Authentication Logs
- Application Logs
- etc

You formulate a theory and look for evidence to support it

But

It's slow, resource intensive and frequently inconclusive

Investigation: Using Recorded Network History



The Process

- Evidence-based forensics
- Analytics tools point to the problems, packets provide the evidence
- Integration with security tools enables fast, conclusive issue investigation

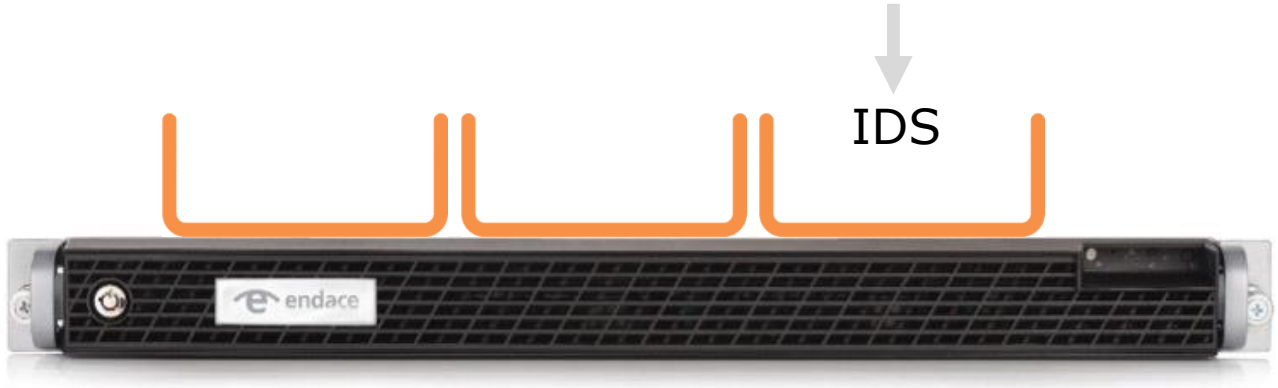
BUT

You need to be continuously recording the history before the event

Example 1 – Dealing With A Zero Day Threat

1. **Record your Network Traffic**
2. **New Zero Day Threat emerges**
3. **New IDS or Firewall rule is released**
4. **Playback to IDS with new rule.**

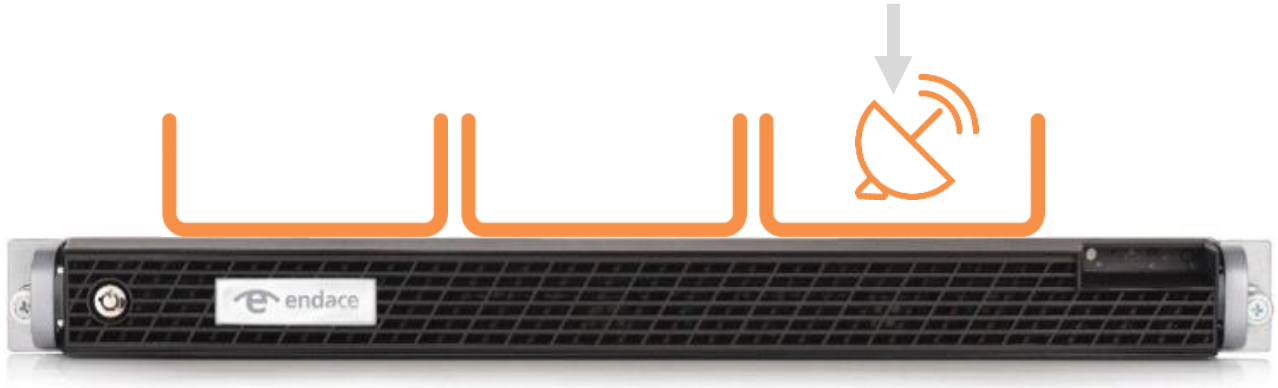
Was my network compromised?



Example 2 – Incident Response & Reporting

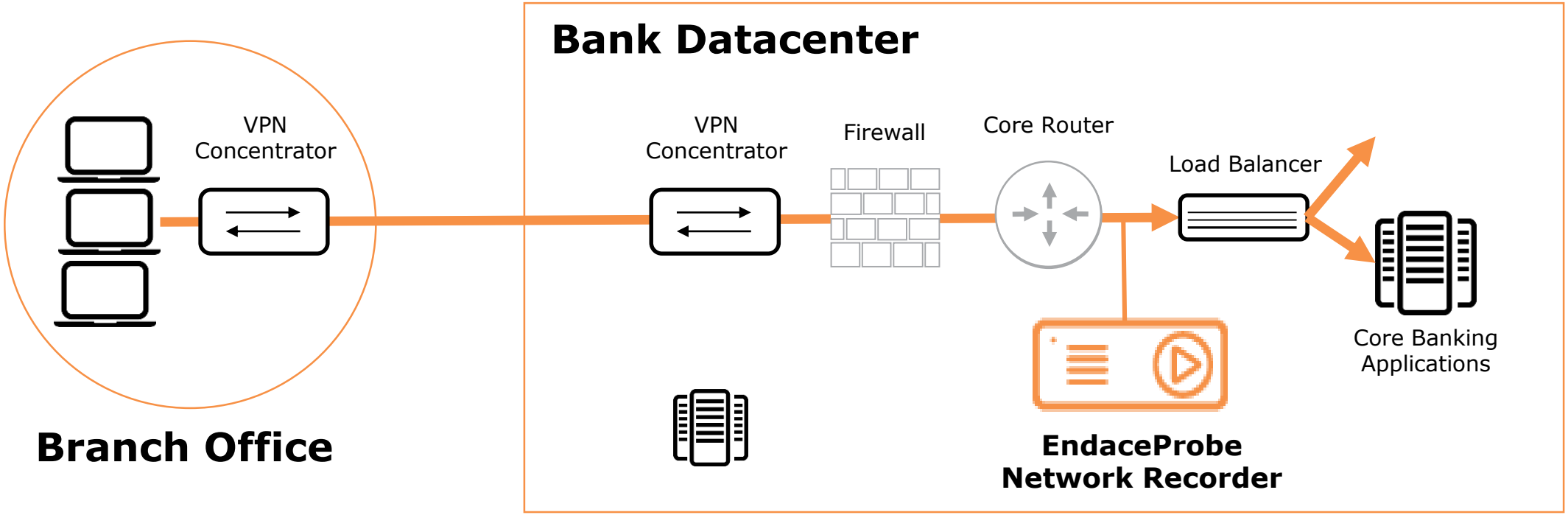
1. **Record your Network Traffic**
2. **Security Tool raises an alert**
3. **Pivot to EndaceVision and EndacePackets to investigate details**
4. **(Optional) Playback to analytics tools for deep analysis**

Was my network compromised?
What data did I lose?



Rapid Fault Resolution for NetOps

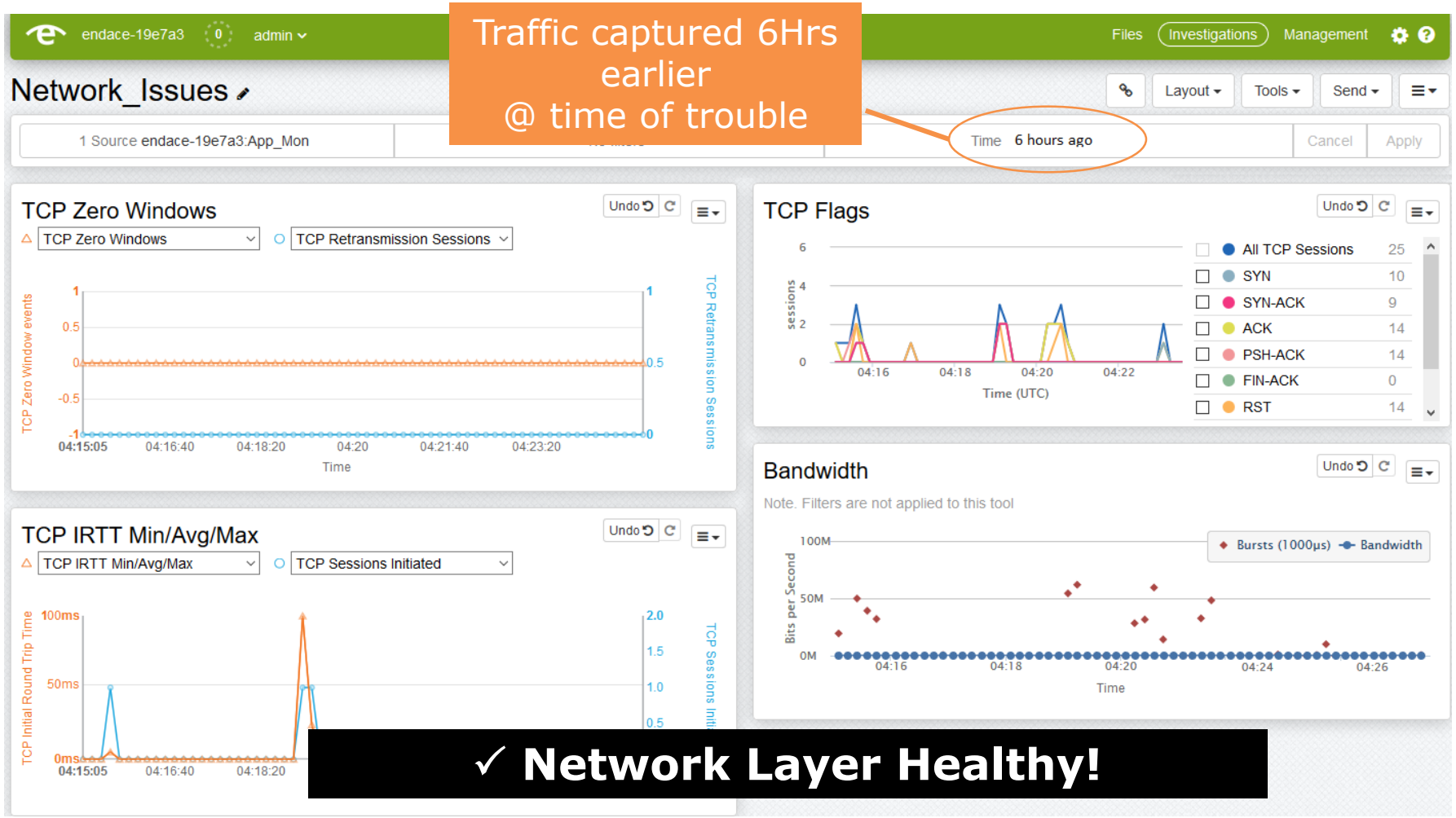
Transactions “Hanging” At Bank Branches



Bank Tellers complaining “**transactions sometimes hang**”.
IT Operations **suspect network is congested** and dropping packets

Investigate Network Traffic In EndaceVision

Traffic captured 6Hrs earlier @ time of trouble



No TCP retransmits or zero windows

TCP flags normal

Low round trip time (RTT) <100ms.

Network bandwidth low

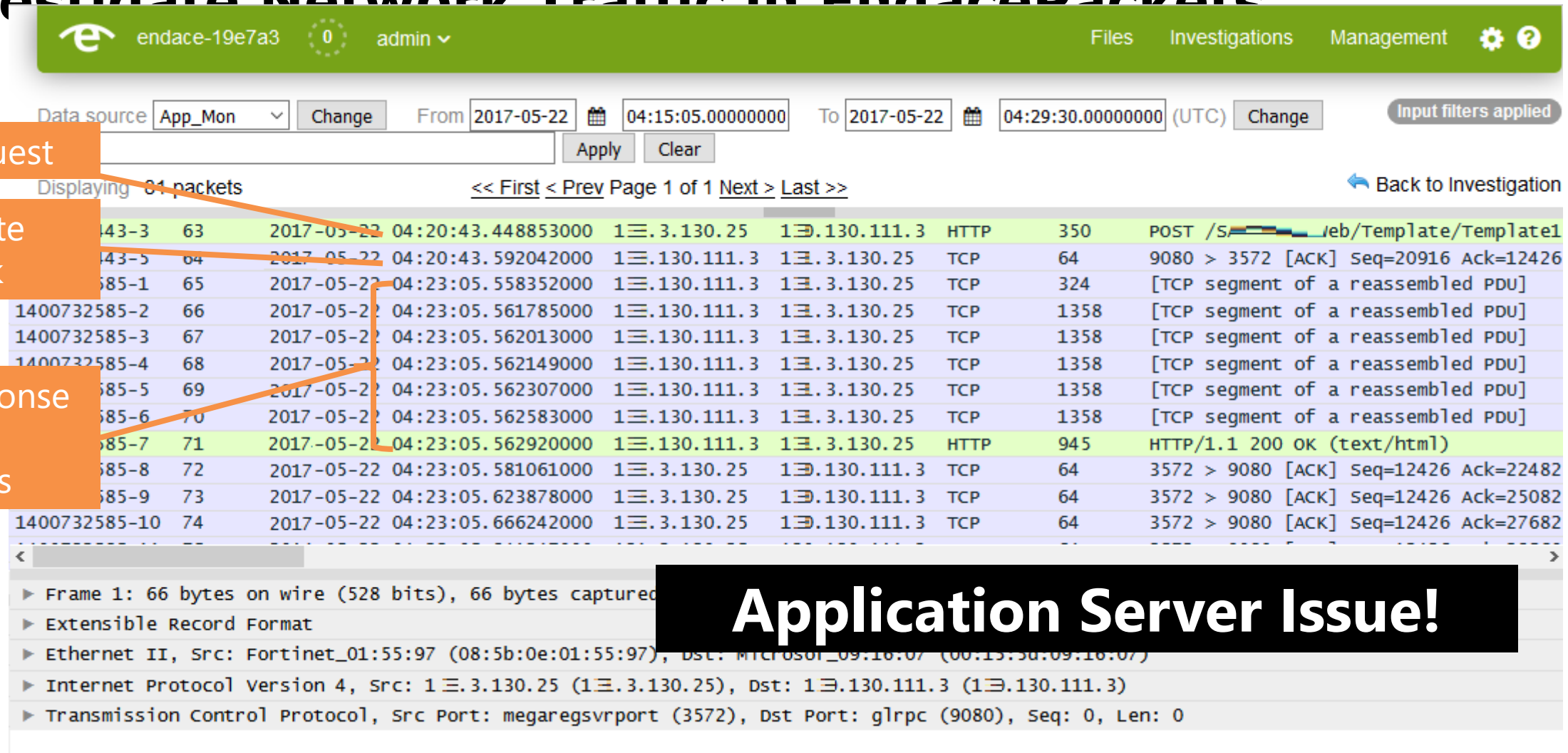
✓ Network Layer Healthy!

Investigate Network Traffic in EndacePackets

Client Request

Immediate TCP Ack

Server Response delayed 2min 48s



Application Server Issue!

Summary

EndaceProbe: Branch Office to Datacenter

- **100% Accurate Recording**
- **High-Fidelity Playback**
- **Open High Performance Platform**
- **Highly Scalable**

Model	Max Monitoring Interfaces	Size (RU)	Max Storage Capacity	Packets with compression and Smart Truncation	Max Sustained Write to Disk Speed	Max Application Dock Instances
vProbe	1 Virtual Interface	-	1TB*		0.5 Gbps*	0
EP114	4 x 10/100/1G	1	3.8TB	>7TB	0.5 Gbps	2
EP124	4 x 1/10G or 1 x 40G	1	3.8TB	>7TB	1Gb/s	2
EP4000	8 x 1/10G or 2 x 40G	1	32TB		3 Gbps	4
EP4100	8 x 1/10G or 2 x 40G	1	15.3TB		15 Gbps	4
EP9000	8 x 1/10G or 2 x 40G	4	192TB	>500TB	20 Gbps	4
EP9200	8 x 1/10G or 2 x 40G	4	432TB	>1PB	40 Gbps	12

* vProbe performance depends on environment setup

Thank you