The Packet Games

Analytics & Troubleshooting On The Wire

Mike Nelson
John Smith

Mike Nelson

Special Olympics

SPECIAL OLYMPICS
2014 USA GAMES
NEW JERSEY

WISCONSIN
VMUG
VMWARE USER GROUP

vmware
vEXPERT

MVP
Microsoft
Most Valuable Professional

ctp
CiTRIX
Technology Professional

Azure
Advisor

ATLANTIS™

John Smith

ExtraHop

ctp CiTRiX Technology Professional

WireData.net

Topics

- Who’s fault is it?
- Putting it all together
- HACCP & PACCP Methodologies
- Critical Control Points
- Exposing the truth

But, we’re not just talking about Citrix, are we?

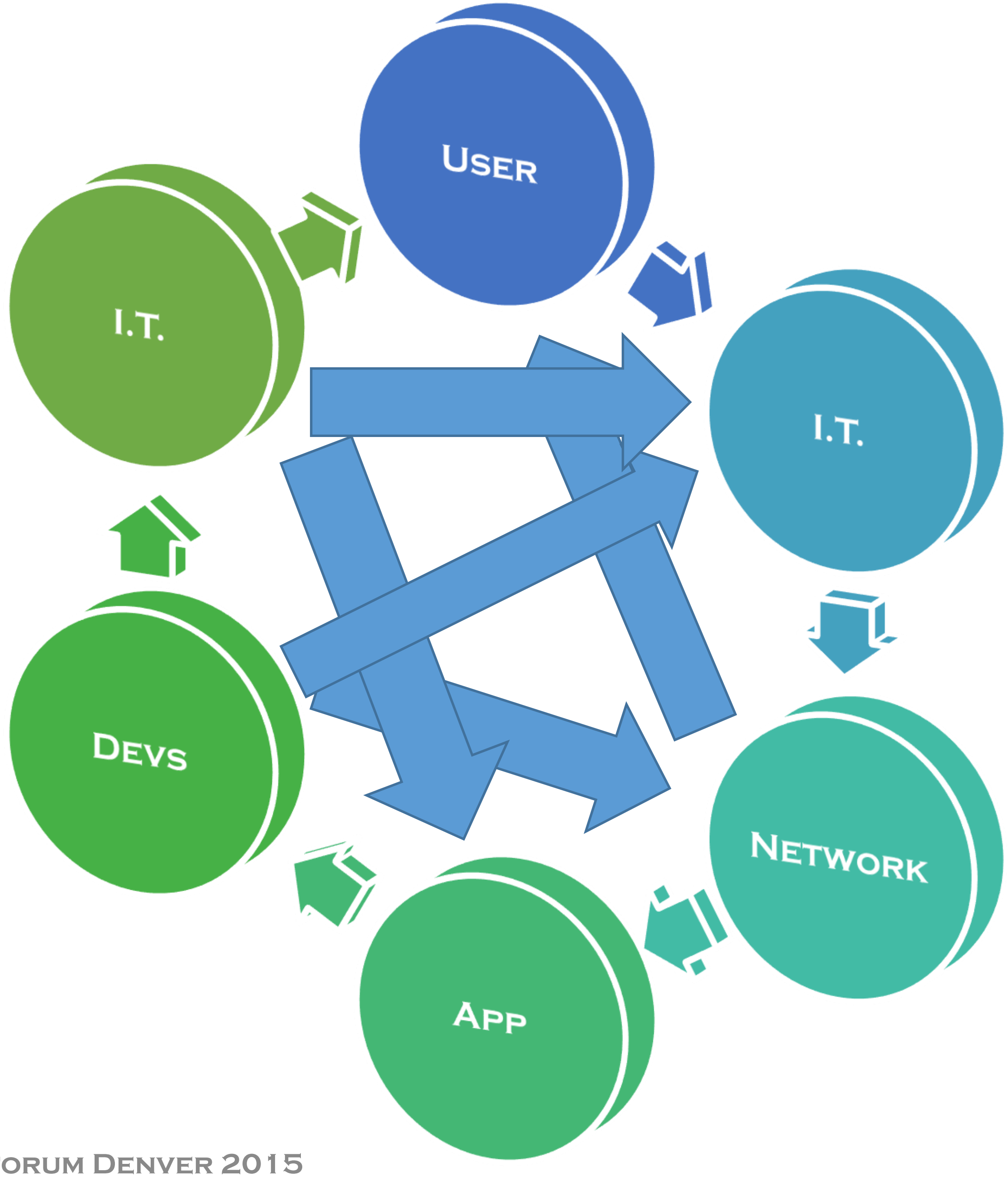
- Apps
- Network
- Client
- Infrastructure
- ID10T

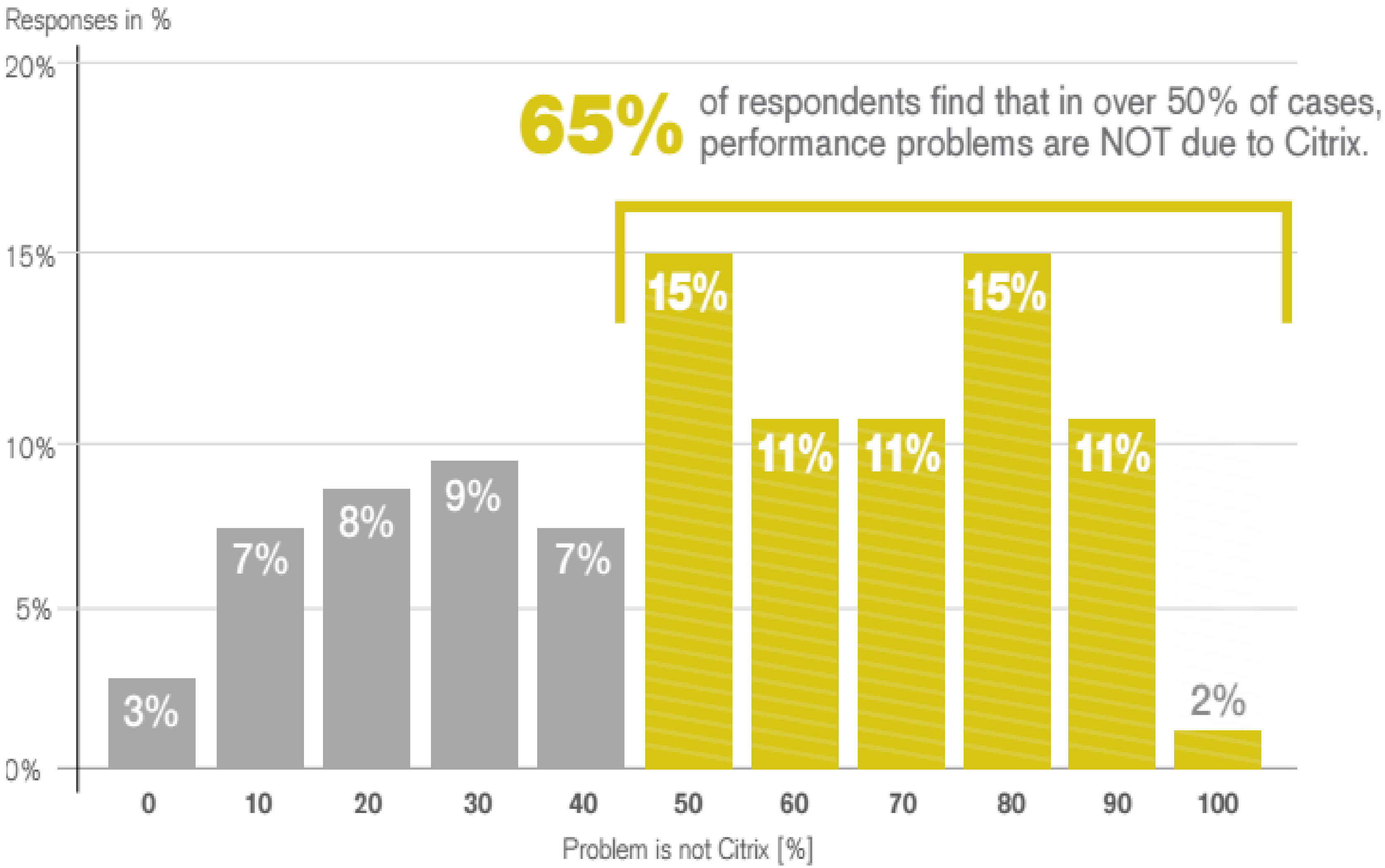
DID SOMEONE SAY "CITRIX"?!

GET OUT OF JAIL, FREE

THIS CARD MAY BE KEPT UNTIL NEEDED OR UNTIL THE CITRIX TEAM PROVES IT ISN'T THEM

The Circle of Blame





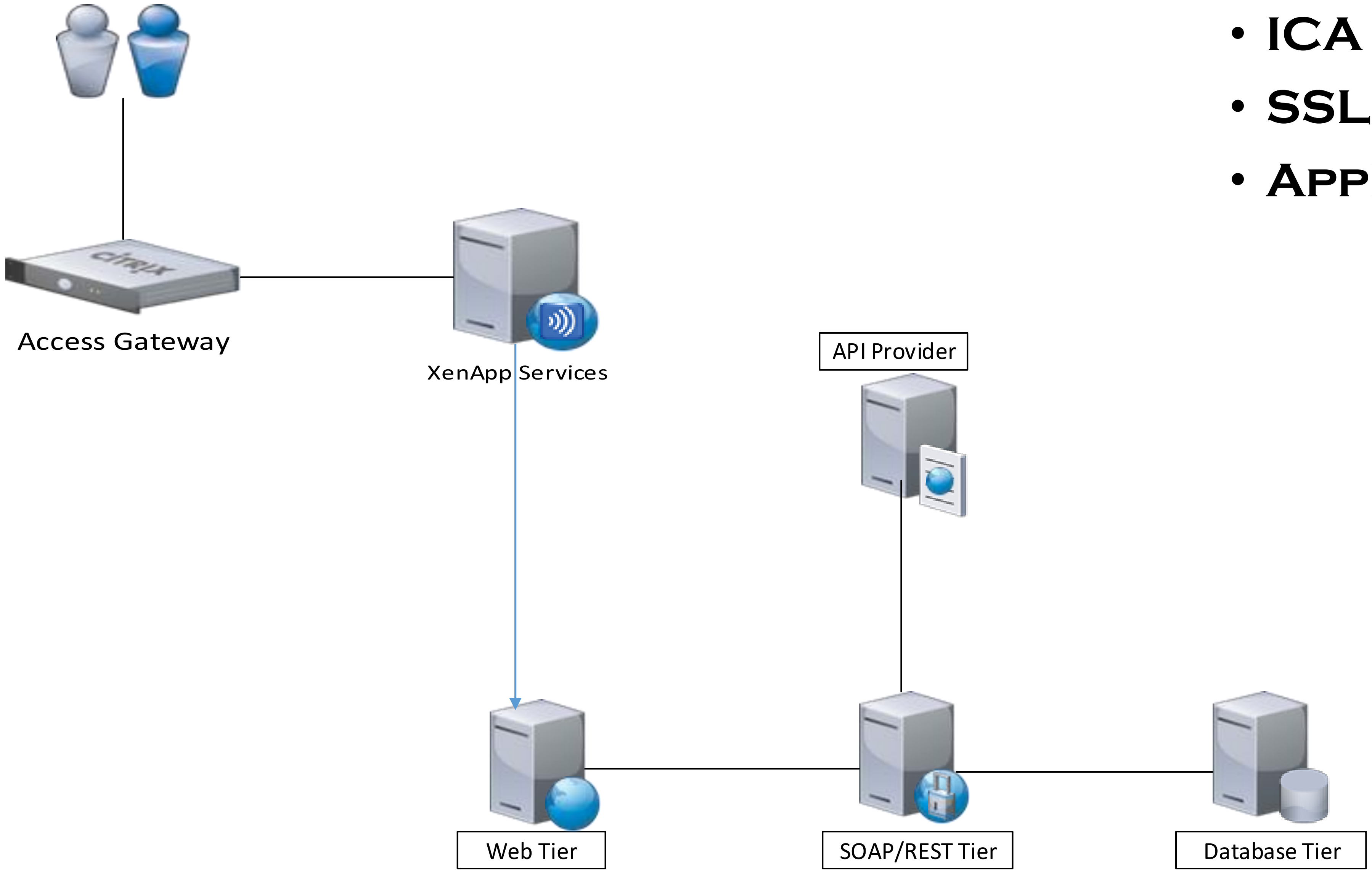
65% state THAT CITRIX IS NOT THE ISSUE AT LEAST 50% OF THE TIME

NEARLY 40% STATE THAT CITRIX IS NOT THE ISSUE AT LEAST 70% OF THE TIME

SOURCE: 2014 CITRIX PERFORMANCE MANAGEMENT REPORT (DOUG BROWN/eGINNOVATIONS)

So if it's not Citrix, what is it?

- ICA Latency
- SSL Latency
- AppFlow Data



Application On-Boarding vs. Publishing

- Demand that the app owners take SOME responsibility for their applications.
- If the application owner cannot provide a PACCP profile, don't publish it.
- Work with App Owners on what baselines and limits should be in place.
- Ensure that changes in the downstream PACCP profile are communicated to you. Insert yourself (barge-in) into the change management/approval process.

HACCP
(Hazard Analysis Critical Control Point)

- Conduct Hazard Analysis
- Identify Critical Control Points
- Establish Limits
- Establish Monitoring
- Establish Corrective Actions
- Establish Procedures to make sure it is working
- Long Term Record Keeping

HACCP SOP Example:

- Cooling:
  - 135 ºF to 70 ºF within 2 hours.
    - Take corrective action immediately if food is not chilled from 135 ºF to 70 ºF within 2 hours. • 70 ºF to 41 ºF or below in remaining time.
  - The total cooling process from 135 ºF to 41 ºF may not exceed 6 hours.
    - Take corrective action immediately if food is not chilled from 135 ºF to 41 ºF within the 6 hour cooling process.
- Cooking:
  - 145 ºF for 15 seconds
    - Seafood, beef, and pork
    - Eggs cooked to order that are placed onto a plate and immediately served
  - 155 ºF for 15 seconds
    - Ground products containing beef, pork, or fish
    - Fish nuggets or sticks
    - Eggs held on a steam table
  - 165 ºF for 15 seconds
    - Poultry
    - Stuffed fish, pork, or beef
    - Pasta stuffed with eggs, fish, pork, or beef (such as lasagna or manicotti)

PACCP (Packet Analysis Critical Control Point)

- Conduct Packet Analysis(Who talks to who and over what ports)
- Identify Critical Control Points
- Establish Limits
- Establish Monitoring
- Establish Corrective Actions
- Establish Procedures to make sure it is working
- Long Term Record Keeping

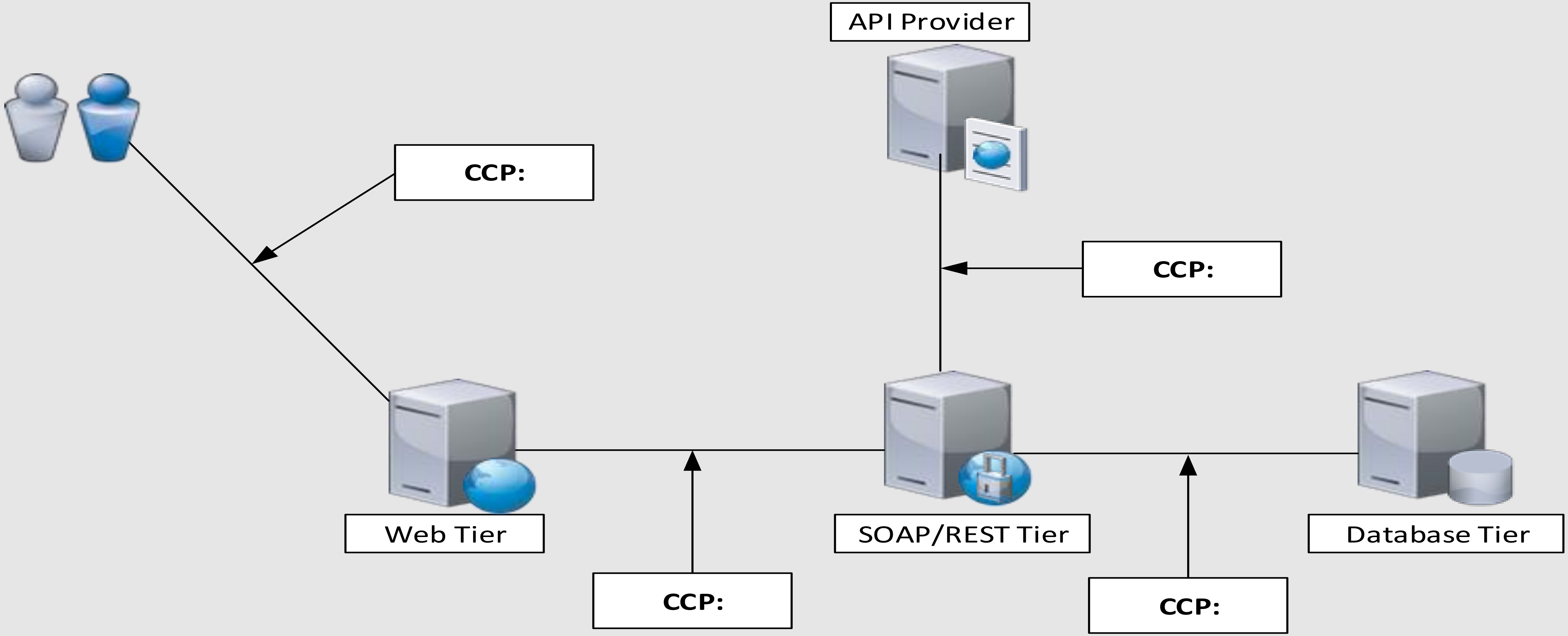
PACCP
Conduct Packet Analysis

- What transactions are taking place
  - Database(SQL, Oracle, DB2, MySQL)
  - HTTP/HTTPs
  - CIFS
  - LDAP/Kerberos/GC
  - ICA
  - Queuing(IBMMQ, ActiveMQ, MSMQ)
  - Storage (NFS, iSCSI)
- Which systems are making which transactions
  - Client to server
  - Tier to tier

PACCP
Identify Critical Control Points

- Transactions and conversations that could negatively impact user experience.
- Where is critical information being passed making it a target for a breach. What type of information is being passed
- Which specific ports and protocols should be traversing each critical control point.
- Who owns (which team) the systems involved in each critical control point.

PACCP
Identify Critical Control Points



PACCP
Establish Limits

- What is the acceptable transaction time for each Critical Control Point.
- What communication is acceptable at each Critical Control Point
  - Stored Procedures vs. Ad Hoc Queries
  - Accessing the profile$ share vs. accessing the c$ share.
- Baseline the number of transactions and report on anomaly's
- Baseline transaction byte size and report on anomaly's
  - SQL Server avg. byte size going from 15K to 400K

PACCP
Establish Monitoring

- Monitor each CCP and ensure that it is within the limits set in the previous step.
  - SQL Transactions are acceptable
    - Processing times are within limits
    - Transaction types are as expected
  - ICA Latency is acceptable
  - HTTP/HTTPs transactions are acceptable
    - Error count is within limits
    - Processing times are within thresholds
  - Storage performance is acceptable

PACCP
Take Corrective Actions

- Understand what can go wrong at each CCP and common fixes
  - Locking down problem Citrix servers
  - Re-deploy software
  - Check SQL Server indexes
  - Rebooting systems
  - Fixing DNS failures
  - Optimize profile servers
- Understand which team is responsible for taking corrective actions

PACCP
Establish procedures to make sure it's working

- Develop and report on KPIs
  - Alerting
  - Dashboarding
    - Show KPI performance at each CCP
    - If possible, show entire cross-tier (holistic) transaction times
- Make it someone's job
  - "Pit Boss"
    - Responsible for making sure KPI's for each CCP are within the thresolds.
    - Knows/understands what the baseline is, what the limits are.

PACCP
Long term record keeping

- Position yourself to be able to answer performance questions
  - What was the traffic pattern, transaction time and CCP performance during Christmas last year?
  - What can we expect to see this Christmas season
  - What communication changes have occurred in the last 18 months (New ports/protocols, transaction types, byte sizes)
- If possible, leverage API's, Syslog and Databases (Big Data or Relational) for long term Data Warehousing.

PACCP SOP Example:

- Database Transactions: **Contact: DBA Team**
  - The average database transaction time will not exceed 100ms.
    - Take corrective action immediately if database transactions exceed 100ms for over 30 minutes during normal working hours.
  - Key stored procedures will not take more than 30ms
      - sp_checkout
      - sp_cc_verification
      - sp_patient_lookup
- Web Transactions:
  - Front End Web Transactions: **Contact: E-Commerce Team**
    - Web transactions will complete in 100ms or less
    - There will be fewer than 1% errors (5xx)
  - Mid-Tier Transactions: **Contact: Middle-Tier Team**
    - Mid Tier transactions will not average more than 20ms for more than 30 minutes
  - 3rd Party API calls: **Contact: API's Inc.**
    - External API transactions will not average more than 500ms for more than 30 minutes

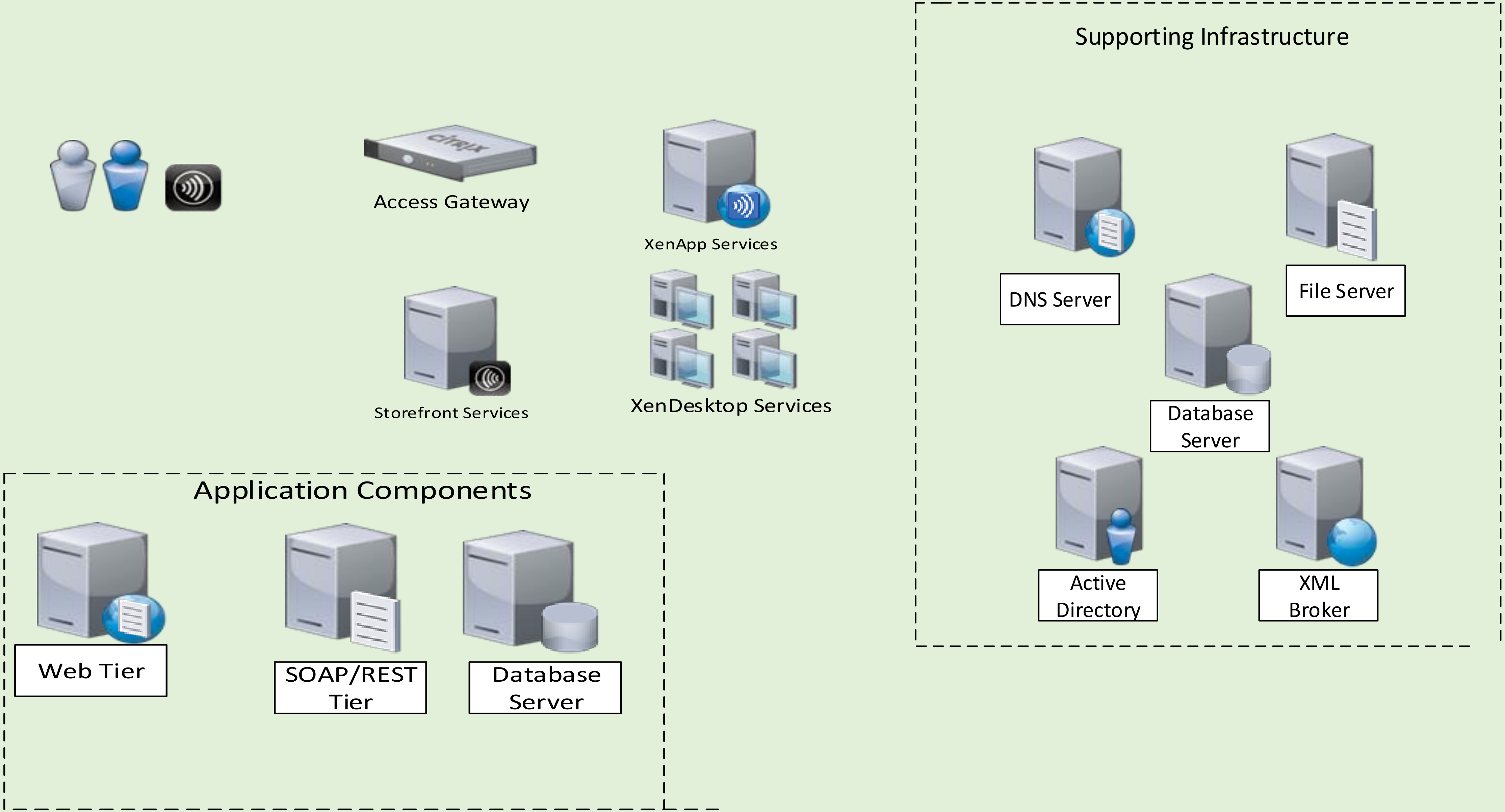
Core Critical Control Points

- Layer 4 Core
    - Retransmission Timeouts (RTOs)
    - Throttles
    - Dropped Segments
    - Zero Windows
- AD/DNS Sub-Core
    - DNS Performance
    - DNS Errors/Timeouts
    - Windows Environments
        - Global Catalog Performance
        - LDAP Performance
        - Kerberos Performance

Citrix Critical Control Points

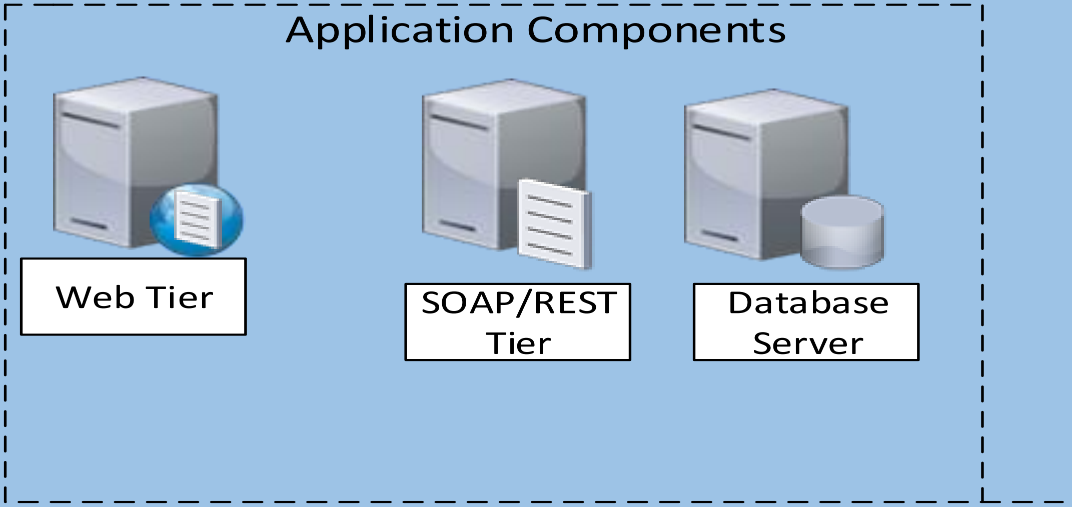
- Citrix Clients
  - Web Interface
  - ICA Client Traffic
- VDA's
  - XML Brokering
  - XML Client (Registration, DDC Communications)
  - ICA Server Traffic
  - Storage
- DDC's
  - Database Client
  - XML Broker
  - Web Server
- Storefront
  - XML Client
  - HTTP Server
  - SSL Client (Authentication Callback)

Citrix Critical Control Points



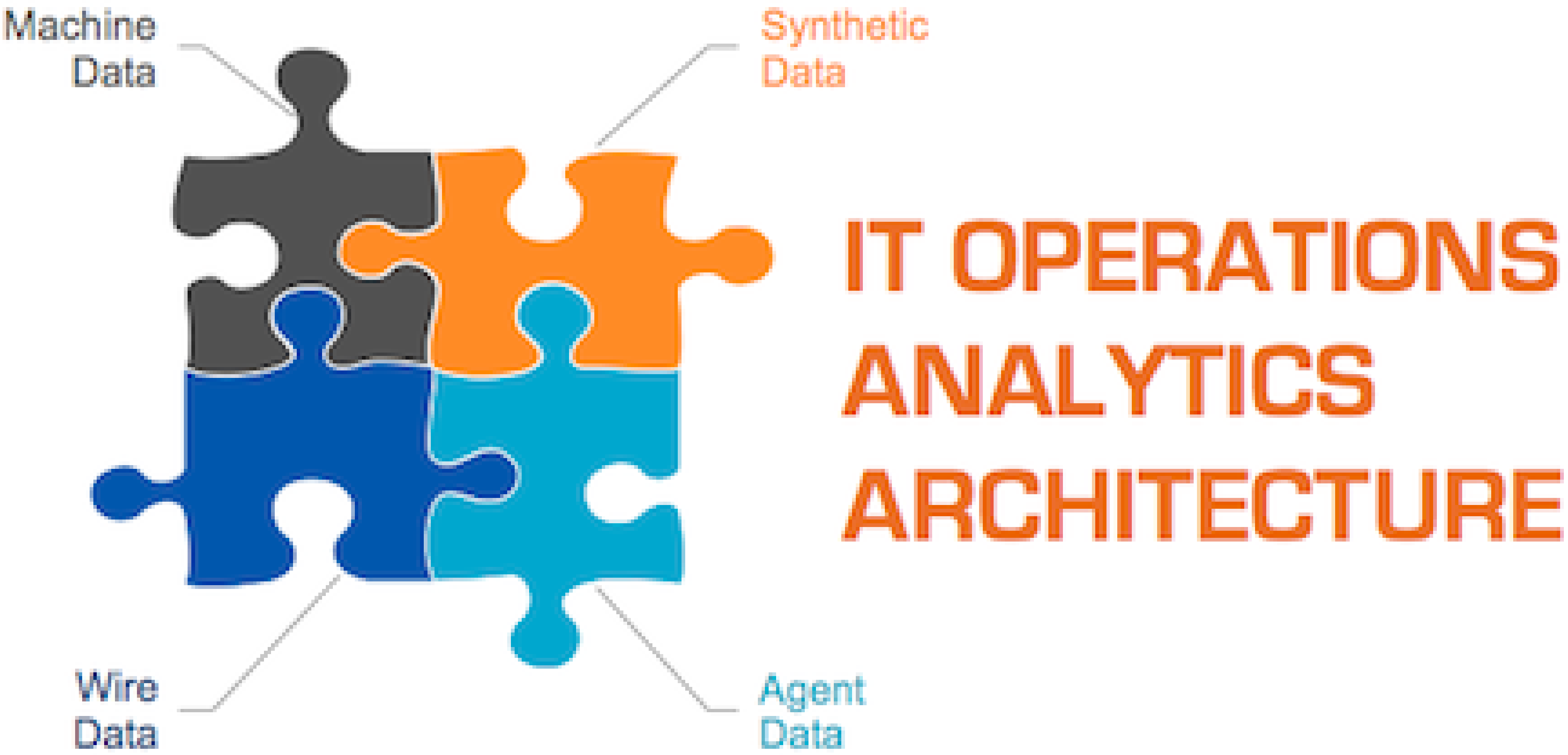
Sample Application (3 Tiered)

- Citrix Receiver (Client)
  - ICA Latency
- Front End (Browser or Installed Application)
  - HTTP Process Time
  - L4 RPC Turn Time
- SOAP/REST Server(s)
  - HTTP Process Time
  - Database Processing Time
- Database Server
  - Processing Time
  - Common Stored Procedures or Queries



Source	Destination	Protocol	Owner	Port	Latency Thresold	Process Time Threshold
Client/Receiver	VDA	ICA	Citrix Team	1494/2598	200ms	NA
VDA	Web Server	HTTP	Web Team	80	50ms	100ms
Web Server	SOAP Tier	HTTP	Mid Tier Team	8080	50ms	100ms
SOAP Tier	SQL Server	TDS	Database Team	1433	50ms	100ms

The Four Data Sources of ITOA



Machine Data

splunk>

elasticsearch.

vmware

vCenter Log Insight

Benefits of Machine Data:

- Provides mash ups from different sources
- Large Development Community
- Logging via Syslog is a very mature technology
- Bringing sanity to unformatted, non-normalized data

Limitations of Machine Data:

- Only as good as the log sent to it
- Most mature product can be expensive
- Large amounts of data can cause horizontal scaling costs
- Is dependent on the system to send it

How it helps us:

- The ability to merge data from several different sources
- Direct search capabilities
- When centralized, everyone is accountable

Demo

Agents

riverbed®

GOLIATH TECHNOLOGIES®

Lakeside®

SysTrack.

eG

Enabling Service Excellence

AppDynamics

splunk®>

control up

Benefits of Agents:

- Kernel Level Visibility
- Machine Resource Reporting
- Individual Process Metrics

Limitations of Agents:

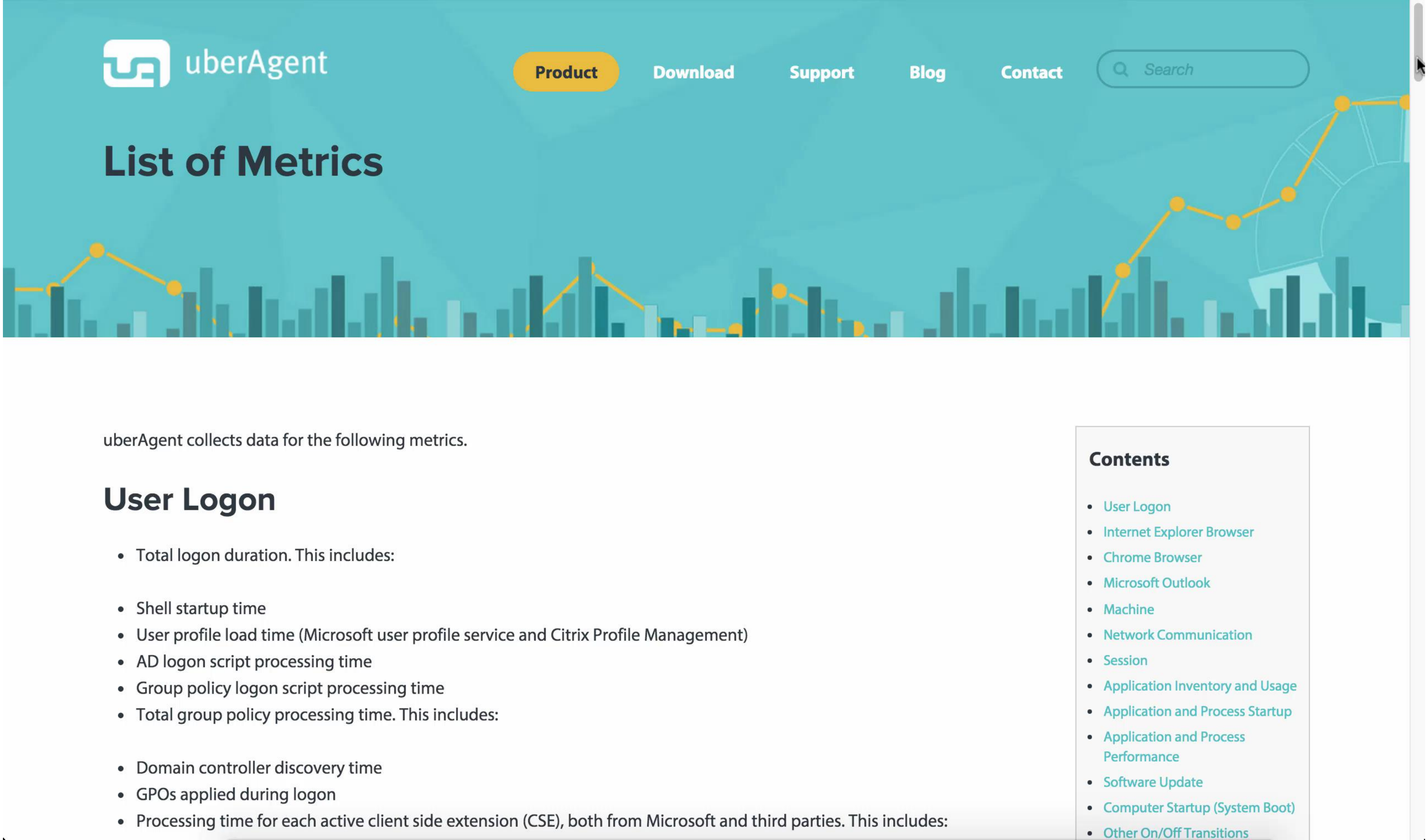
- Smaller Aperture (System Only, one hop visibility)
- They have to be installed/updated/patched
- Can be impacted by system problems

How they help us:

- They tell you if YOU are definitely the problem
- Can tell you Resource Details
- They can report on immediate, next-hop transactions.

Uber Agent

- Very Lightweight
- Fantastic Dashboards for Splunk
- Great for downstream visibility
- They are transactional focused not just system resource focused.



List of Metrics

uberAgent collects data for the following metrics.

User Logon

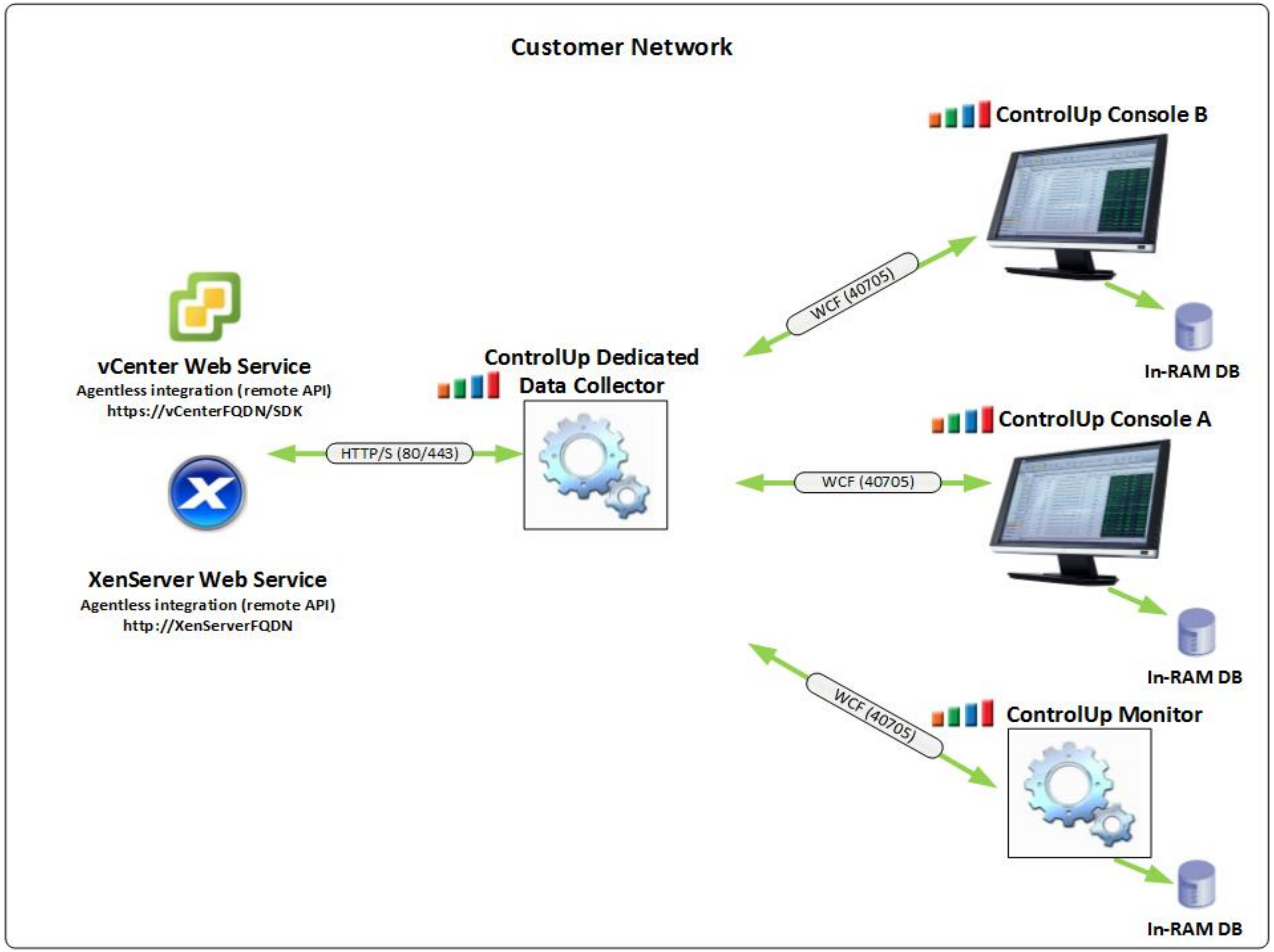
- Total logon duration. This includes:

- Shell startup time
- User profile load time (Microsoft user profile service and Citrix Profile Management)
- AD logon script processing time
- Group policy logon script processing time
- Total group policy processing time. This includes:

- Domain controller discovery time
- GPOs applied during logon
- Processing time for each active client side extension (CSE), both from Microsoft and third parties. This includes:

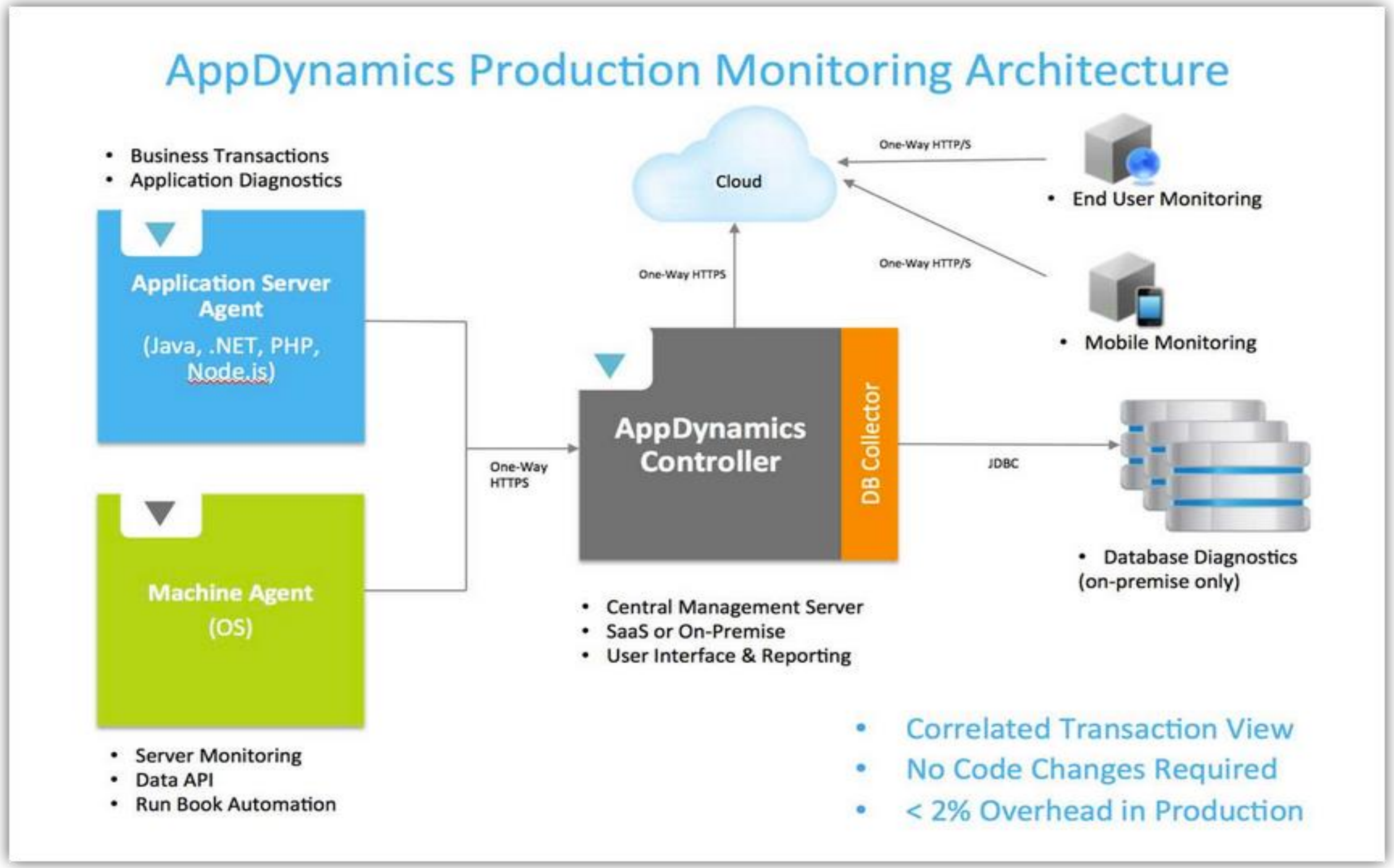
Contents

control up



- Easy to install – up and running in minutes
- Flexible and scalable
- Impressive analytics and reporting

App Dynamics



AppDynamics Production Monitoring Architecture

- Business Transactions
- Application Diagnostics

- End User Monitoring
- Mobile Monitoring
- Database Diagnostics (on-premise only)

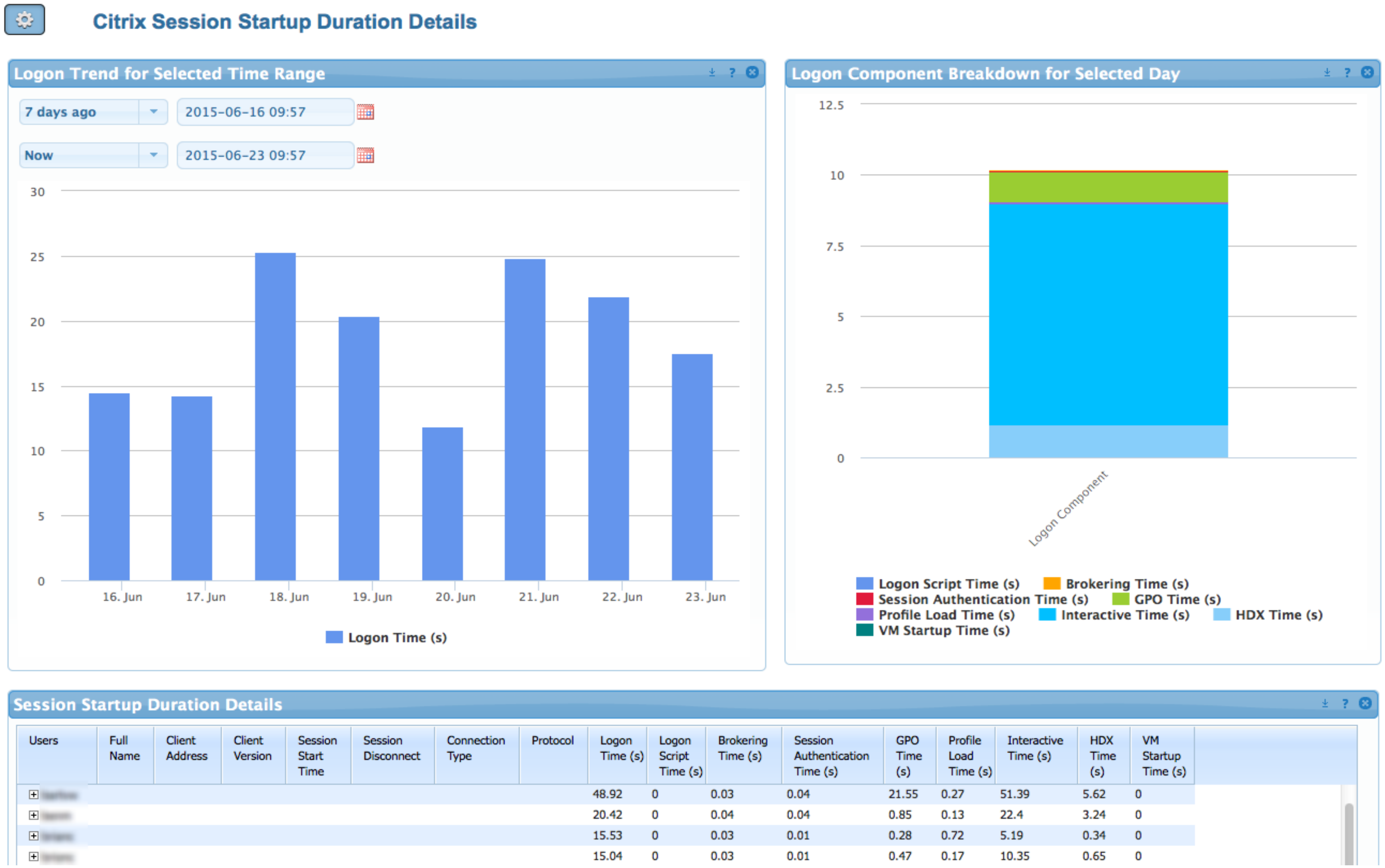
- Central Management Server
- SaaS or On-Premise
- User Interface & Reporting

- Server Monitoring
- Data API
- Run Book Automation

- Correlated Transaction View
- No Code Changes Required
- < 2% Overhead in Production

- Threading Application Flows.
- Flexible "cloud ready" infrastructure.
- Great for downstream visibility

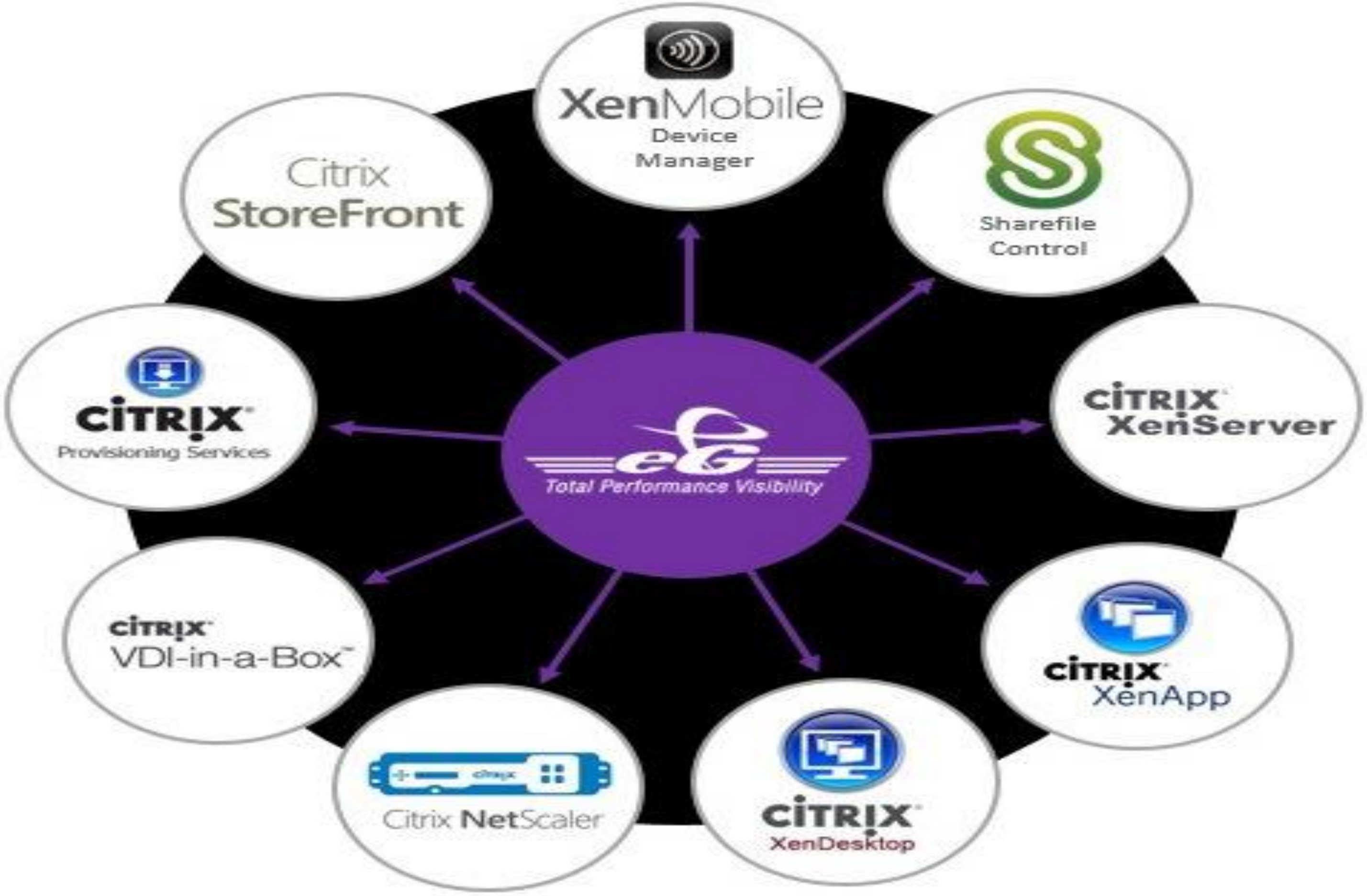
Lakeside Software



Users	Full Name	Client Address	Client Version	Session Start Time	Session Disconnect	Connection Type	Protocol	Logon Time (s)	Logon Script Time (s)	Brokering Time (s)	Session Authentication Time (s)	GPO Time (s)	Profile Load Time (s)	Interactive Time (s)	HDX Time (s)	VM Startup Time (s)
⊞ [redacted]								48.92	0	0.03	0.04	21.55	0.27	51.39	5.62	0
⊞ [redacted]								20.42	0	0.04	0.04	0.85	0.13	22.4	3.24	0
⊞ [redacted]								15.53	0	0.03	0.01	0.28	0.72	5.19	0.34	0
⊞ [redacted]								15.04	0	0.03	0.01	0.47	0.17	10.35	0.65	0

- Considerable Citrix DNA.
- They are creating customized "kits" which gives them an agile architecture
- Great for downstream visibility
- They are transactional focused not just system resource focused.

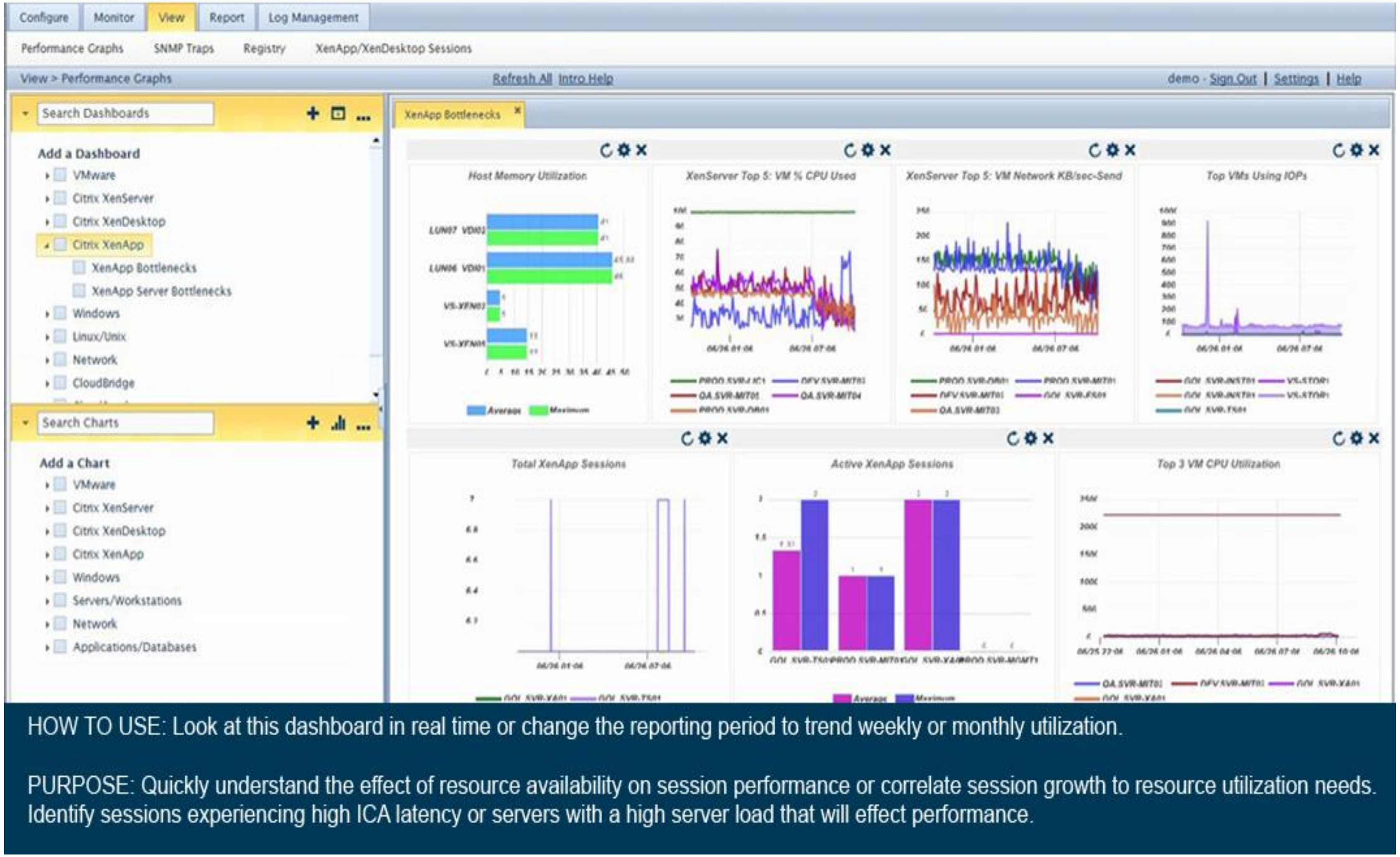
eG Innovations



- Custom metrics for majority of Citrix portfolio
- Rich Dashboards
- Extensive Citrix experience

BE PROACTIVE.

Goliath Technologies



HOW TO USE: Look at this dashboard in real time or change the reporting period to trend weekly or monthly utilization.

PURPOSE: Quickly understand the effect of resource availability on session performance or correlate session growth to resource utilization needs. Identify sessions experiencing high ICA latency or servers with a high server load that will effect performance.

- Large portfolio with support for AppFlow and Agents
- Expansive variety of solutions for Citrix
- Custom solutions for targeted technologies beyond Citrix
- Rich Dashboards with relevant information

Exposing the Truth

ExtraHop

WIRESHARK

Benefits of Agentless Wire Data:

- Ease of deployment
- Unparalleled use cases
  - Performance
  - Security
  - An
- Cross
- No im
  - Can make changes without impacting local systems.
- No Liability to Systems
  - High CPU, Disk Memory issues will not impact reporting ability

Wire Data does not lie

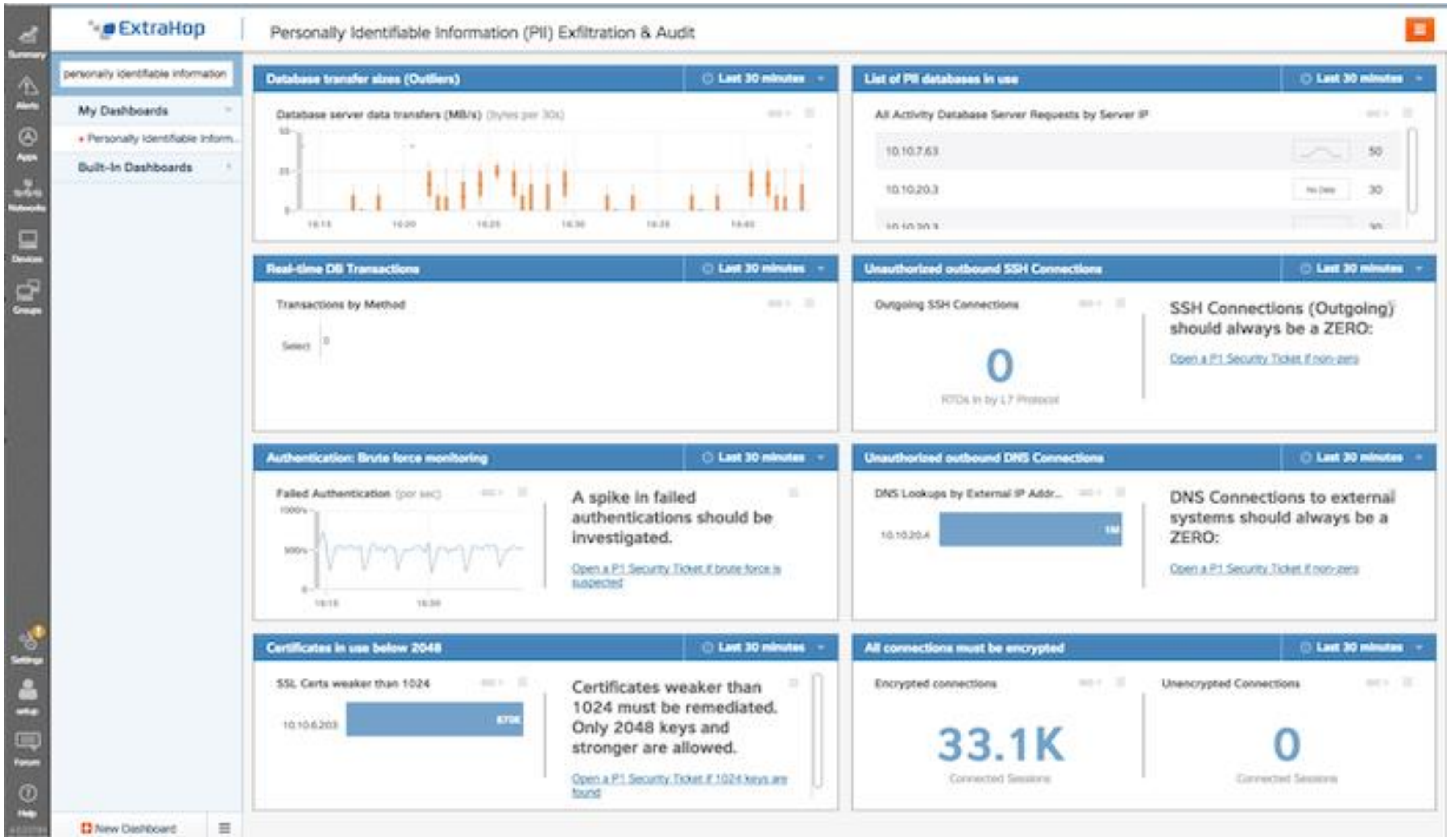
Limitations of Wire Data:

- Depend on a SPAN (In most cases)
- No visibility into system resources
- Cannot see individual processes

How it helps us:

- Holistic visibility
  - You can see other tiers weather they like it or not
- Only pre-requisite is an IP Address
- Almost totally transaction focused

ExtraHop



Personally Identifiable Information (PII) Exfiltration & Audit

Database transfer sizes (Outliers)

Database server data transfers (MB/s) (bytes per 30s)

List of PII databases in use

All Activity Database Server Requests by Server IP

Real-time DB Transactions

Transactions by Method

Unauthorized outbound SSH Connections

Outgoing SSH Connections

0

RTOs In by L7 Protocol

SSH Connections (Outgoing) should always be a ZERO:

Open a P1 Security Ticket if non-zero

Authentication: Brute force monitoring

Failed Authentication (per sec)

A spike in failed authentications should be investigated.

Open a P1 Security Ticket if brute force is suspected

Unauthorized outbound DNS Connections

DNS Lookups by External IP Addr...

DNS Connections to external systems should always be a ZERO:

Open a P1 Security Ticket if non-zero

Certificates in use below 2048

SSL Certs weaker than 1024

Certificates weaker than 1024 must be remediated. Only 2048 keys and stronger are allowed.

Open a P1 Security Ticket if 1024 keys are found

All connections must be encrypted

Encrypted connections

33.1K

Connected Sessions

Unencrypted Connections

0

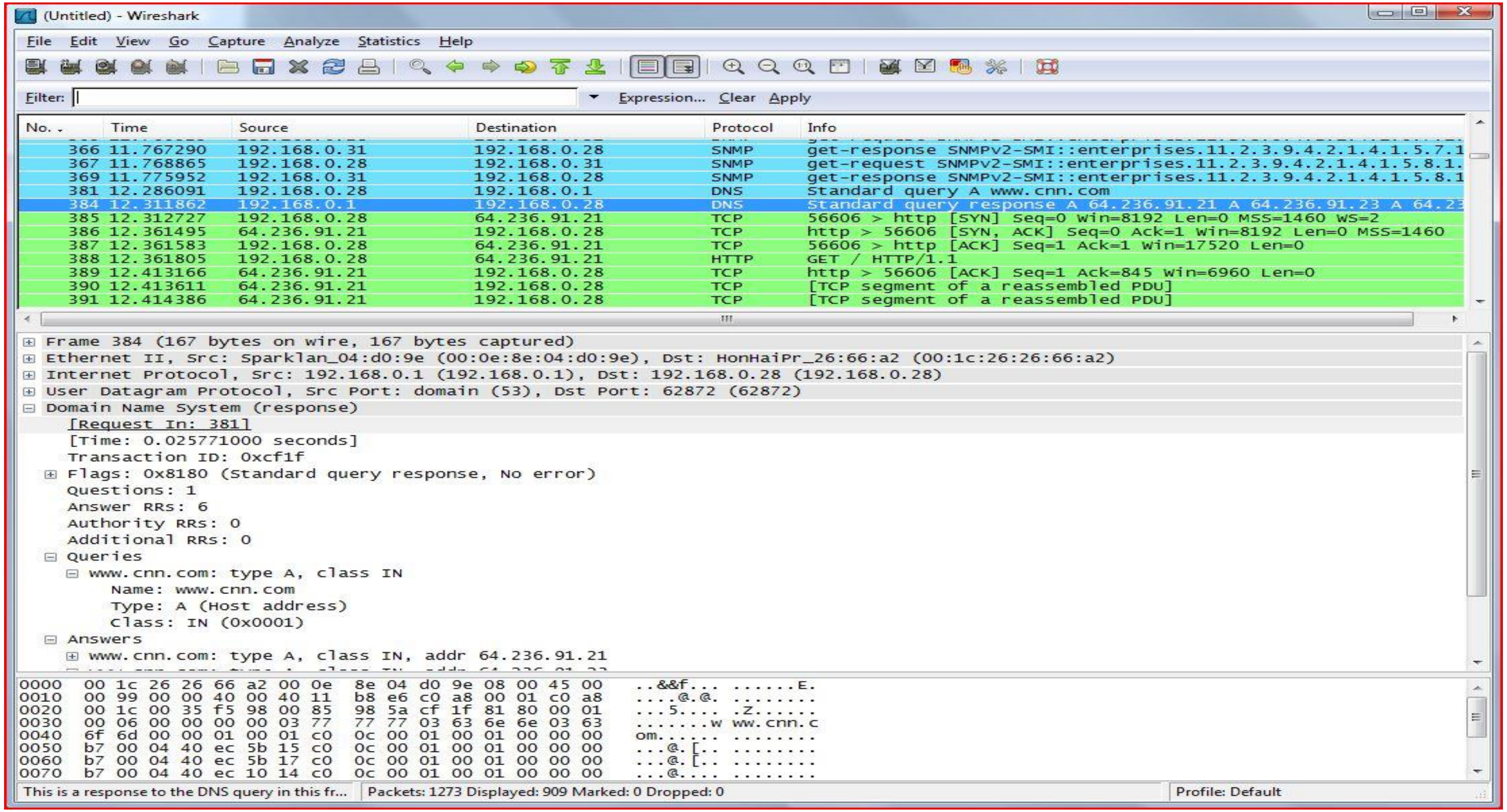
Connected Sessions

- Completely Agent-Less
- No Polling
- 40 GB/s throughput
- Breadth of use cases
- Licensed ICA SPEC
- Cloud Ready
- Agile architecture (Bundles, API, Triggers)

Things I've observed on the wire

- 90% or better DNS Failure
- Malware phoning home to China
- XML Broker transactions that take over 90 seconds
- 7 minutes of Latency

WIRESHARK



```
No. -  Time        Source          Destination     Protocol  Info
  366 11.767290   192.168.0.31    192.168.0.28    SNMP      get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.7.1
  367 11.768865   192.168.0.28    192.168.0.31    SNMP      get-request SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1.
  369 11.775952   192.168.0.31    192.168.0.28    SNMP      get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1
  381 12.286091   192.168.0.28    192.168.0.1     DNS       Standard query A www.cnn.com
  384 12.311862   192.168.0.1     192.168.0.28    DNS       Standard query response A 64.236.91.21 A 64.236.91.23 A 64.23
  385 12.312727   192.168.0.28    64.236.91.21    TCP       56606 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
  386 12.361495   64.236.91.21    192.168.0.28    TCP       http > 56606 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
  387 12.361583   192.168.0.28    64.236.91.21    TCP       56606 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
  388 12.361805   192.168.0.28    64.236.91.21    HTTP      GET / HTTP/1.1
  389 12.413166   64.236.91.21    192.168.0.28    TCP       http > 56606 [ACK] Seq=1 Ack=845 Win=6960 Len=0
  390 12.413611   64.236.91.21    192.168.0.28    TCP       [TCP segment of a reassembled PDU]
  391 12.414386   64.236.91.21    192.168.0.28    TCP       [TCP segment of a reassembled PDU]
```

```
⊞ Frame 384 (167 bytes on wire, 167 bytes captured)
⊞ Ethernet II, Src: Sparklan_04:d0:9e (00:0e:8e:04:d0:9e), Dst: HonHaiPr_26:66:a2 (00:1c:26:26:66:a2)
⊞ Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.28 (192.168.0.28)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 62872 (62872)
⊟ Domain Name System (response)
    [Request In: 381]
    [Time: 0.025771000 seconds]
    Transaction ID: 0xcf1f
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.cnn.com: type A, class IN
        Name: www.cnn.com
        Type: A (Host address)
        Class: IN (0x0001)
  ⊟ Answers
    ⊞ www.cnn.com: type A, class IN, addr 64.236.91.21
```

```
0000  00 1c 26 26 66 a2 00 0e  8e 04 d0 9e 08 00 45 00   ..&&f... ......E.
0010  00 99 00 00 40 00 40 11  b8 e6 c0 a8 00 01 c0 a8   ....@.@. ........
0020  00 1c 00 35 f5 98 00 85  98 5a cf 1f 81 80 00 01   ...5.... .Z......
0030  00 06 00 00 00 00 03 77  77 77 03 63 6e 6e 03 63   .......w ww.cnn.c
0040  6f 6d 00 00 01 00 01 c0  0c 00 01 00 01 00 00 00   om...... ........
0050  b7 00 04 40 ec 5b 15 c0  0c 00 01 00 01 00 00 00   ...@.[.. ........
0060  b7 00 04 40 ec 5b 17 c0  0c 00 01 00 01 00 00 00   ...@.[.. ........
0070  b7 00 04 40 ec 10 14 c0  0c 00 01 00 01 00 00 00   ...@.... ........
```

This is a response to the DNS query in this fr... | Packets: 1273 Displayed: 909 Marked: 0 Dropped: 0 | Profile: Default

- FREE
- INSANELY WELL DOCUMENTED
- SEMI-CUSTOMIZABLE
- STRONG FILTERING CAPABILITIES
- FANTASTIC DEVELOPMENT COMMUNITY

WireShark Demo

Handy Wireshark Filters:

- DNS Failures:
  - dns && (dns.flags.response == 0) && ! dns.response_in
- Turn Time (TCP) (Latency or RTT)
  - tcp.time_delta
- Web Server processing time
  - http.time
- Potential Throttling issues
  - tcp.analysis.bytes_in_flight
  - tcp.window_size
- I/O Related Issues
  - tcp.analysis.zero_window

WireShark Demo

Finding High Client Latency:
Client: 50.23.218.78
Server: 10.10.1.110
Metric: tcp.time_delta

- ICA Latency
  - tcp.srcport==1494 && tcp.time_delta > .3
    In English: Give me all records with a Round Trip Time of over 300ms for the ICA Port 1494.
  - tcp.srcport==1494 && ip.host==10.10.1.110
    In English: Filter for all ICA Traffic for the server in question.
  - tcp.srcport==1494 && ip.host contains 50.23.218
    In English: Filter for all ICA Traffic for the CIDR block to see if you have an issue with a specific subnet.

WireShark Demo

From the VDA:
Client: 10.10.1.110
Server: 10.10.1.110
Metric: tcp.time_delta, http.time

- **ICA Latency**
  - tcp.srcport==1494 && tcp.time_delta > .3
    In English: Give me all records with a Round Trip Time of over 300ms for the ICA Port 1494.
  - tcp.srcport==1494 && ip.host==10.10.1.110
    In English: Filter for all ICA Traffic for the server in question.
  - tcp.srcport==1494 && ip.host contains 50.23.218
    In English: Filter for all ICA Traffic for the CIDR block to see if you have an issue with a specific subnet.

Demo

Thank You

Please – don't forget
To fill out the survey!