BALABIT
A ONE IDENTITY BUSINESS

ADVANCED SOC OPERATION

Reduce cost, improve reliability and detect suspicious behavior

Péter SOPRONI | Cyber Security Consultant| peter.soproni@balabit.com

2018

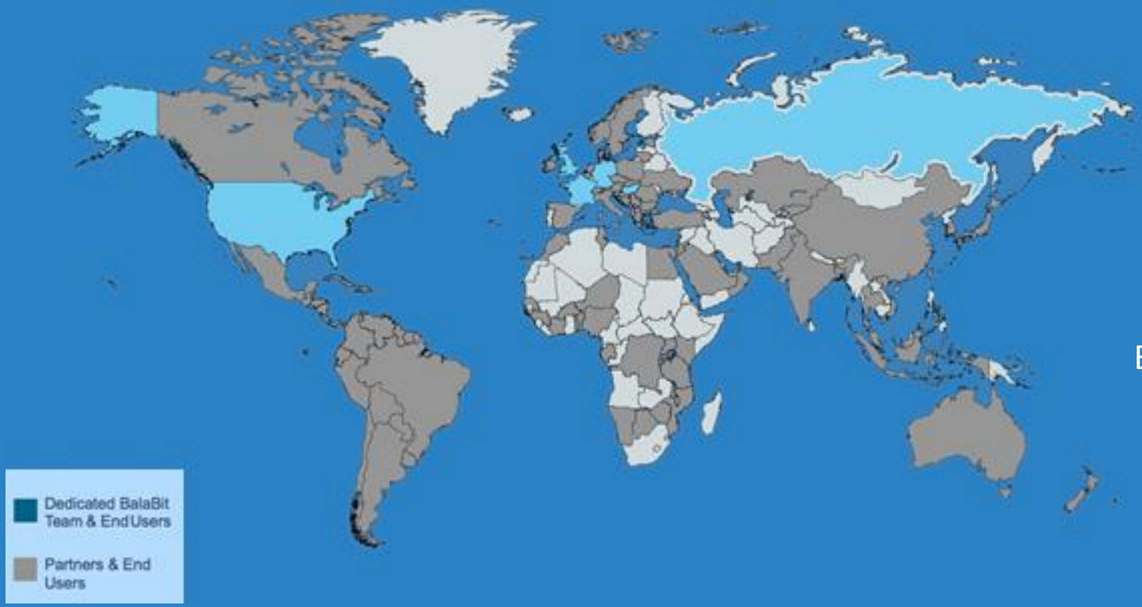
AGENDA

01 Data Collection Challanges and Solutions

02 Privileged Access Challange and Demonstration

03 How Balabit can help
to increase security and reliability?

BALABIT AT A GLANCE



100+ PARTNERS
In 50+ countries

REFERENCES
25 Fortune 100 companies

1600+ CLIENTS

More than 1 MILLION INSTALLATIONS

OFFICES
Budapest, NY, London, Paris, Munich, Moscow

TRACK RECORD
17 years in IT security

BALABIT
A ONE IDENTITY BUSINESS

DTASIA
Security with Confidence

REFERENCE CUSTOMERS

TELCO

- telenor
- orange
- MTS
- Magyar Telekom
- MedNautilus TELECOM ITALIA SPARKLE GROUP
- etisalat
- Bouygues Telecom

IT

- facebook
- encode Cyber Threat Management
- Tecnocom
- fon share WiFi at home... ...enjoy WiFi everywhere!
- lrz
- DATA BASE FACTORY
- Hush
- FIDUCIA Ihr IT-Partner
- NICE
- Solvinity This is IT

FINANCE

- alBaraka
- Handelsbanken
- Alfa-Bank
- الوطني NBK
- MAGYAR NEMZETI BANK
- EMP EMERGING MARKETS PAYMENTS
- merkantilbank az otp csoport tagja
- CENTRAL BANK OF THE REPUBLIC OF AZERBAIJAN
- Credigen Bank Crédit Agricole Consumer Finance csoport tagja
- BAI TUSHUM BANK
- Tinkoff Bank
- بنك دبي الإسلامي Dubai Islamic Bank

OTHER INDUSTRIES

- e.on
- betfair
- CEZ GROUP
- AIRFRANCE
- ANKARA UNIVERSITY
- coop
- BYU BRIGHAM YOUNG UNIVERSITY
- EADS
- University of Victoria
- DOCAPOST
- MNT
- Apria Healthcare
- University of Exeter
- LEEKIE ENTERPRISES INCORPORATED

Péter SOPRONI | Cyber Security Consultant| peter.soproni@balabit.com

DATA COLLECTION CHALLANGES AND SOLUTIONS

BUSINESS DRIVER

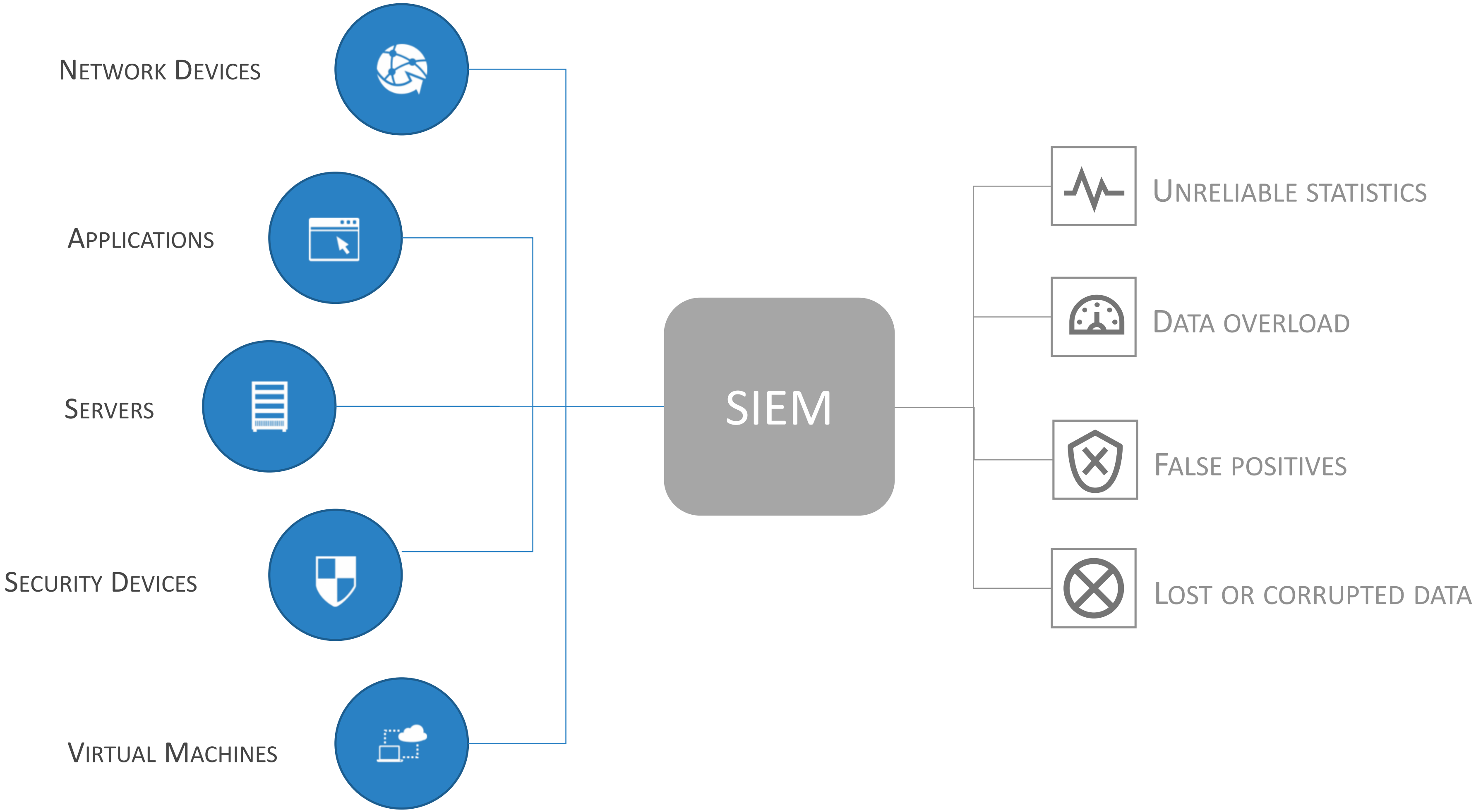
COMPLIANCE

FORENSICS

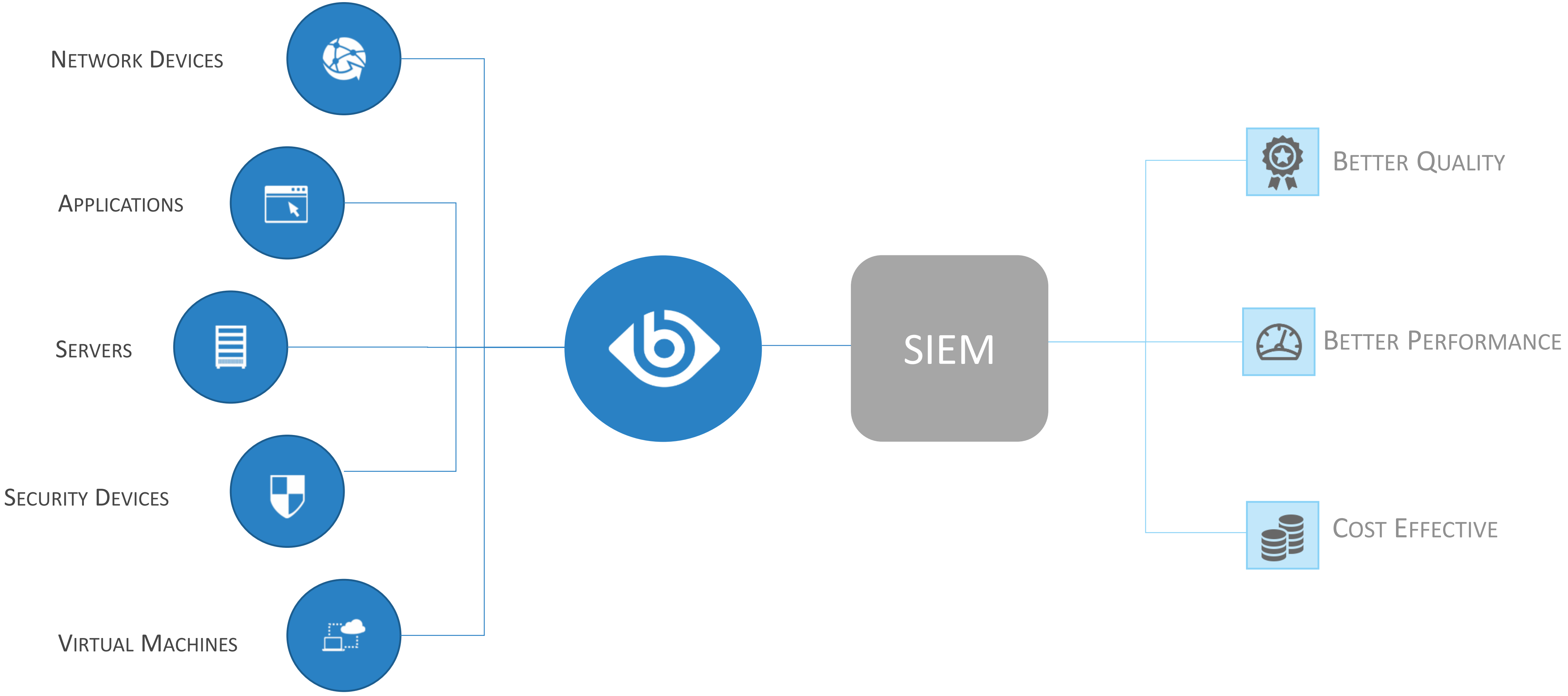
SIEM OPTIMIZING

ENTERPRISE
LOG MANAGEMENT

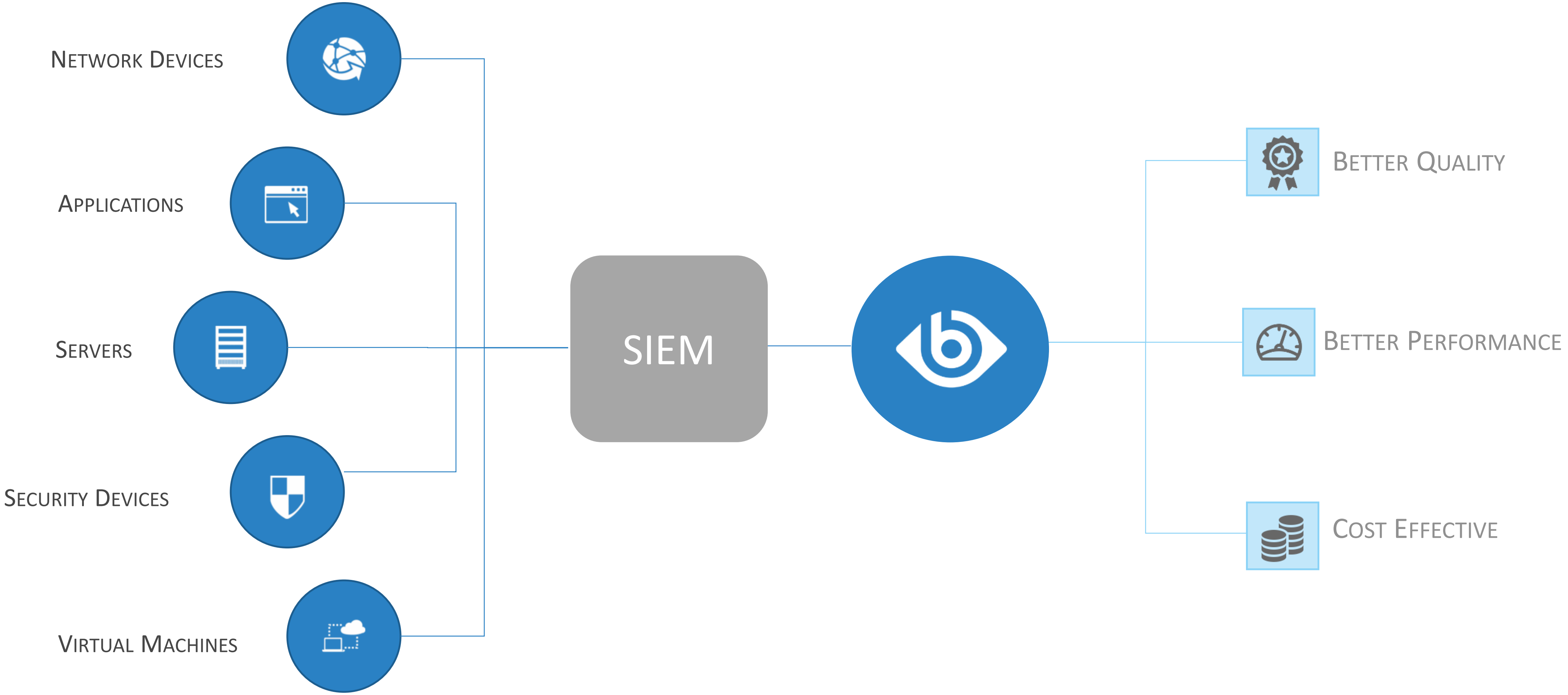
DATA COLLECTION CHALLANGES



SIEM OPTIMIZING



SIEM OPTIMIZING



LOG MANAGEMENT USE CASES

OPTIMIZING SIEM

Reduced noise and improve data quality

FEEDING BIG DATA

Hadoop, Elasticsearch, MongoDB, Kafka

SECURE LOG DATA ARCHIVE

Store up to 10TB of raw logs

RAPID SEARCH AND TROUBLESHOOTING

Search billions of logs in seconds

UNIVERSAL LOG COLLECTION AND ROUTING

Flexible routing

MEETING COMPLIANCE REQUIREMENTS

Tamper-proof storage and custom reporting

LONG-TERM STORAGE & SEARCH

Challenges:

Usage based licensing

Storage costs

Varying retention requirements

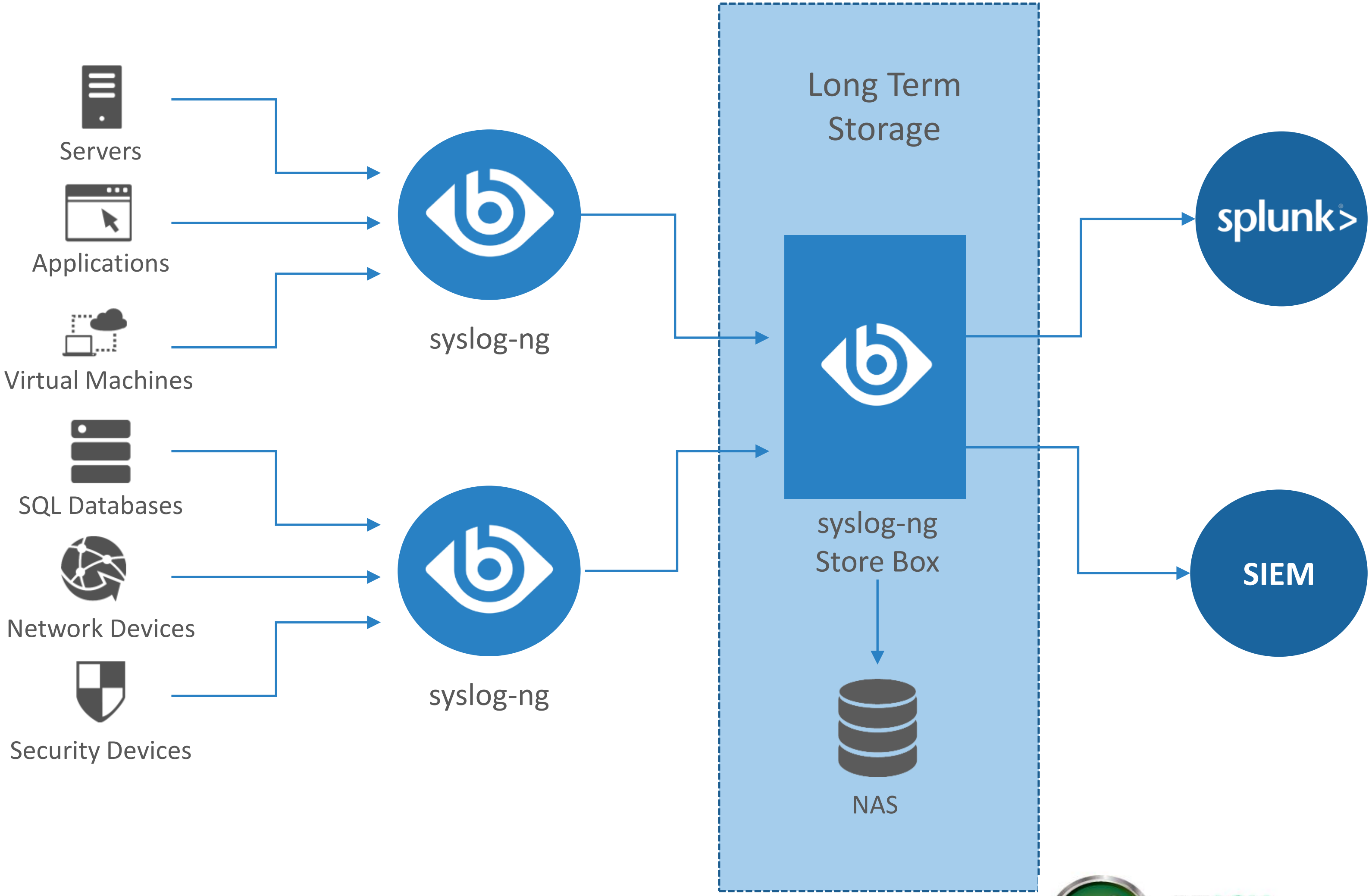
End-goals:

Implement long-term storage layer

Automated retention policies

Automated archiving

Indexed & compressed



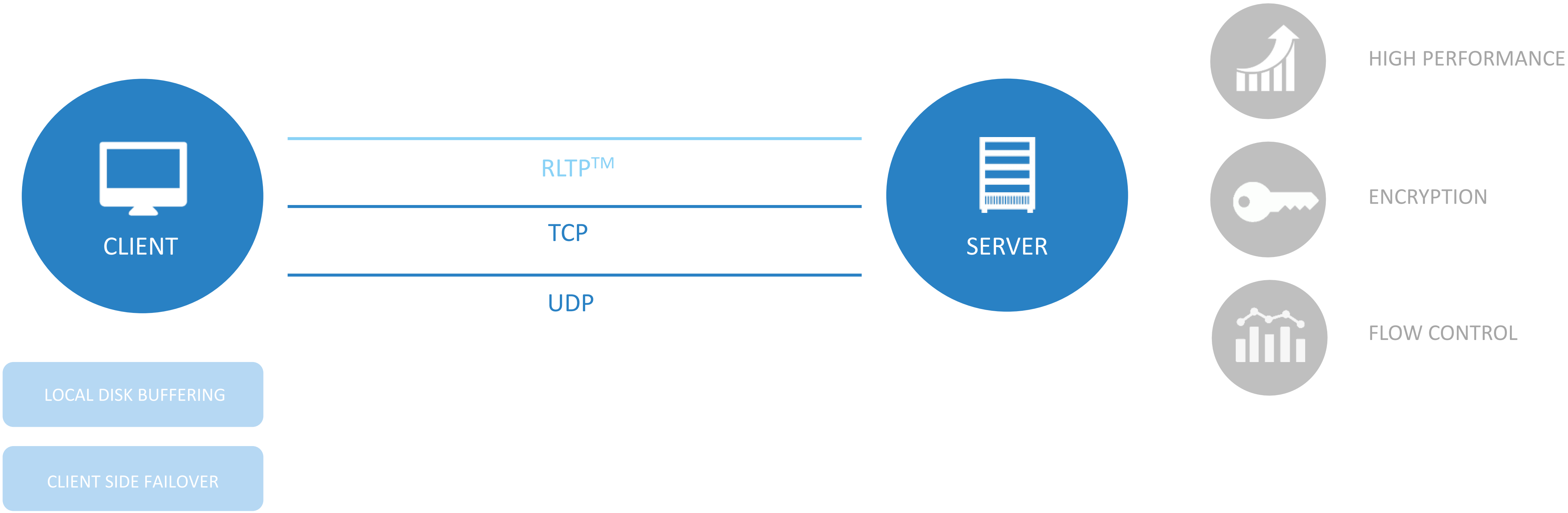
THE VERIZON LOG BREACH

2017 January – June
14 million subscribers were impacted

The actual data that was obtained were log files

Included: name, cell phone number, and the PIN associated with account.

RELIABILITY AND SECURITY



CLIENT

RLTP™

TCP

UDP

SERVER

HIGH PERFORMANCE

ENCRYPTION

FLOW CONTROL

LOCAL DISK BUFFERING

CLIENT SIDE FAILOVER

SYSLOG-NG PRODUCT FAMILY

SYSLOG-NG STORE BOX

High performance, enterprise-class log management appliance

- Price-performance champion turnkey appliance
- Web-based UI - for easy configuration and reporting
- Ultra-fast, full-text search
- Unified search
- Content-based alerting

SYSLOG-NG PREMIUM EDITION

Enterprise-class reliable multiplatform log management

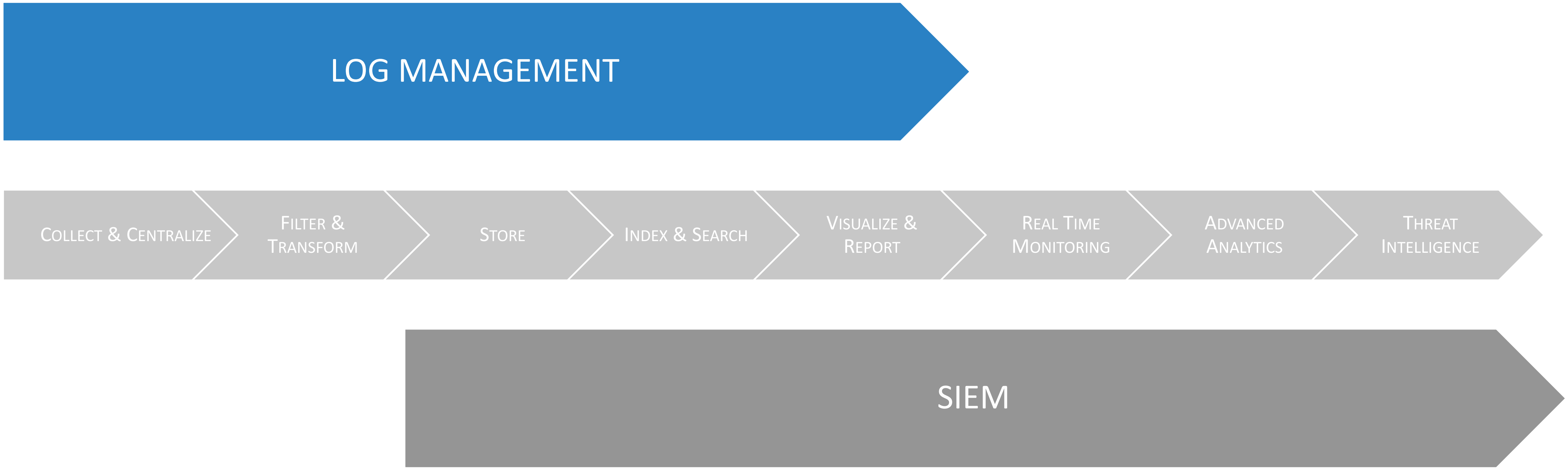
- Enterprise-grade technical and platform support
- Encrypted, time-stamped log store
- Official installation packages, including Windows
- Extended data enrichment
- Zero message loss

SYSLOG-NG OPEN SOURCE EDITION

World renown open source technology

- Rock-solid
- Wide community support
- De facto industry standard
- Message parsing and re-writing

MARKET POSITION



LOG MANAGEMENT

Collect & Centralize

Filter & Transform

Store

Index & Search

Visualize & Report

Real Time Monitoring

Advanced Analytics

Threat Intelligence

SIEM

SYSLOG-NG STORE BOX DESCRIPTION

Turnkey solution
Physical / Virtual Appliance

High performance indexing
100,000 logs/sec sustained
35 GB/hr (collection up to 500,000 logs/sec)

Web- Based Intuitive GUI
Visualization Statistics

Full text search

Reports

Automated Archiving
Raw storage: 1TB - 10 TB

Granular access control
LDAP/Radius Integration

RESTful API

SYSLOG-NG LICENSING

log source hosts

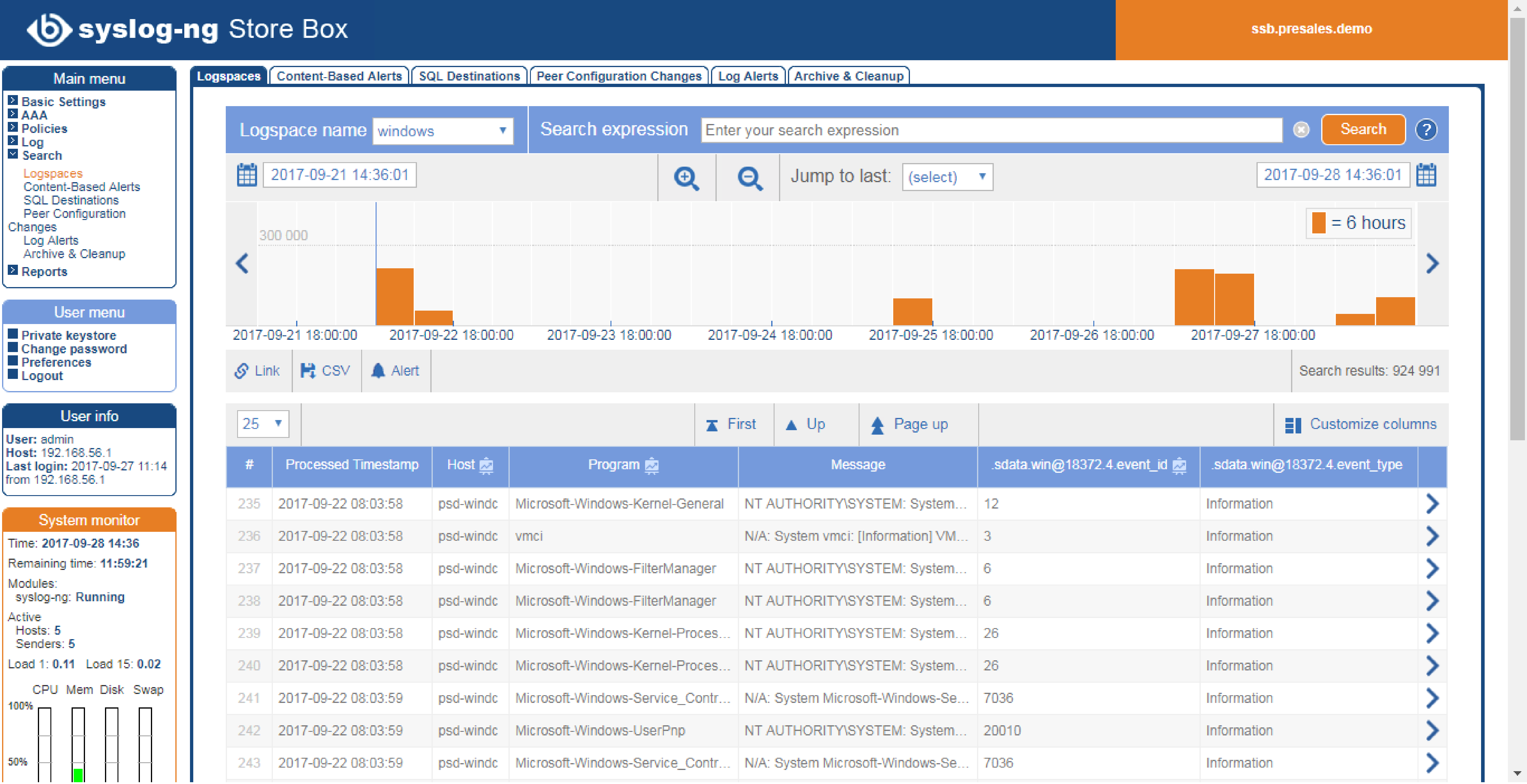
yearly support

powerful hardwares

Vmware ESXi, Microsoft Hyper-V, Microsoft Azure, Amazon AWS

permanent license

easy upgrade



Logspace name: windows

Search expression: Enter your search expression

2017-09-21 14:36:01 – Jump to last: (select) – 2017-09-28 14:36:01

Search results: 924 991

25

User info

User: admin
Host: 192.168.56.1
Last login: 2017-09-27 11:14 from 192.168.56.1

System monitor

Time: **2017-09-28 14:36**
Remaining time: **11:59:21**
Modules:
syslog-ng: **Running**
Active
Hosts: **5**
Senders: **5**
Load 1: **0.11** Load 15: **0.02**

#	Processed Timestamp	Host	Program	Message	.sdata.win@18372.4.event_id	.sdata.win@18372.4.event_type
235	2017-09-22 08:03:58	psd-windc	Microsoft-Windows-Kernel-General	NT AUTHORITY\SYSTEM: System...	12	Information
236	2017-09-22 08:03:58	psd-windc	vmci	N/A: System vmci: [Information] VM...	3	Information
237	2017-09-22 08:03:58	psd-windc	Microsoft-Windows-FilterManager	NT AUTHORITY\SYSTEM: System...	6	Information
238	2017-09-22 08:03:58	psd-windc	Microsoft-Windows-FilterManager	NT AUTHORITY\SYSTEM: System...	6	Information
239	2017-09-22 08:03:58	psd-windc	Microsoft-Windows-Kernel-Proces...	NT AUTHORITY\SYSTEM: System...	26	Information
240	2017-09-22 08:03:58	psd-windc	Microsoft-Windows-Kernel-Proces...	NT AUTHORITY\SYSTEM: System...	26	Information
241	2017-09-22 08:03:59	psd-windc	Microsoft-Windows-Service_Contr...	N/A: System Microsoft-Windows-Se...	7036	Information
242	2017-09-22 08:03:59	psd-windc	Microsoft-Windows-UserPnp	NT AUTHORITY\SYSTEM: System...	20010	Information
243	2017-09-22 08:03:59	psd-windc	Microsoft-Windows-Service_Contr...	N/A: System Microsoft-Windows-Se...	7036	Information

SEARCH INTERFACE

Péter SOPRONI | Cyber Security Consultant | peter.sopronі@balabit.com

PRIVILEGED ACCESS CHALLANGE AND DEMONSTRATION

THESE ARE NOT ENOUGH

FIREWALLS

No granular access control

Admins & APTs can bypass FWs

LOGGING/SIEM PRODUCTS

Several types of events are not logged!

Difficult to understand

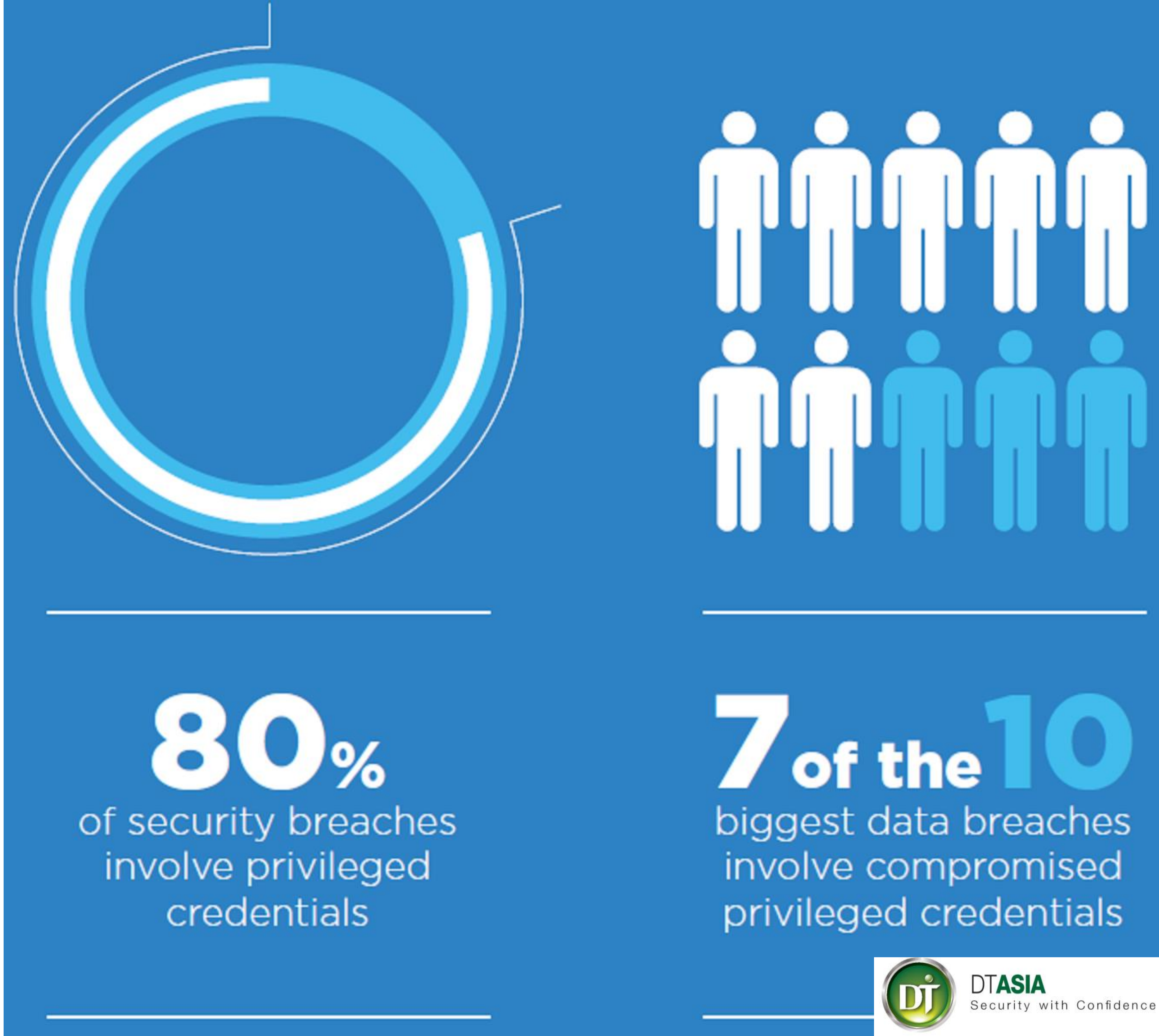
Admins (or attackers) can delete the logs!

PASSWORD MANAGERS

Complex and costly systems

No answer to „who did what?”

PRIVILEGED ACCESS CHALLENGE



80% of security breaches involve privileged credentials

7 of the 10 biggest data breaches involve compromised privileged credentials

Source: Verizon DBIR 2017;
Gemalto Breach Level Index

BALABIT
A ONE IDENTITY BUSINESS

DTASIA
Security with Confidence

THE DELOITTE BREACH

Attack: Oct 2016 – Mar 2017

Announcement: 25 Sep 2017

5 millions emails exposed

6 clients' records stolen

Admin accounts compromised

BUSINESS DRIVERS

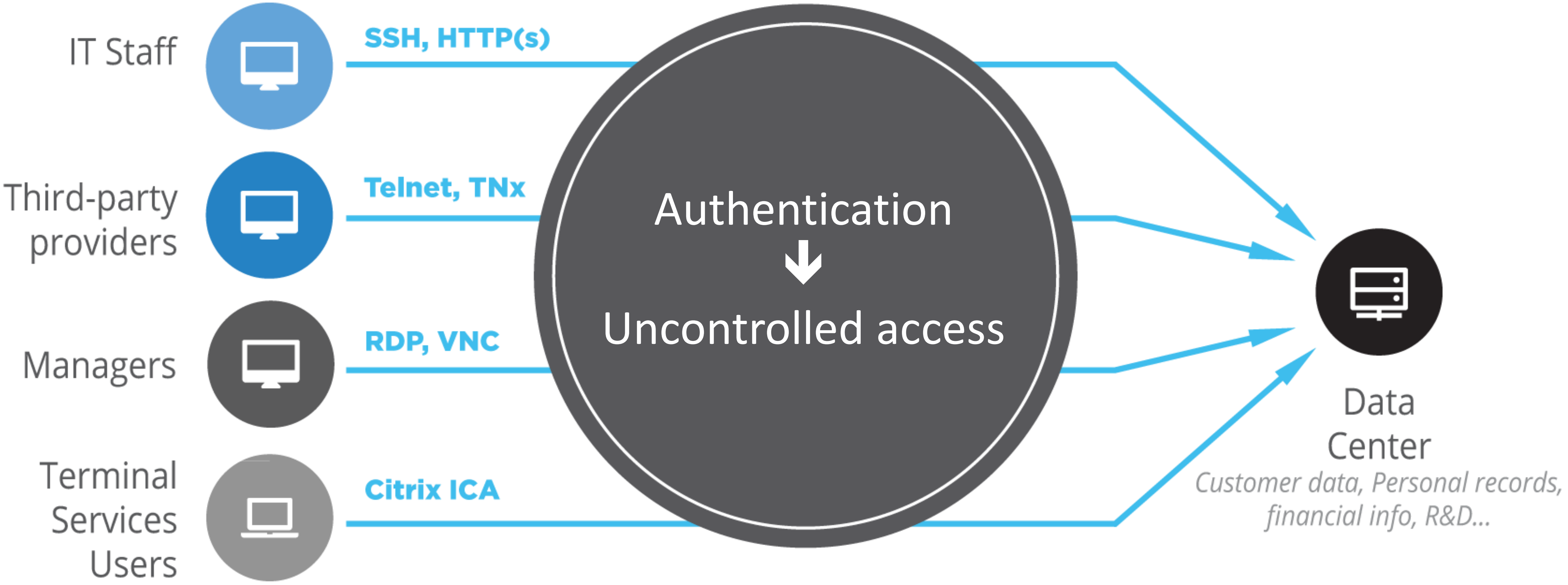
COMPLIANCE

FORENSICS

OUTSOURCING CONTROL

IT STAFF CONTROL

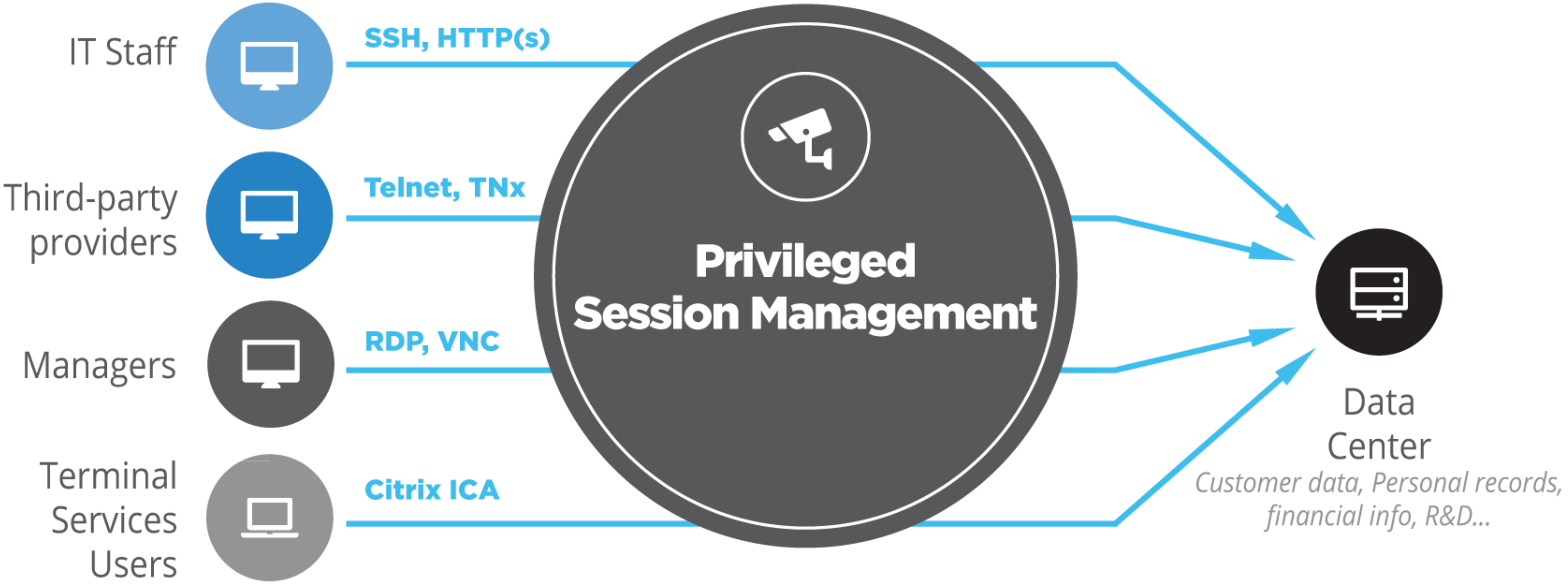
TURNKEY, TRANSPARENT AUDITING



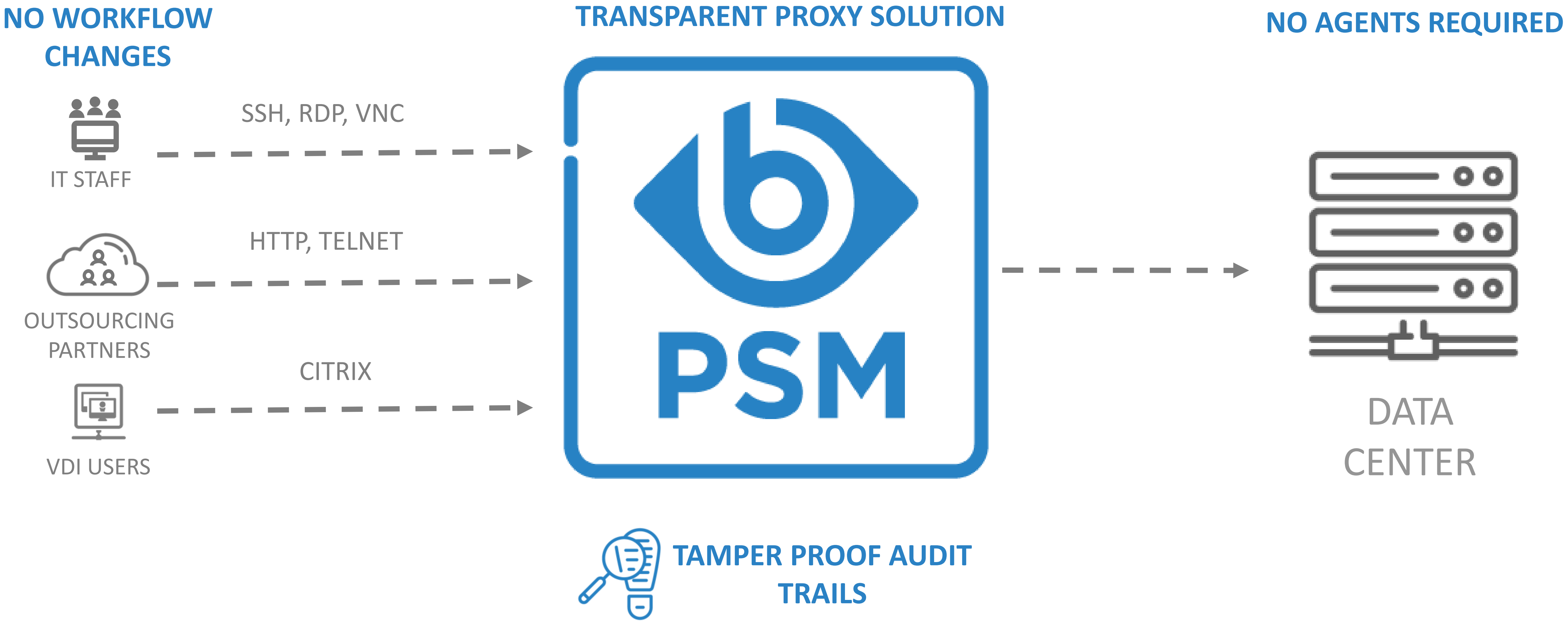
BALABIT
A ONE IDENTITY BUSINESS

DTASIA
Security with Confidence

TURNKEY, TRANSPARENT AUDITING

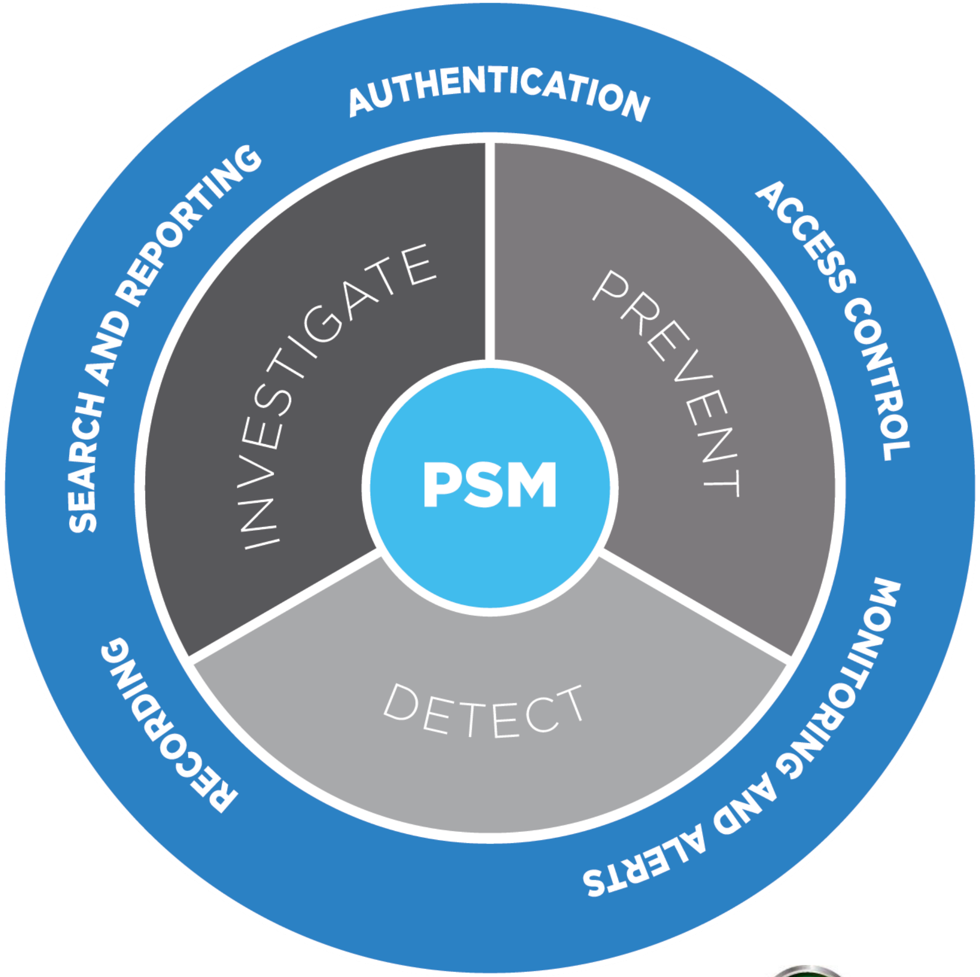


PRIVILEGED SESSION MANAGEMENT

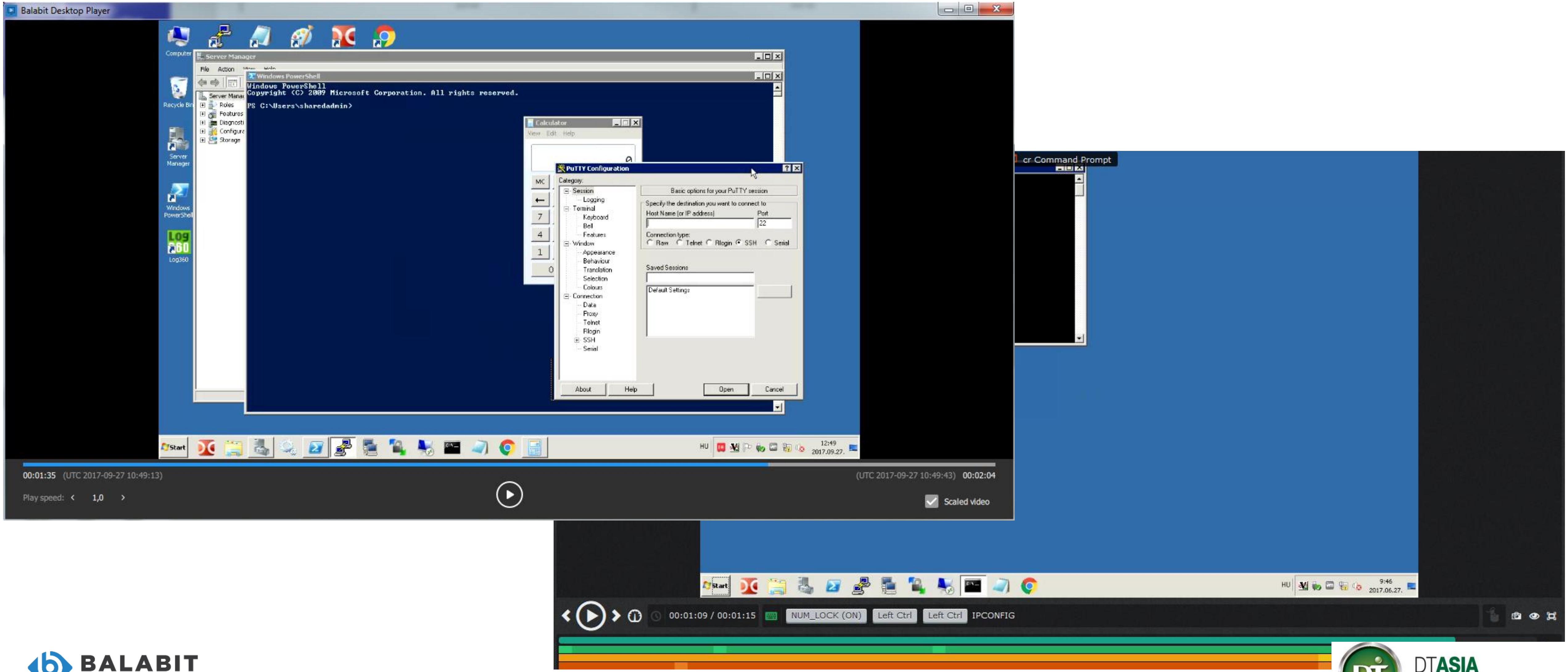


PRIVILEGED SESSION MANAGEMENT

- Controls privileged access to remote servers
- Records activities into movie-like audit trails
- Monitors privileged sessions and send alerts in real-time
- Reports actions for compliance and/or decision support reasons



HIGH-QUALITY AUDIT TRAILS



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\sharedadmin>
```

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) | Port 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Saved Sessions

Default Settings

00:01:35 (UTC 2017-09-27 10:49:13)

(UTC 2017-09-27 10:49:43) 00:02:04

Play speed: ‹ 1,0 ›

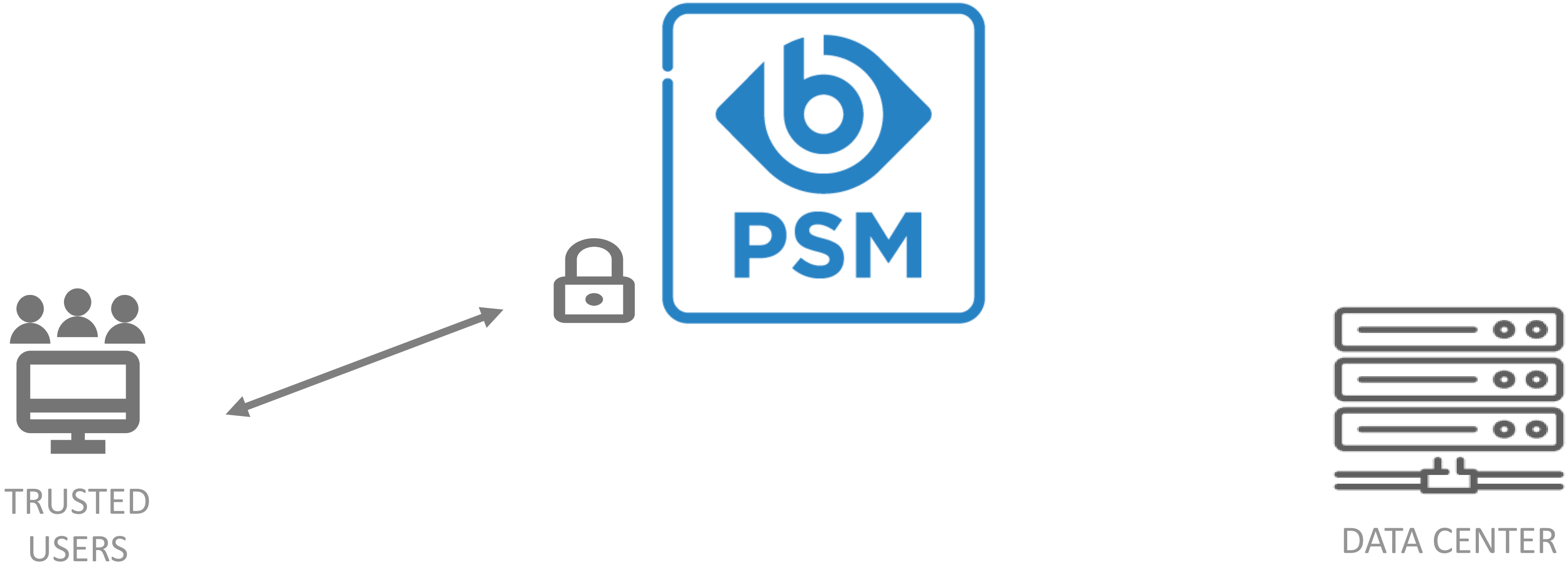
☑ Scaled video

00:01:09 / 00:01:15 NUM_LOCK (ON) Left Ctrl Left Ctrl IPCONFIG

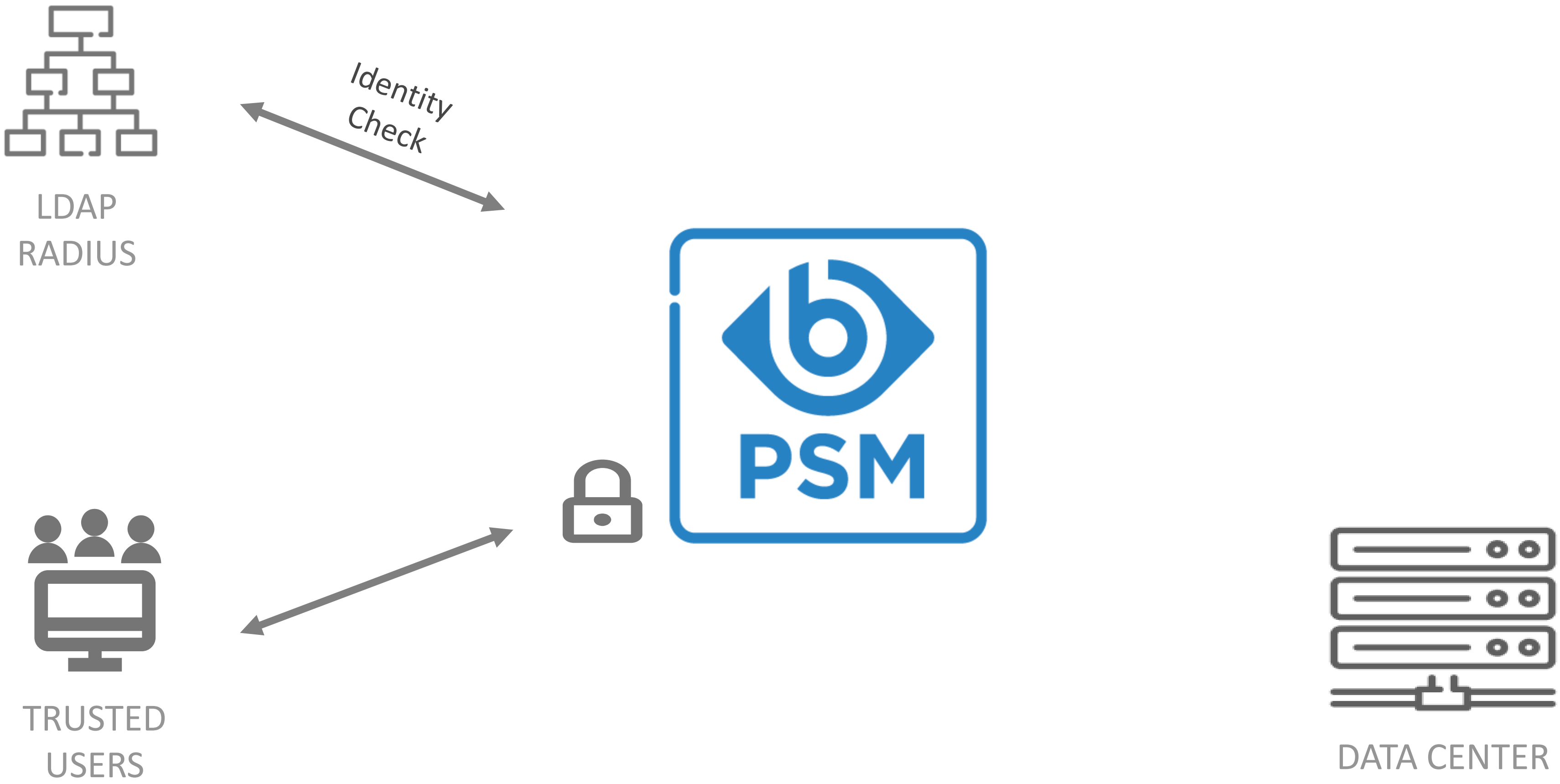
BALABIT
A ONE IDENTITY BUSINESS

DTASIA
Security with Confidence

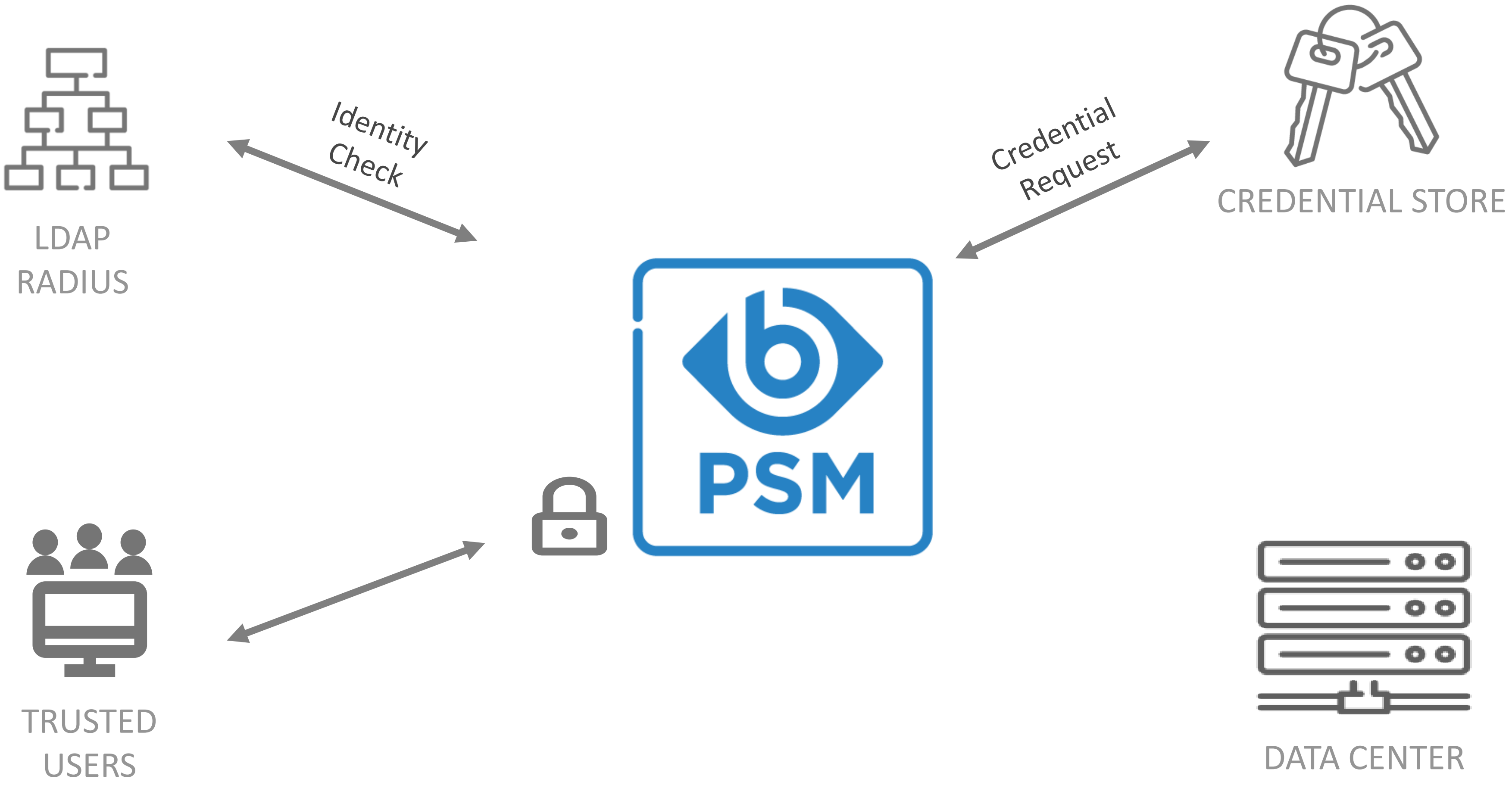
GATEWAY AND SHARED ACCOUNTS



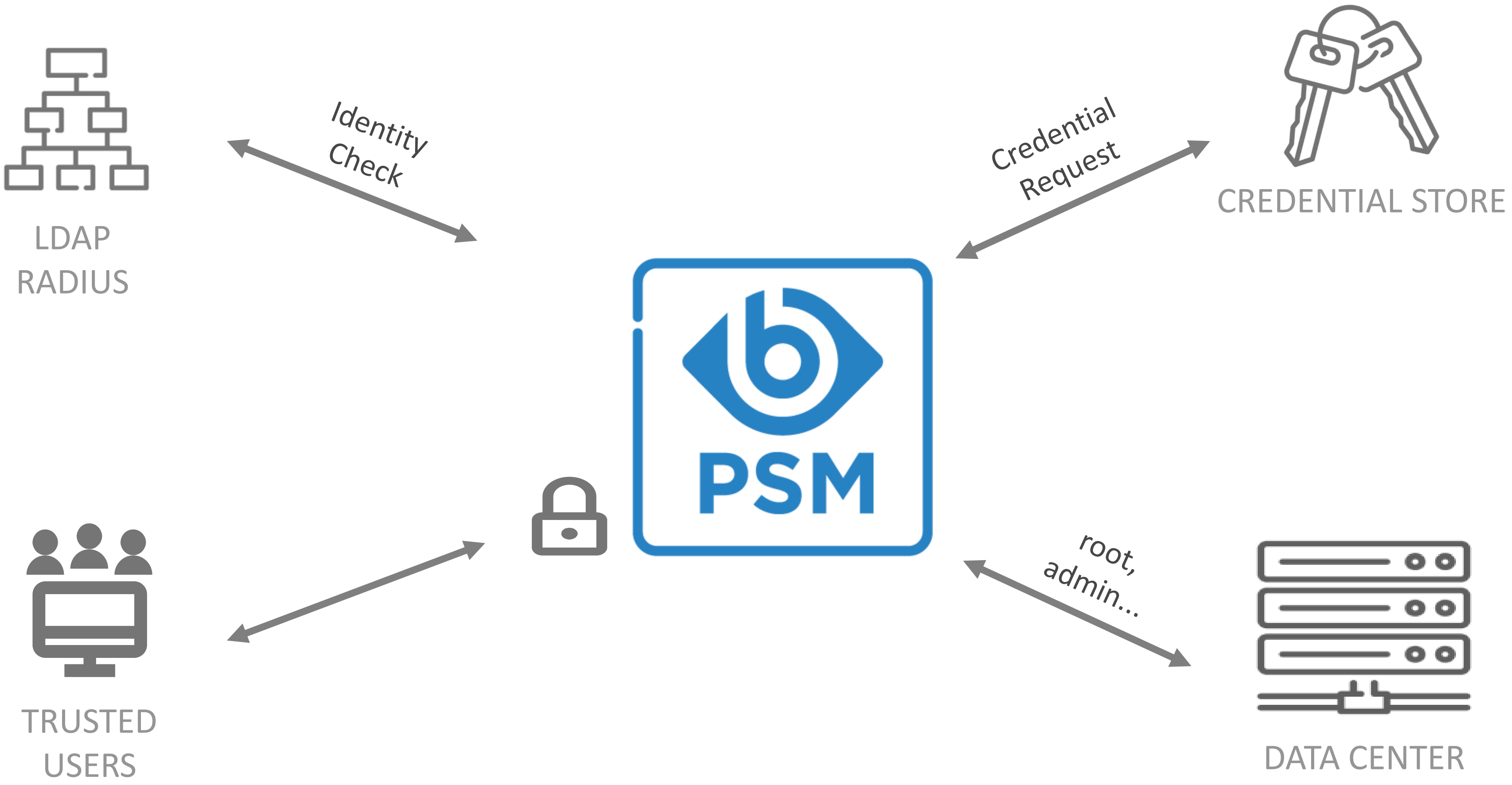
GATEWAY AND SHARED ACCOUNTS



GATEWAY AND SHARED ACCOUNTS



GATEWAY AND SHARED ACCOUNTS



LDAP
RADIUS

Identity
Check

Credential
Request

CREDENTIAL STORE

PSM

TRUSTED
USERS

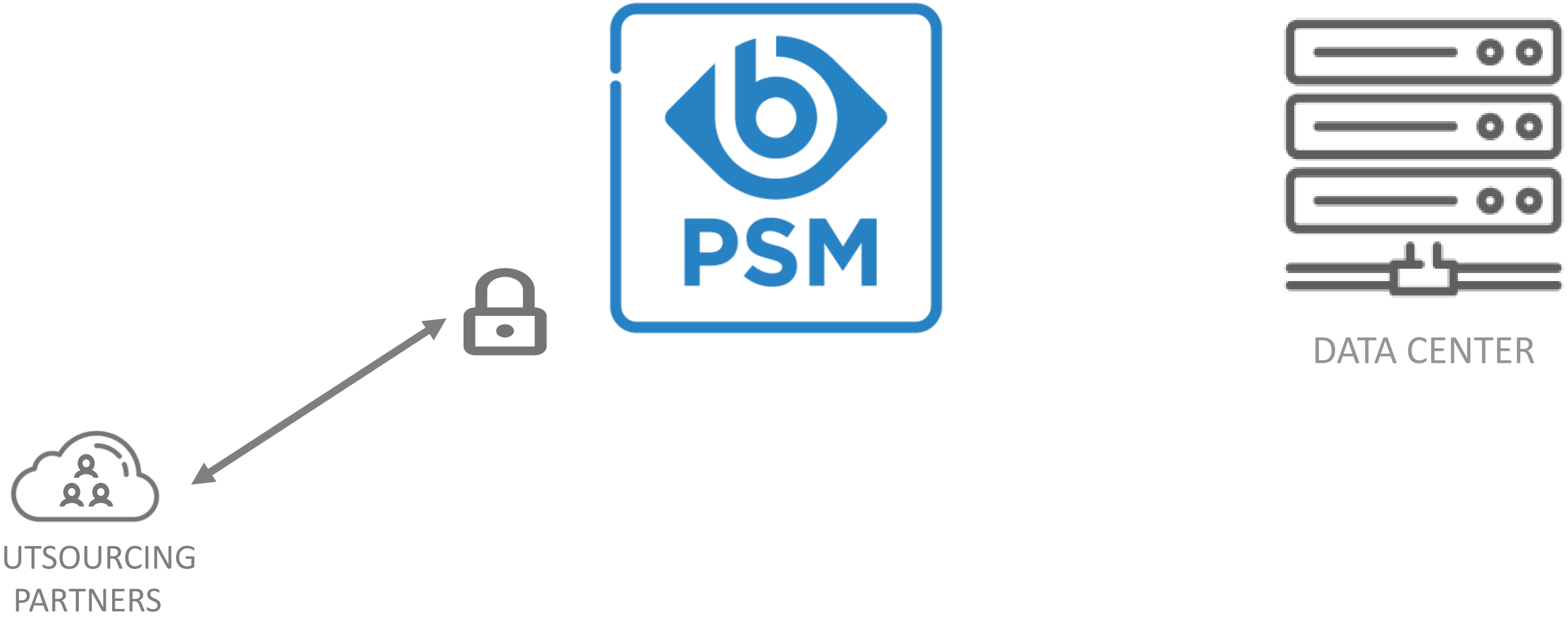
root,
admin...

DATA CENTER

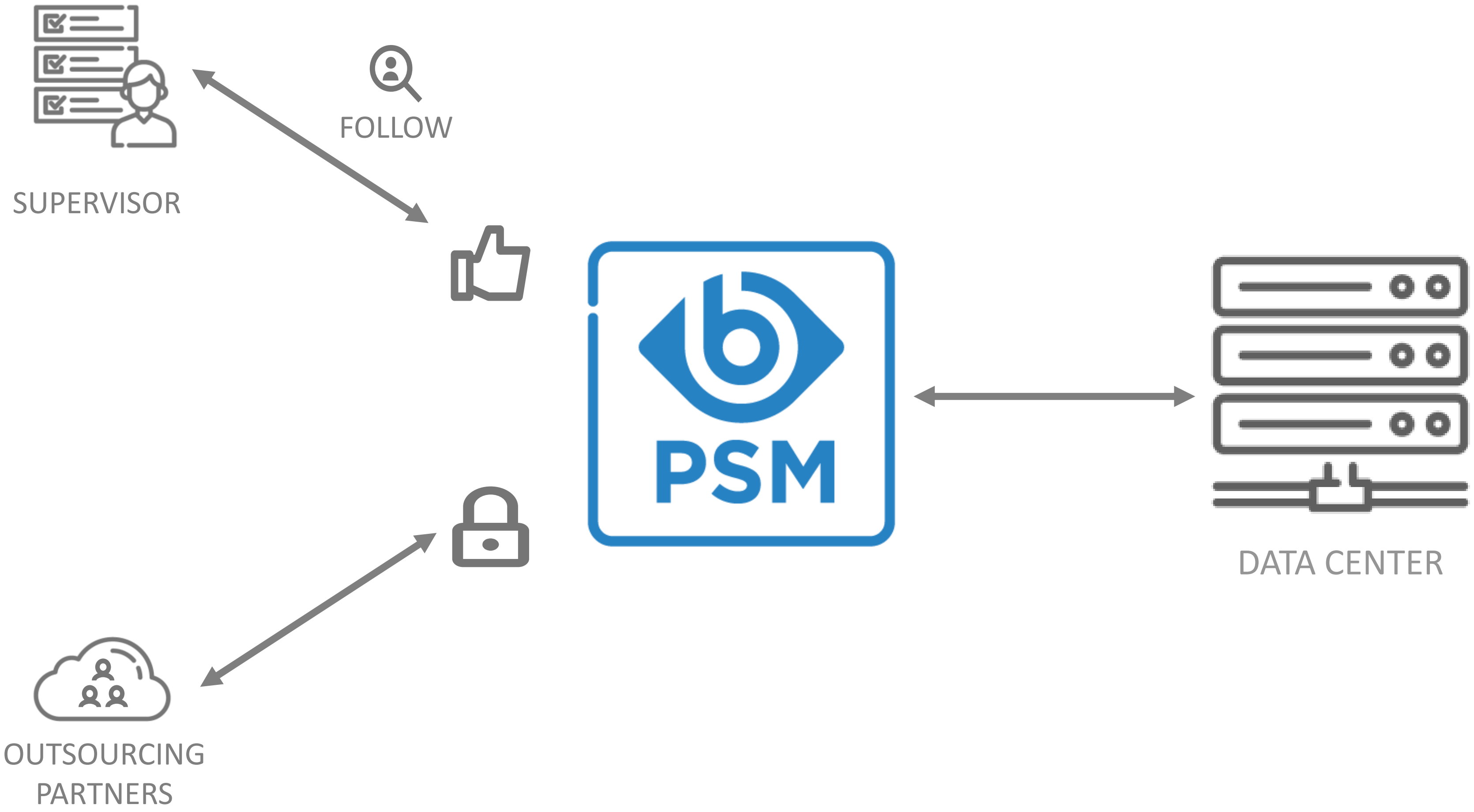
BALABIT
A ONE IDENTITY BUSINESS

DTASIA
Security with Confidence

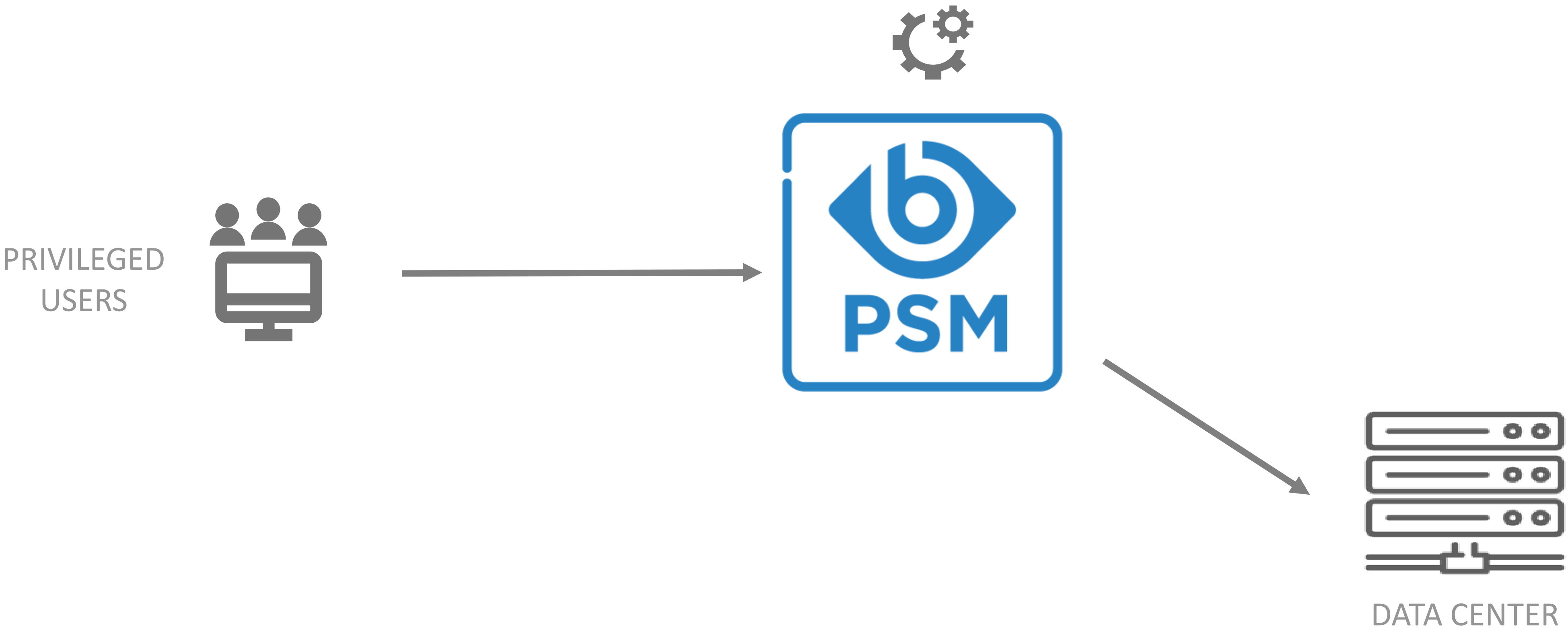
AUTHORIZATION AND SUPERVISION



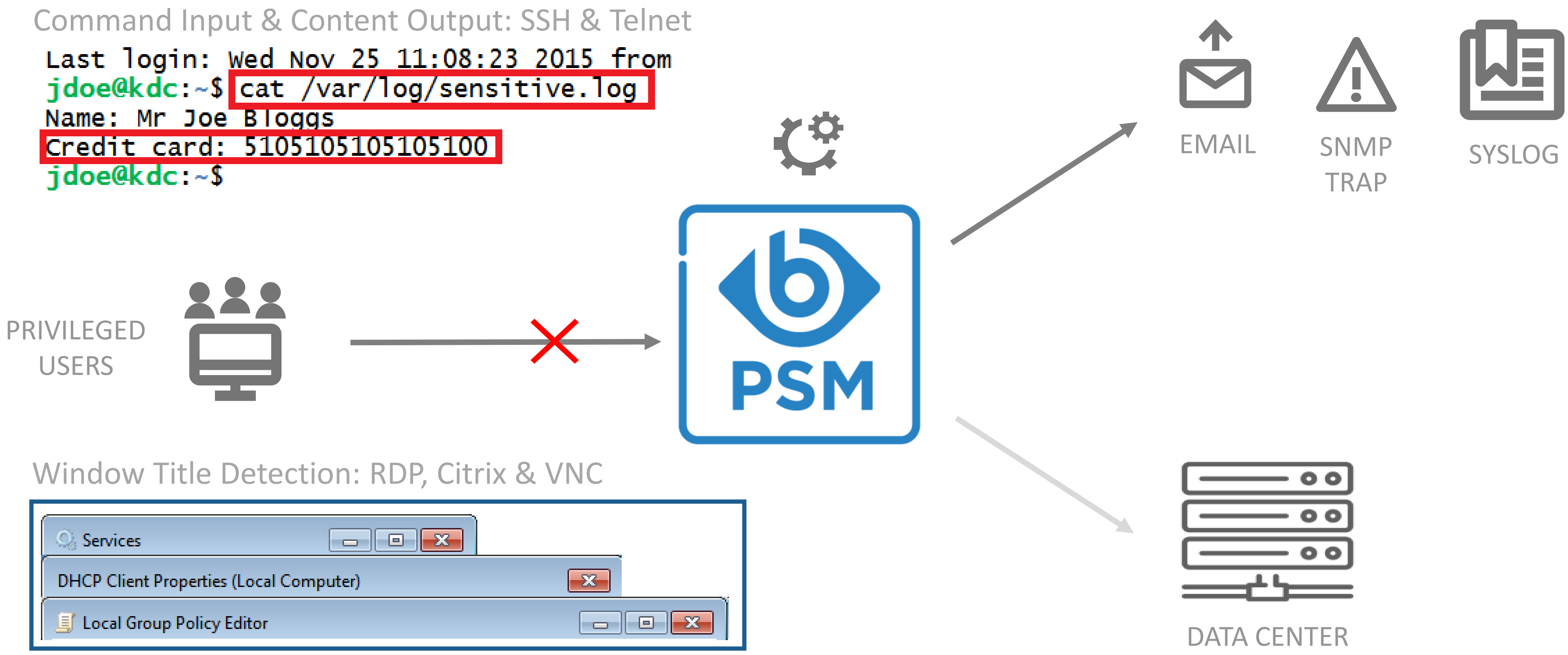
AUTHORIZATION AND SUPERVISION



CONTENT ALERTING & BLOCKING



CONTENT ALERTING & BLOCKING



Command Input & Content Output: SSH & Telnet

```
Last login: Wed Nov 25 11:08:23 2015 from
jdoe@kdc:~$ cat /var/log/sensitive.log
Name: Mr Joe Bloggs
Credit card: 5105105105105100
jdoe@kdc:~$
```

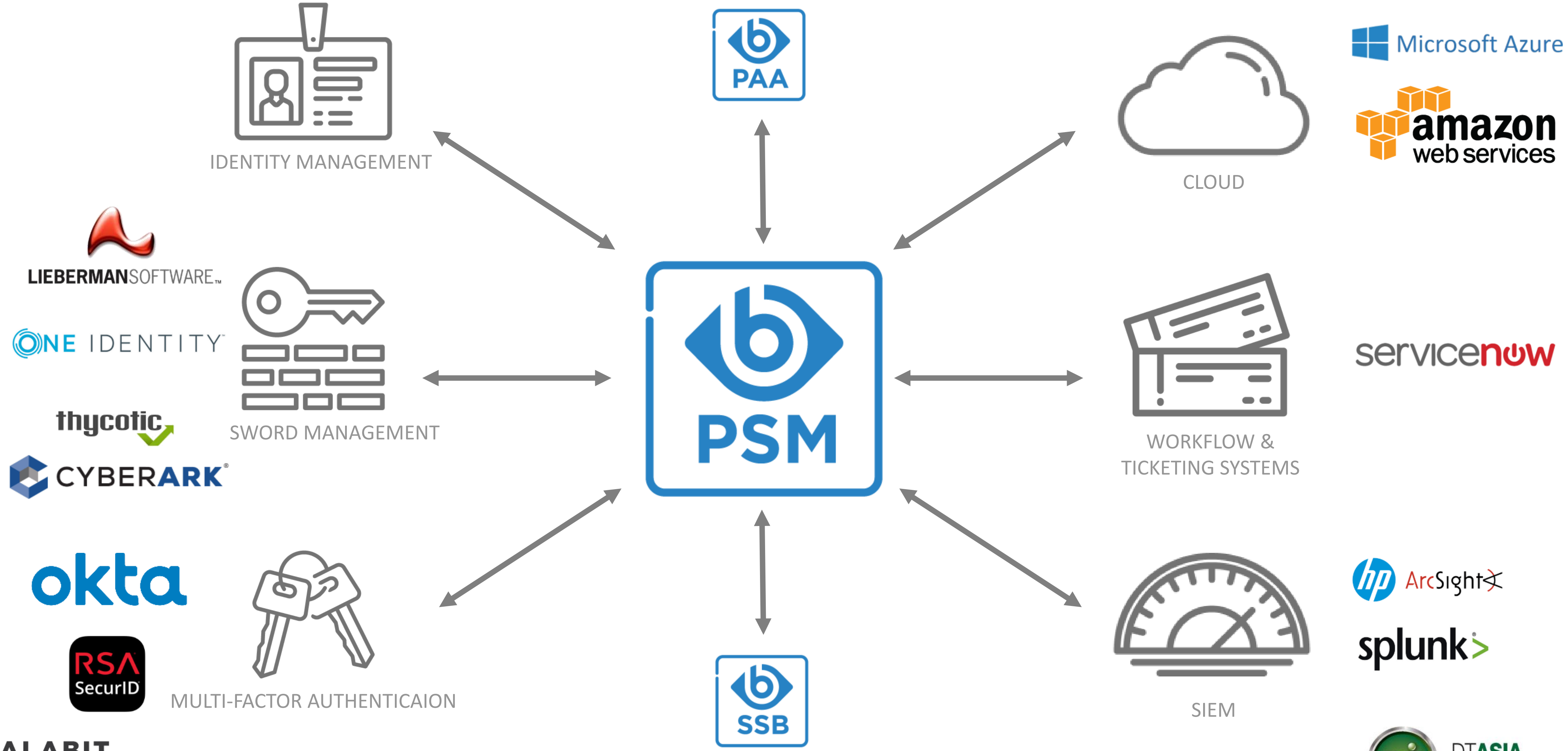
Window Title Detection: RDP, Citrix & VNC

Services

DHCP Client Properties (Local Computer)

Local Group Policy Editor

SEAMLESS ENTERPRISE INTEGRATION

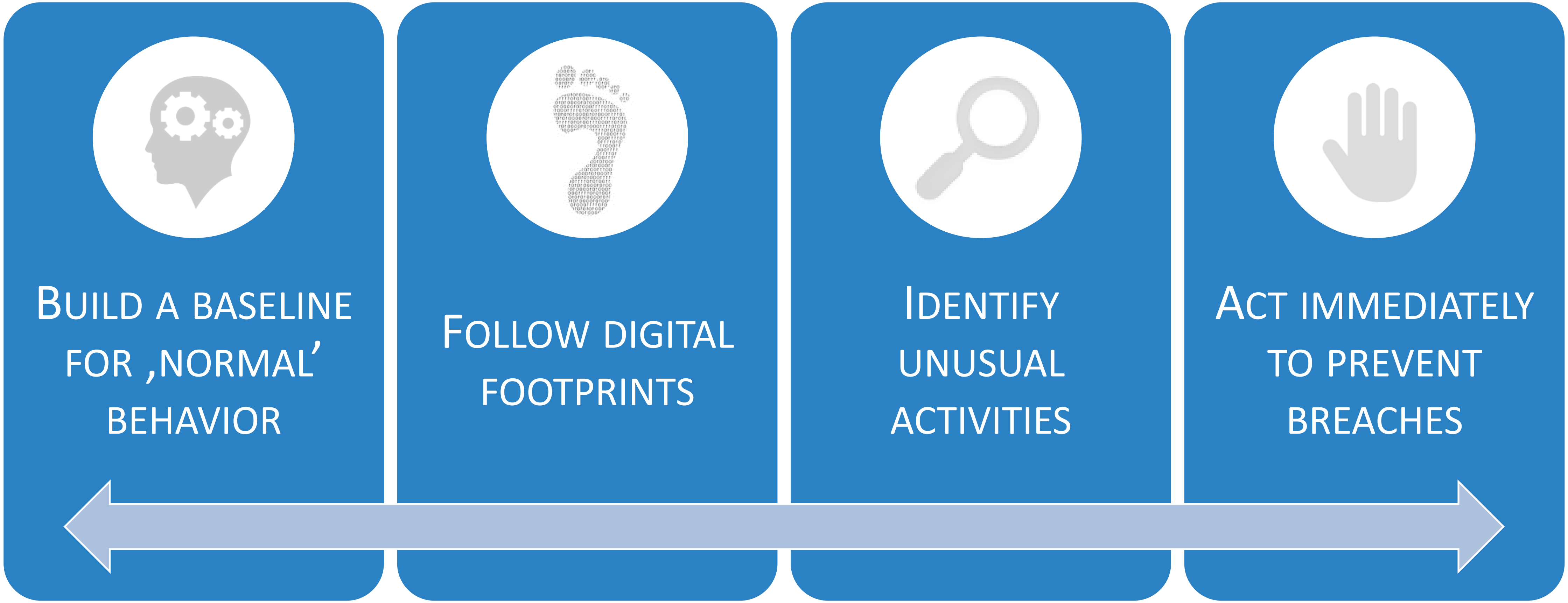


BALABIT
A ONE IDENTITY BUSINESS

All registered and unregistered logos and trademarks used on this slide are the property of their respective owners. Balabit is not an authorized partner of CyberArk®. The technical inte
on CyberArk® Enterprise Password Vault® ver.7.20. The interoperability has not been endorsed or authorized by CyberArk®.

DTASIA
Security with Confidence

PRIVILEGED ACCOUNT ANALYTICS



BUILD A BASELINE FOR ‚NORMAL’ BEHAVIOR

FOLLOW DIGITAL FOOTPRINTS

IDENTIFY UNUSUAL ACTIVITIES

ACT IMMEDIATELY TO PREVENT BREACHES

DIGITAL BEHAVIOR

Behavioral information based on log data

Typical time of logging in

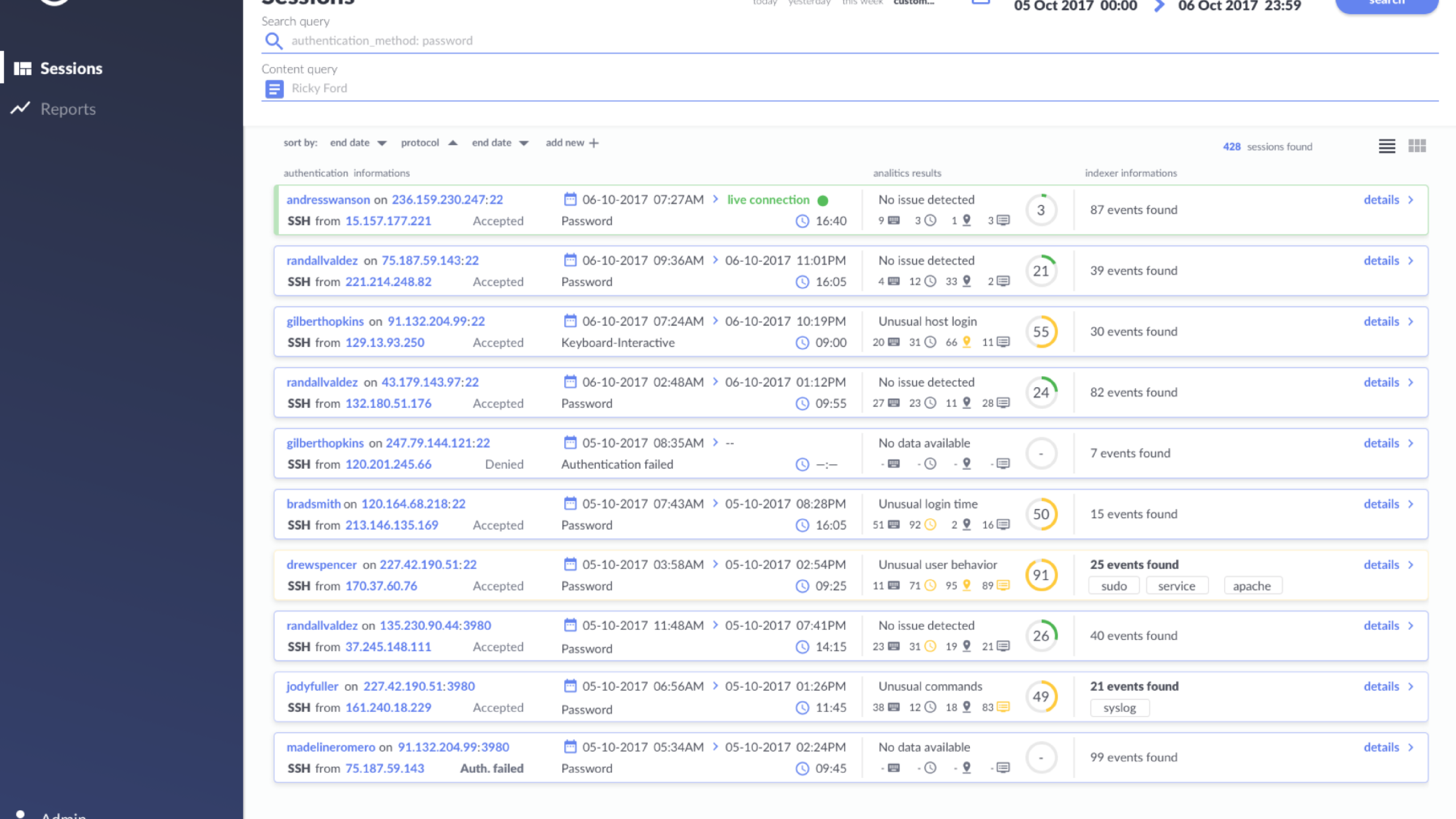
Range of accessed servers and applications

Behavioral information based on granular PSM data

Activities performed

Mouse movement characteristics

Keystroke dynamics analysis



Sessions

05 Oct 2017 00:00 > 06 Oct 2017 23:59

Search query

authentication_method: password

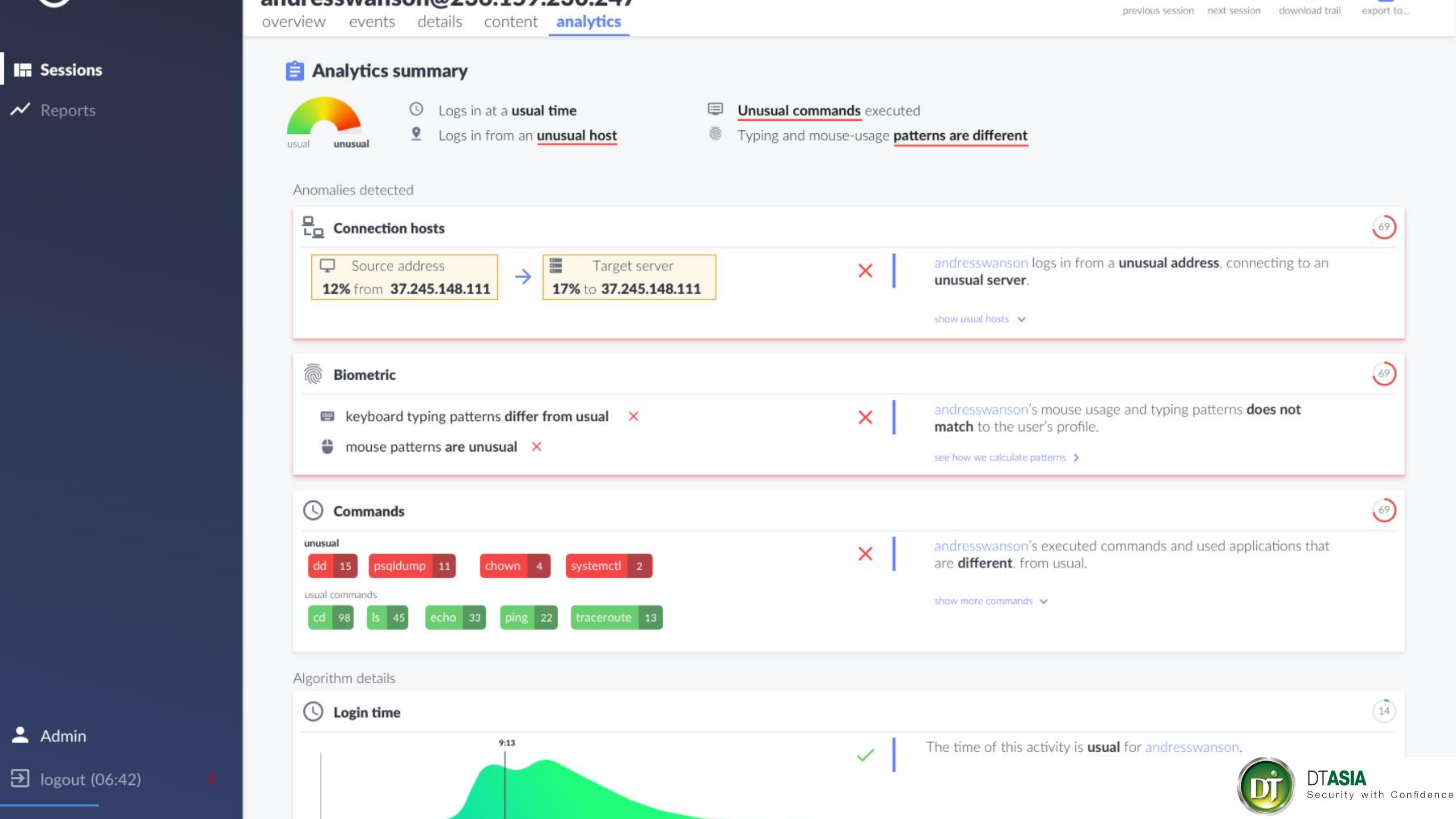
Content query

Ricky Ford

sort by: end date ▼ protocol ▲ end date ▼ add new +

428 sessions found

authentication informations		analitics results		indexer informations	
andresswanson on 236.159.230.247:22 SSH from 15.157.177.221 Accepted	06-10-2017 07:27AM > live connection ● Password 🕒 16:40	No issue detected 9 ⌨ 3 🕒 1 📍 3 ▤	3	87 events found	details >
randallvaldez on 75.187.59.143:22 SSH from 221.214.248.82 Accepted	06-10-2017 09:36AM > 06-10-2017 11:01PM Password 🕒 16:05	No issue detected 4 ⌨ 12 🕒 33 📍 2 ▤	21	39 events found	details >
gilberthopkins on 91.132.204.99:22 SSH from 129.13.93.250 Accepted	06-10-2017 07:24AM > 06-10-2017 10:19PM Keyboard-Interactive 🕒 09:00	Unusual host login 20 ⌨ 31 🕒 66 📍 11 ▤	55	30 events found	details >
randallvaldez on 43.179.143.97:22 SSH from 132.180.51.176 Accepted	06-10-2017 02:48AM > 06-10-2017 01:12PM Password 🕒 09:55	No issue detected 27 ⌨ 23 🕒 11 📍 28 ▤	24	82 events found	details >
gilberthopkins on 247.79.144.121:22 SSH from 120.201.245.66 Denied	05-10-2017 08:35AM > -- Authentication failed 🕒 --:--	No data available - ⌨ - 🕒 - 📍 - ▤	-	7 events found	details >
bradsmith on 120.164.68.218:22 SSH from 213.146.135.169 Accepted	05-10-2017 07:43AM > 05-10-2017 08:28PM Password 🕒 16:05	Unusual login time 51 ⌨ 92 🕒 2 📍 16 ▤	50	15 events found	details >
drewspencer on 227.42.190.51:22 SSH from 170.37.60.76 Accepted	05-10-2017 03:58AM > 05-10-2017 02:54PM Password 🕒 09:25	Unusual user behavior 11 ⌨ 71 🕒 95 📍 89 ▤	91	**25 events found** sudo service apache	details >
randallvaldez on 135.230.90.44:3980 SSH from 37.245.148.111 Accepted	05-10-2017 11:48AM > 05-10-2017 07:41PM Password 🕒 14:15	No issue detected 23 ⌨ 31 🕒 19 📍 21 ▤	26	40 events found	details >
jodyfuller on 227.42.190.51:3980 SSH from 161.240.18.229 Accepted	05-10-2017 06:56AM > 05-10-2017 01:26PM Password 🕒 11:45	Unusual commands 38 ⌨ 12 🕒 18 📍 83 ▤	49	**21 events found** syslog	details >
madelineromero on 91.132.204.99:3980 SSH from 75.187.59.143 **Auth. failed**	05-10-2017 05:34AM > 05-10-2017 02:24PM Password 🕒 09:45	No data available - ⌨ - 🕒 - 📍 - ▤	-	99 events found	details >



Analytics summary

Logs in at a **usual time**

Logs in from an **unusual host**

Unusual commands executed

Typing and mouse-usage **patterns are different**

Anomalies detected

Connection hosts

Source address: **12%** from **37.245.148.111** → Target server: **17%** to **37.245.148.111** ✗

andresswanson logs in from a **unusual address**, connecting to an **unusual server**.

show usual hosts

Biometric

keyboard typing patterns **differ from usual** ✗

mouse patterns **are unusual** ✗

✗ andresswanson's mouse usage and typing patterns **does not match** to the user's profile.

see how we calculate patterns

Commands

unusual

dd	15
psqldump	11
chown	4
systemctl	2

usual commands

cd	98
ls	45
echo	33
ping	22
traceroute	13

✗ andresswanson's executed commands and used applications that are **different**. from usual.

show more commands

Algorithm details

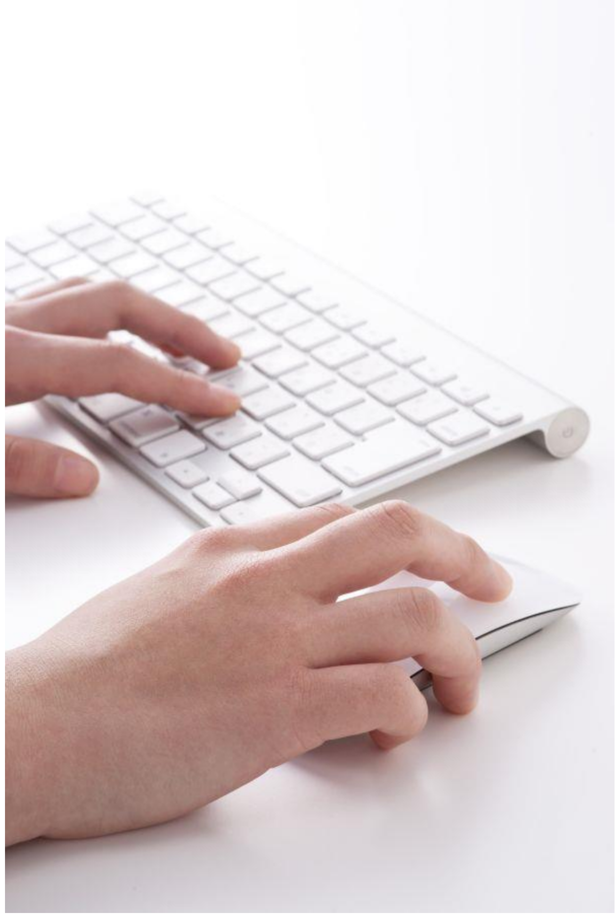
Login time

✓ The time of this activity is **usual** for andresswanson.

DTASIA
Security with Confidence

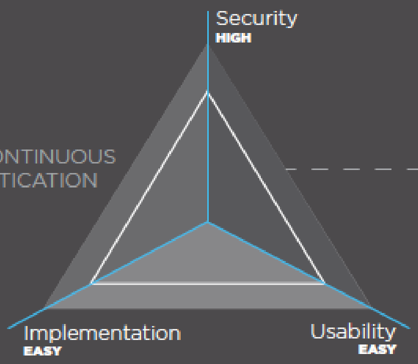
BEHAVIORAL BIOMETRICS

- How a user interacts with a device
- Dynamic information – difficult to steal
- Continuous monitoring of all traffic to identify hijacked accounts in real-time



EVOLUTION OF AUTHENTICATION

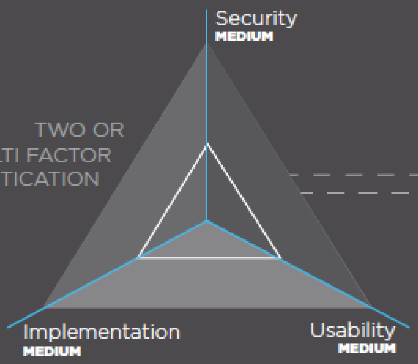
CONTINUOUS AUTHENTICATION



[Since 2015] Continuous Authentication
Combining MFA, real time monitoring and anomaly detection into one unified authentication method

[Late 2010] Multi Factor Authentication
2FA evolved into Multi Factor Authentication by introducing biometric identifiers as authentication variables

TWO OR MULTI FACTOR AUTHENTICATION



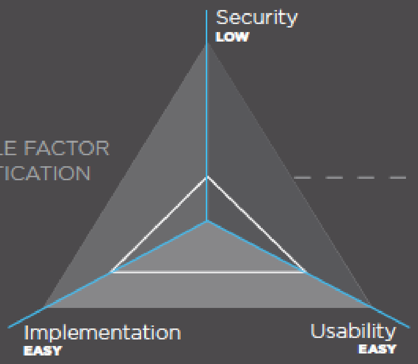
[Mid 2000's] Two Factor Authentication
With the introduction of software tokens Two Factor Authentication was born

[Early 2000's] Privileged Identity & Session Management
Enterprise level password and access management hit the market

[Mid 1990's] Hardware tokens
Hardware tokens were introduced as an additional authentication factor

[1990] The World Wide Web
Authentication procedures were introduced on secured websites

SINGLE FACTOR AUTHENTICATION



[1988] Single Factor Authentication
The Morris Internet Worm lead to development of strong passwords and Single Factor Authentication on all critical devices

[1970] Secured storage of passwords on UNIX
Storing passwords in hashed format

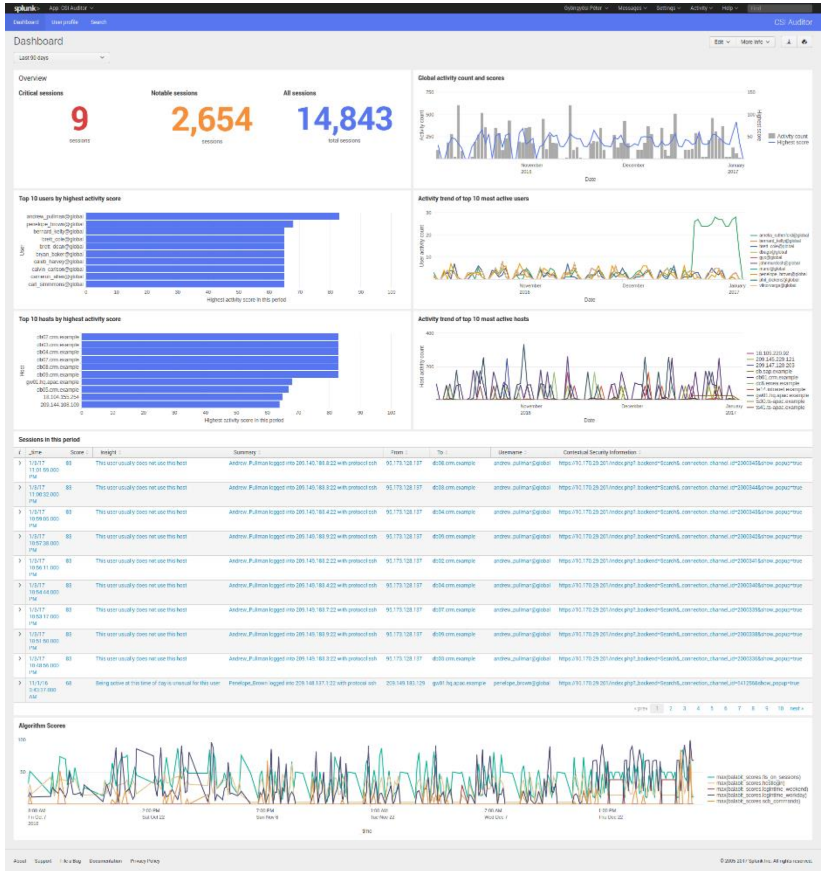
[1961] MIT CTSS
Earliest entry of passwords in IT

BALABIT

www.balabit.com

3RD PARTY INTEGRATION: SPLUNK

- Balabit app in Splunk displays all information available in the web-based UI of Privileged Account Analytics, including:
  - All raw data, such as commands or window titles
  - Algorithm scores
  - Prioritized activity and user top lists
  - Quick access to the session recordings of privileged users



Sessions in this period

_time	Score	Insight	Summary	From	To	Username	Contextual Security Information
1/3/17 11:01:59.000 PM	83	This user usually does not use this host	Andrew_Pullman logged into 209.149.183.8:22 with protocol ssh	93.173.128.137	dc08.crm.example	andrew_pullman@global	https://10.170.29.201/index.php?_backend=Search&_connection_channel_id=2000345&show_popup=true
1/3/17 11:00:32.000 PM	83	This user usually does not use this host	Andrew_Pullman logged into 209.149.183.3:22 with protocol ssh	93.173.128.137	dc03.crm.example	andrew_pullman@global	https://10.170.29.201/index.php?_backend=Search&_connection_channel_id=2000344&show_popup=true
1/3/17 10:59:05.000 PM	83	This user usually does not use this host	Andrew_Pullman logged into 209.149.183.4:22 with protocol ssh	93.173.128.137	dc04.crm.example	andrew_pullman@global	https://10.170.29.201/index.php?_backend=Search&_connection_channel_id=2000343&show_popup=true
1/3/17 10:57:38.000 PM	83	This user usually does not use this host	Andrew_Pullman logged into 209.149.183.9:22 with protocol ssh	93.173.128.137	dc09.crm.example	andrew_pullman@global	https://10.170.29.201/index.php?_backend=Search&_connection_channel_id=2000342&show_popup=true
1/3/17 10:56:11.000 PM	83	This user usually does not use this host	Andrew_Pullman logged into 209.149.183.2:22 with protocol ssh	93.173.128.137	dc02.crm.example	andrew_pullman@global	https://10.170.29.201/index.php?_backend=Search&_connection_channel_id=2000341&show_popup=true
1/3/17 10:54:44.000 PM	83	This user usually does not use this host	Andrew_Pullman logged into 209.149.183.4:22 with protocol ssh	93.173.128.137	dc04.crm.example	andrew_pullman@global	https://10.170.29.201/index.php?_backend=Search&_connection_channel_id=2000340&show_popup=true
1/3/17 10:53:17.000 PM	83	This user usually does not use this host	Andrew_Pullman logged into 209.149.183.7:22 with protocol ssh	93.173.128.137	dc07.crm.example	andrew_pullman@global	https://10.170.29.201/index.php?_backend=Search&_connection_channel_id=2000339&show_popup=true
1/3/17 10:51:50.000 PM	83	This user usually does not use this host	Andrew_Pullman logged into 209.149.183.9:22 with protocol ssh	93.173.128.137	dc09.crm.example	andrew_pullman@global	https://10.170.29.201/index.php?_backend=Search&_connection_channel_id=2000338&show_popup=true
1/3/17 10:48:56.000 PM	83	This user usually does not use this host	Andrew_Pullman logged into 209.149.183.3:22 with protocol ssh	93.173.128.137	dc03.crm.example	andrew_pullman@global	https://10.170.29.201/index.php?_backend=Search&_connection_channel_id=2000336&show_popup=true
11/1/16 3:43:17.000 AM	68	Being active at this time of day is unusual for this user	Penelope_Brown logged into 209.148.137.1:22 with protocol ssh	209.149.183.129	gw01.hq.apac.example	penelope_brown@global	https://10.170.29.201/index.php?_backend=Search&_connection_channel_id=1412568&show_popup=true

« prev 1 2 3 4 5 6 7 8 9 10 next »

PAM LICENSING

yearly support

protected devices

powerful hardwares

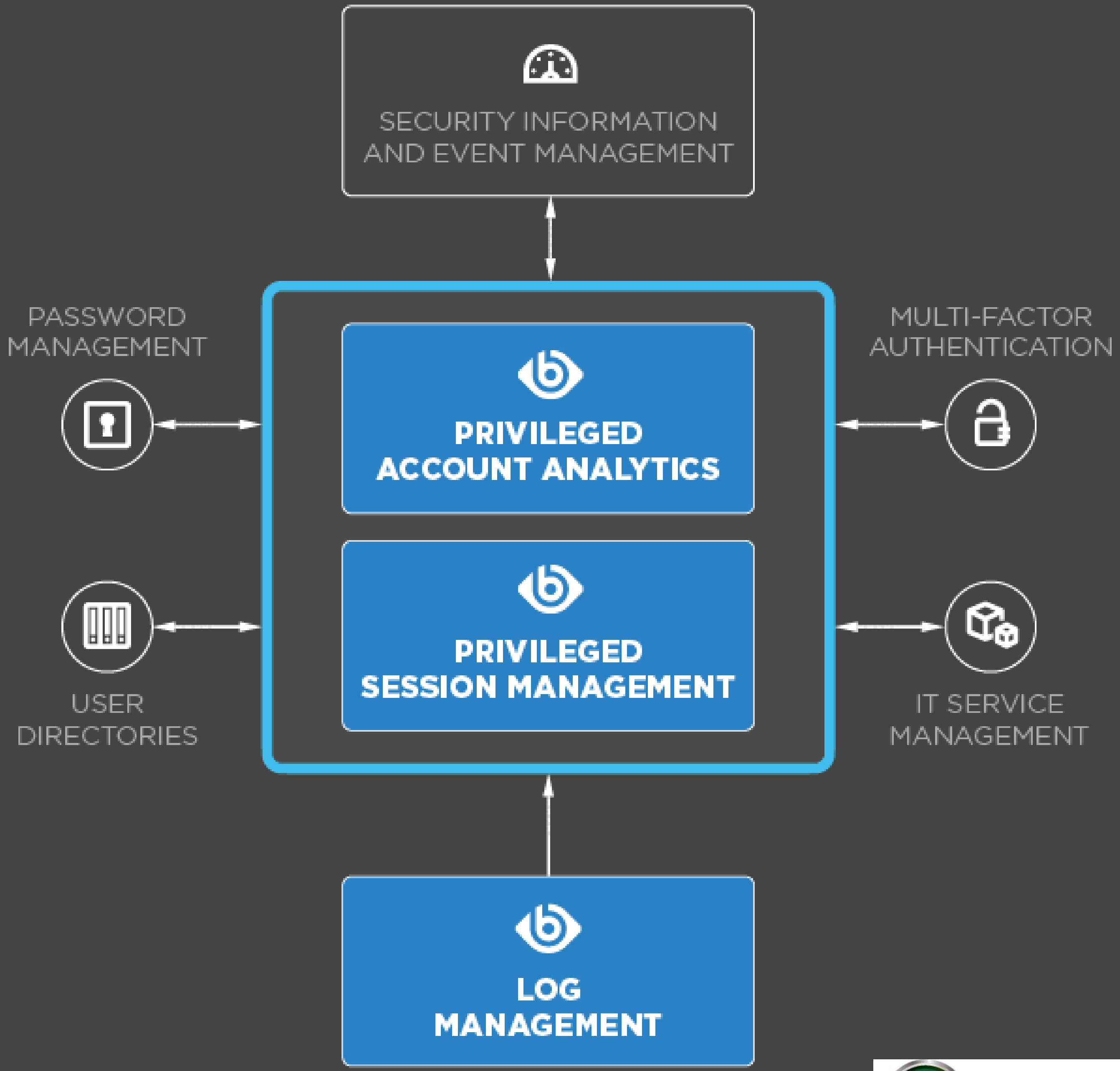
Vmware ESXi, KVM, Microsoft Hyper-V, Microsoft Azure, Amazon AWS

permanent license

easy upgrade

HOW BALABIT CAN HELP TO INCREASE SECURITY AND RELIABILITY?

BALABIT PRIVILEGED ACCESS MANAGEMENT


SECURITY INFORMATION AND EVENT MANAGEMENT
PASSWORD MANAGEMENT
PRIVILEGED ACCOUNT ANALYTICS
MULTI-FACTOR AUTHENTICATION
USER DIRECTORIES
PRIVILEGED SESSION MANAGEMENT
IT SERVICE MANAGEMENT
LOG MANAGEMENT

BALABIT
A ONE IDENTITY BUSINESS

DTASIA
Security with Confidence

Reliabe and Secure Log collection

- Single instance scale up to 300k EPS
- Licensed based on IP addresses
- Integration with SIEM and Big Data
- RLTP, Disk buffer

Protection against Privileged Account misusage

- Free text content search
- Tamper-proof audit trails
- User behavior analytics
- Real-time alerting

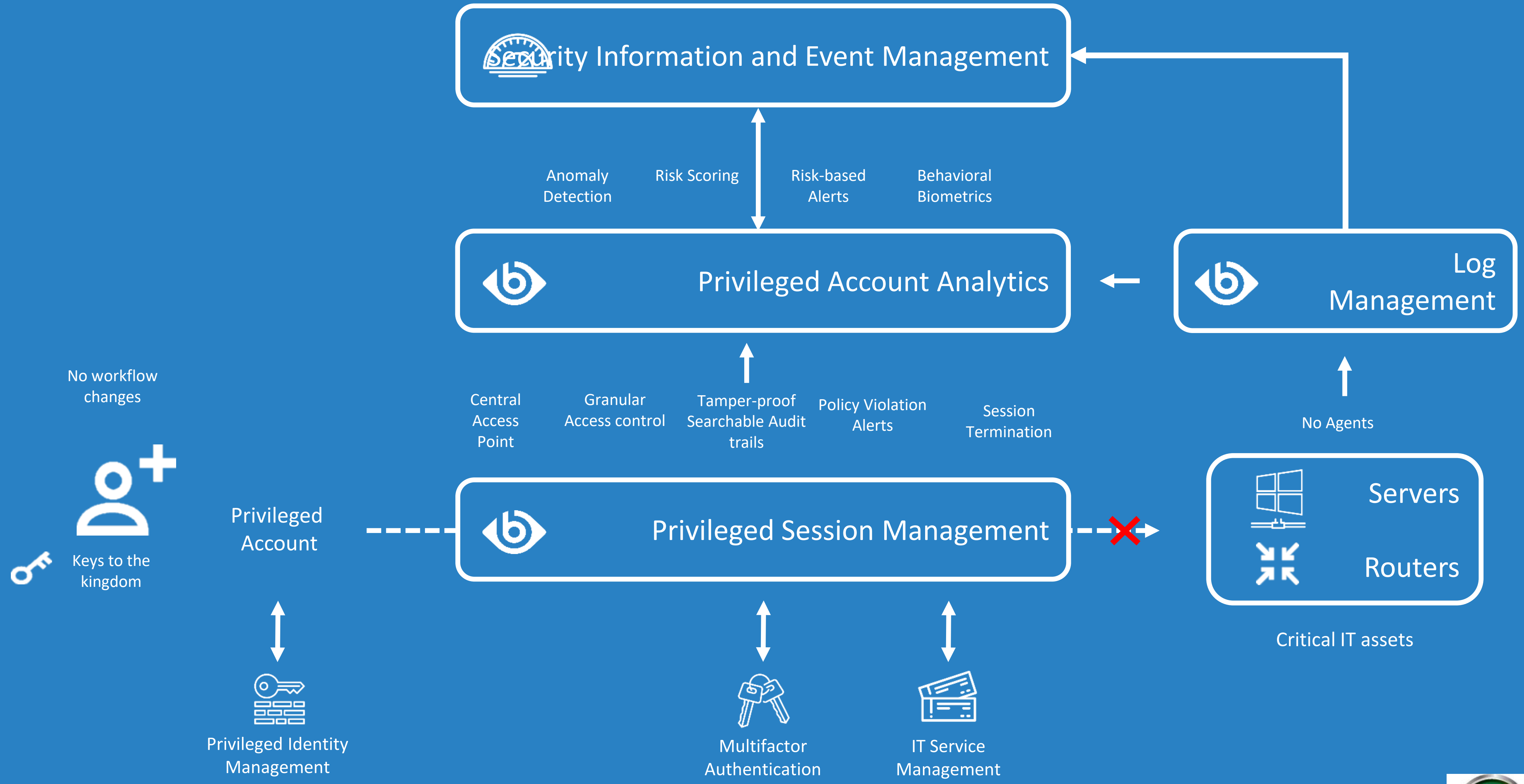
Integration with wide variety of 3rd party system

- SIEM
Splunk, ArcSight, QRadar, ...
- MFA, Identity Management
- Password Management
- Workflow Management

Faster Incident Response

- Fastest deployment time
- No change to workflows
- Detailed reports
- Extra metadata

HOW BALABIT PROVIDES DEFENSE IN DEPTH



BALABIT

THANK YOU
QUESTIONS?

DTASIA
Security with Confidence