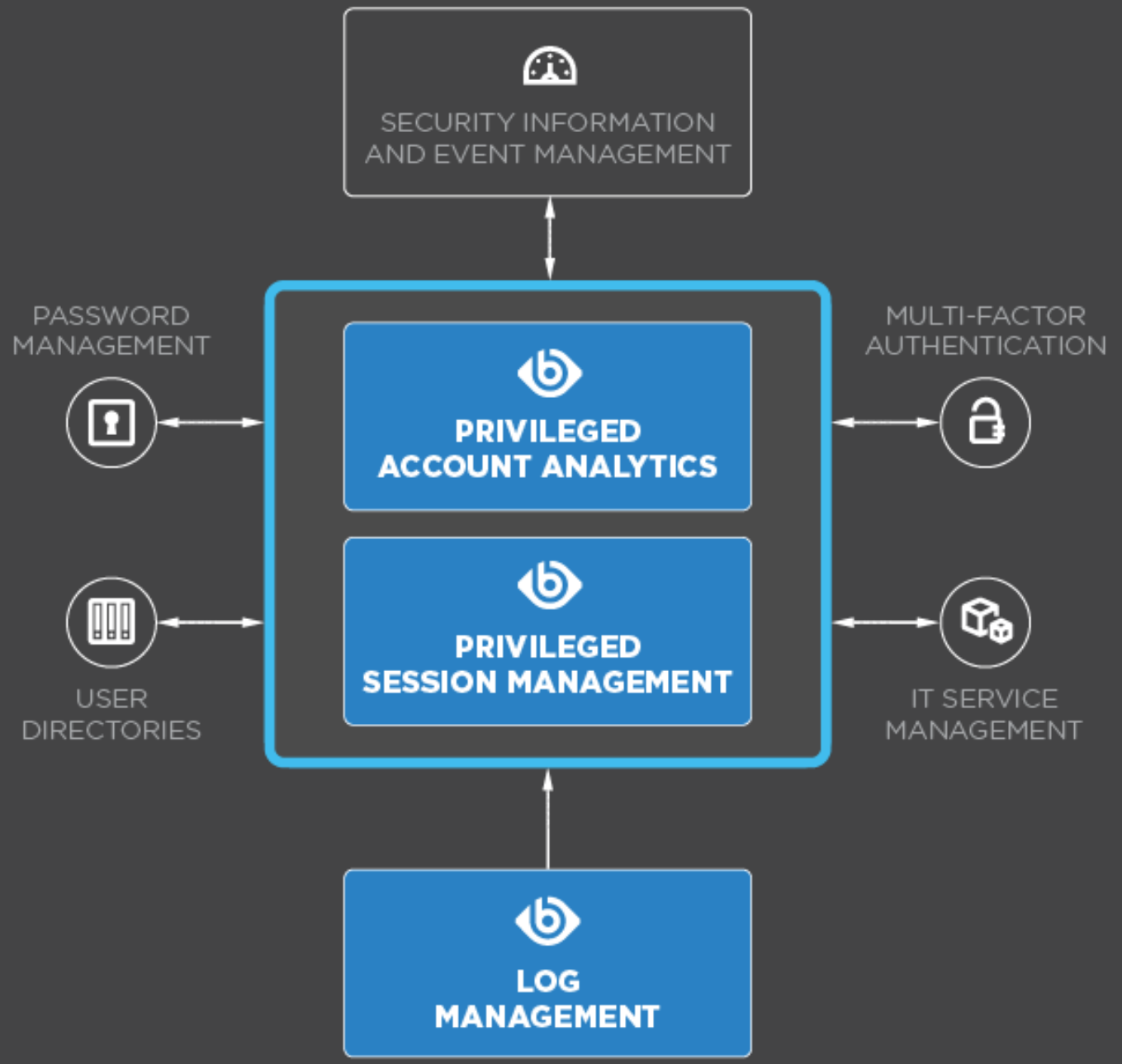
BALABIT

REDEFINING PRIVILEGED ACCESS MANAGEMENT

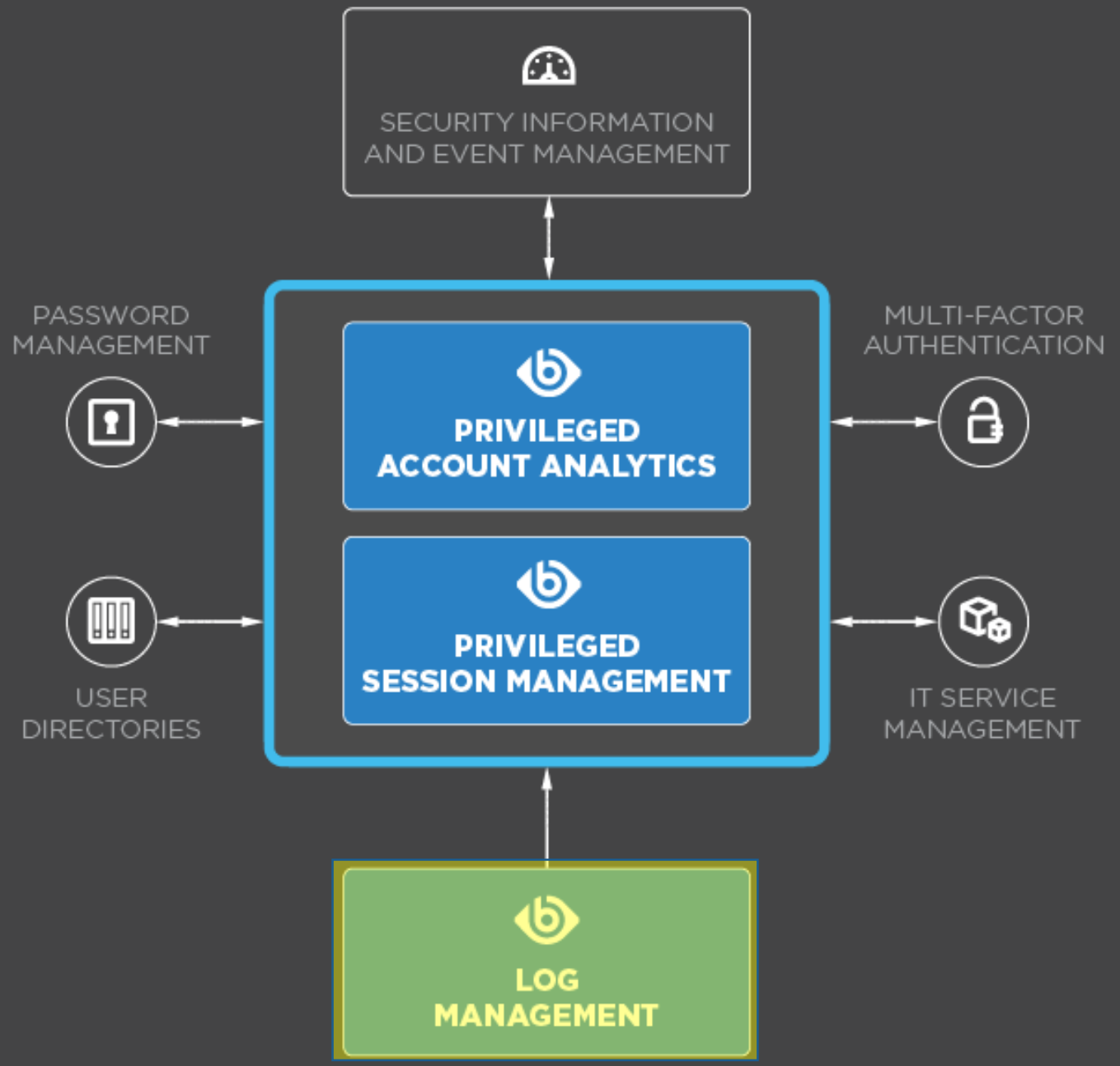
Defense in Depth

Péter SOPRONI | Pre-Sales Engineer | peter.soproni@balabit.com

BALABIT PRIVILEGED ACCESS MANAGEMENT



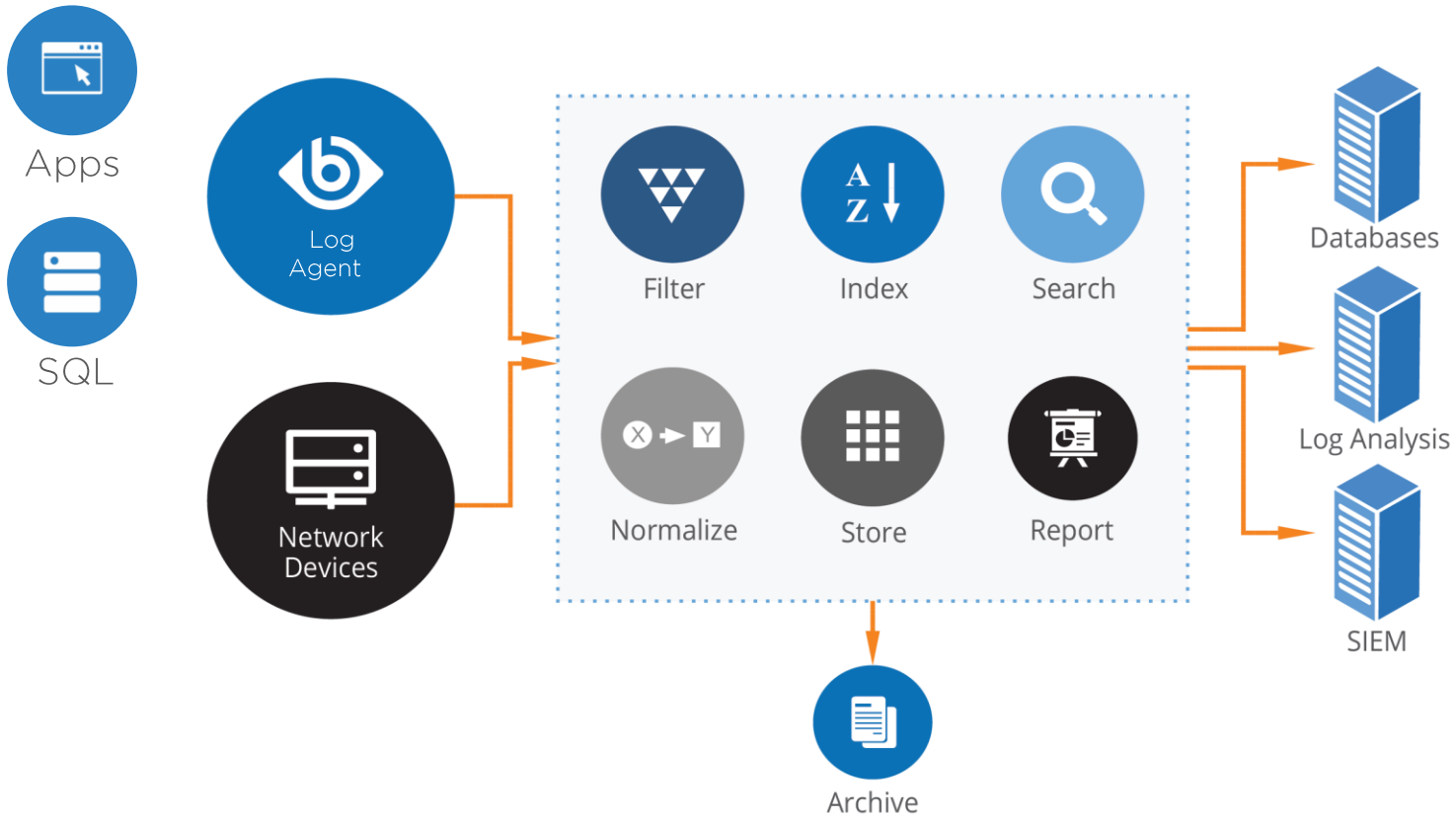
BALABIT PRIVILEGED ACCESS MANAGEMENT



SYSLOG-NG PRODUCT LINE

Widely adopted log management solution

Collects
Filters
Classifies
Normalizes
Centralizes



SYSLOG-NG PRODUCT LINE

SYSLOG-NG OSE

POPULAR

GLOBALLY

RECOGNIZED

ACTIVE COMMUNITY

SYSLOG-NG PE

ENTERPRISE GRADE

FEATURES

PROFESSIONAL

SUPPORT

SYSLOG-NG STORE BOX

TURNKEY APPLIANCE

WEB GUI

INDEXING, REPORTING

ALERTS

Use-case #1:
Platform Agnostic Log Management

Challenges:

Variety of sources & schema

Multiple destinations

Delivery guarantee

Fault-tolerance

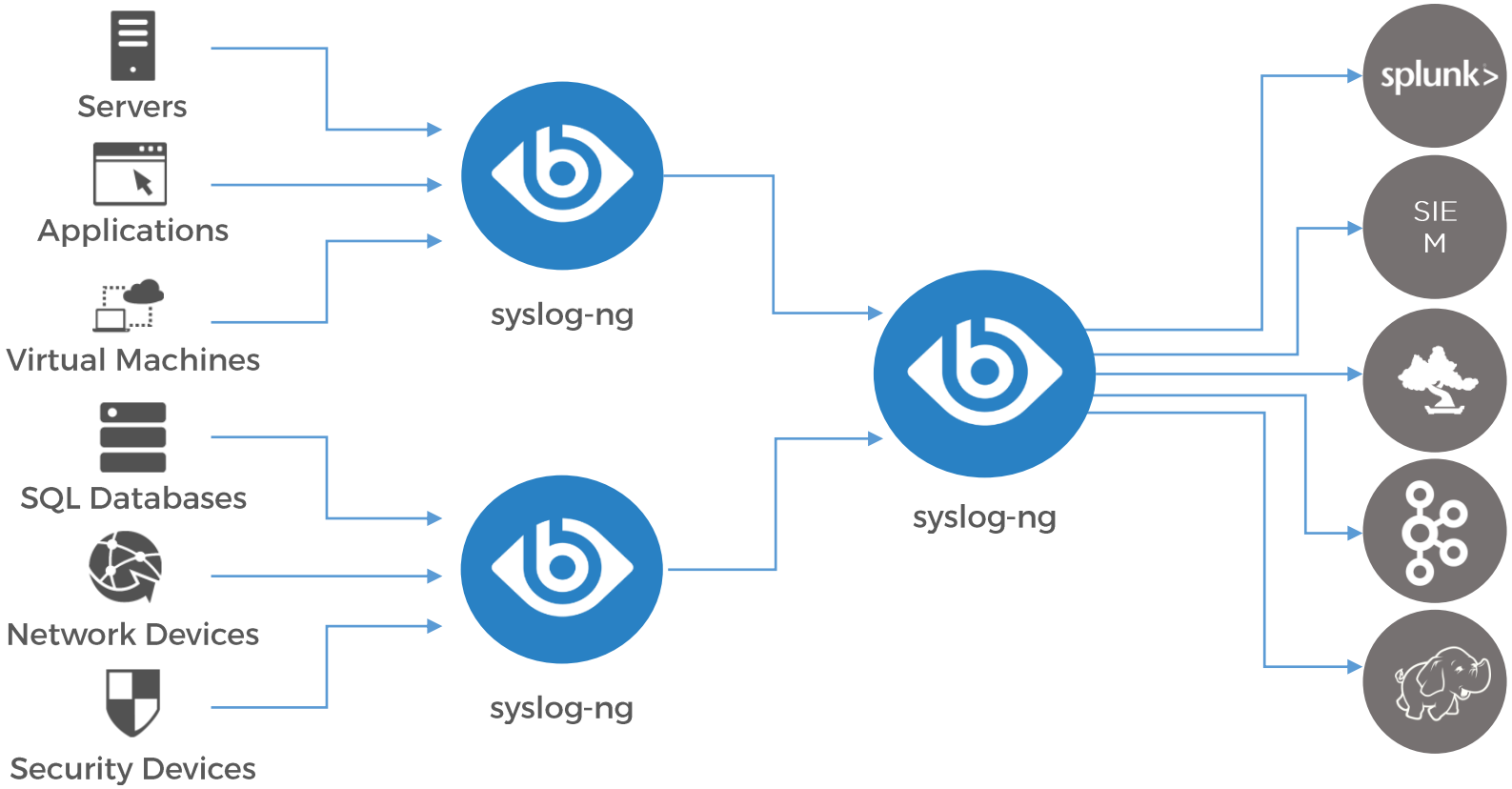
End-goals:

Unified collection

Real-time transformation

Secure transit

Buffering / caching



BALABIT

Use-case #2: Long-term storage & search

Challenges:

Usage based licensing

Storage costs

Varying retention requirements

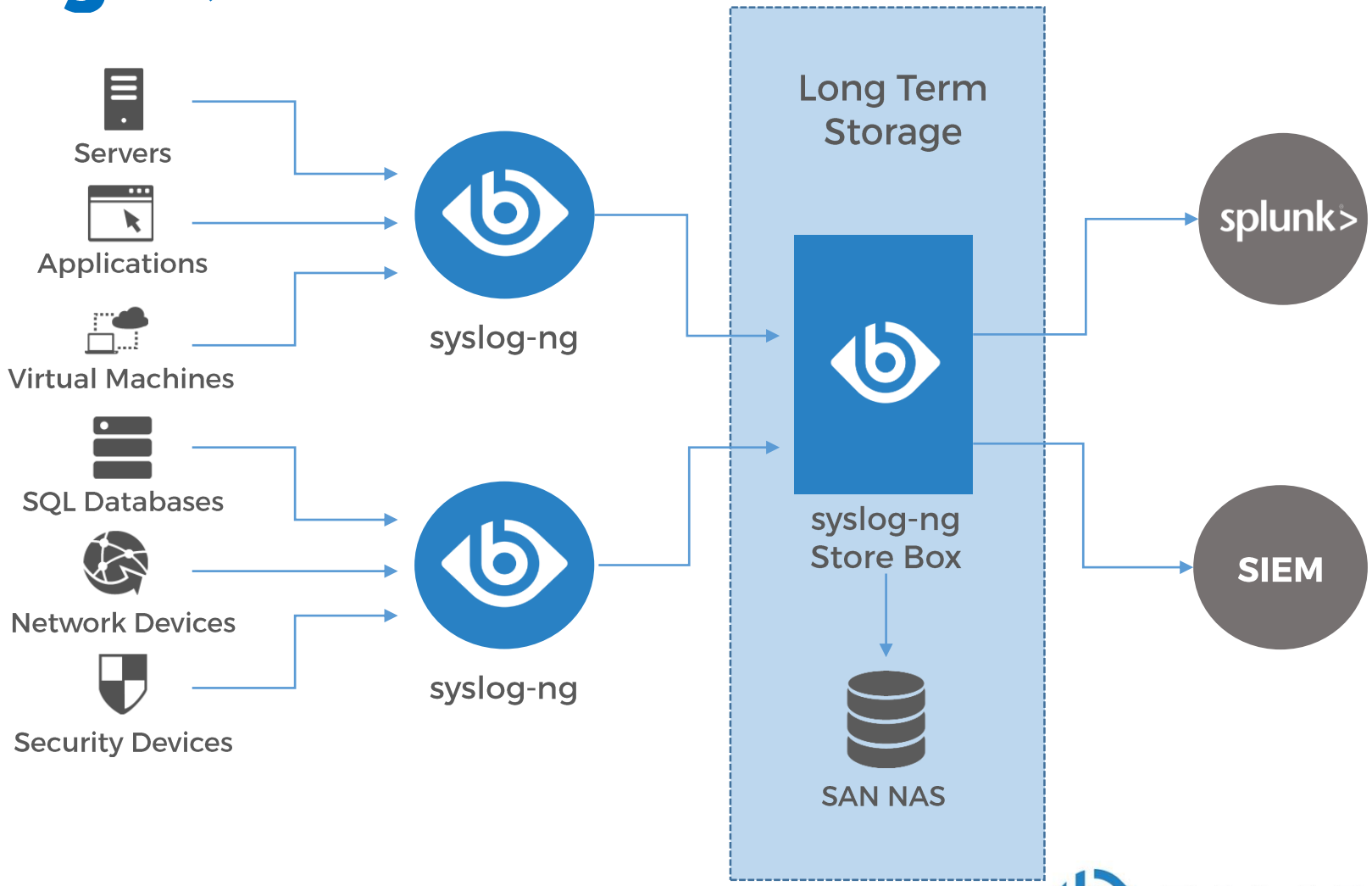
End-goals:

Implement long-term storage layer

Automated retention policies

Automated archiving

Indexed & compressed



BALABIT

Use-case #3: Advanced routing / filtering

Challenges:

Varying EPS

Usage-based licensing

Usage-based planning

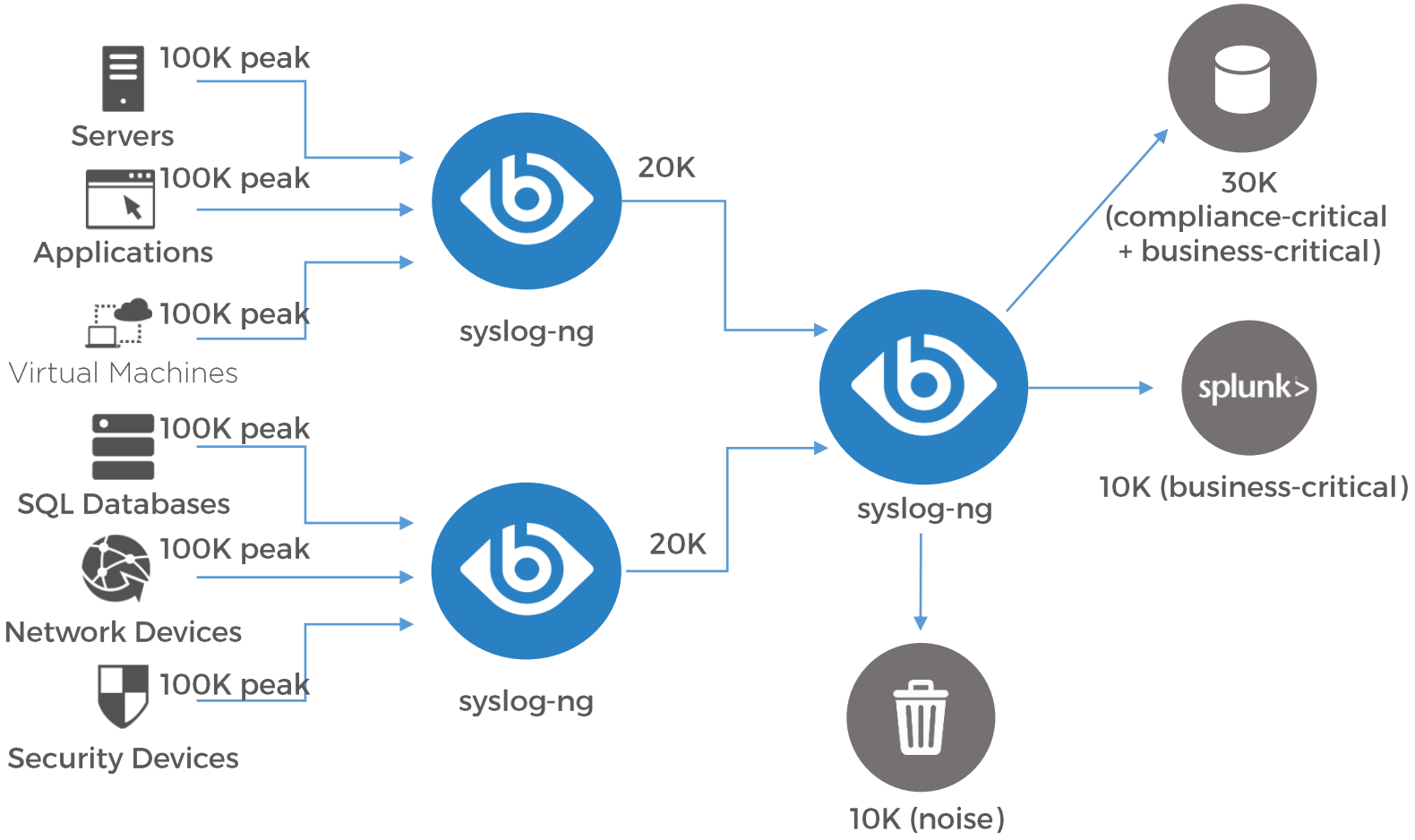
Cost implications

Solution:

Filter out irrelevant data

Asset-based planning

Cost-effective Retention



Note: EPS - Events-per-second

BALABIT

Use-case #4: Compliance, even without a SIEM

Challenges:

Unsorted, mixed content

Too noisy for correlation

Mixed compliance models

Unfiltered data exposed

End-goals:

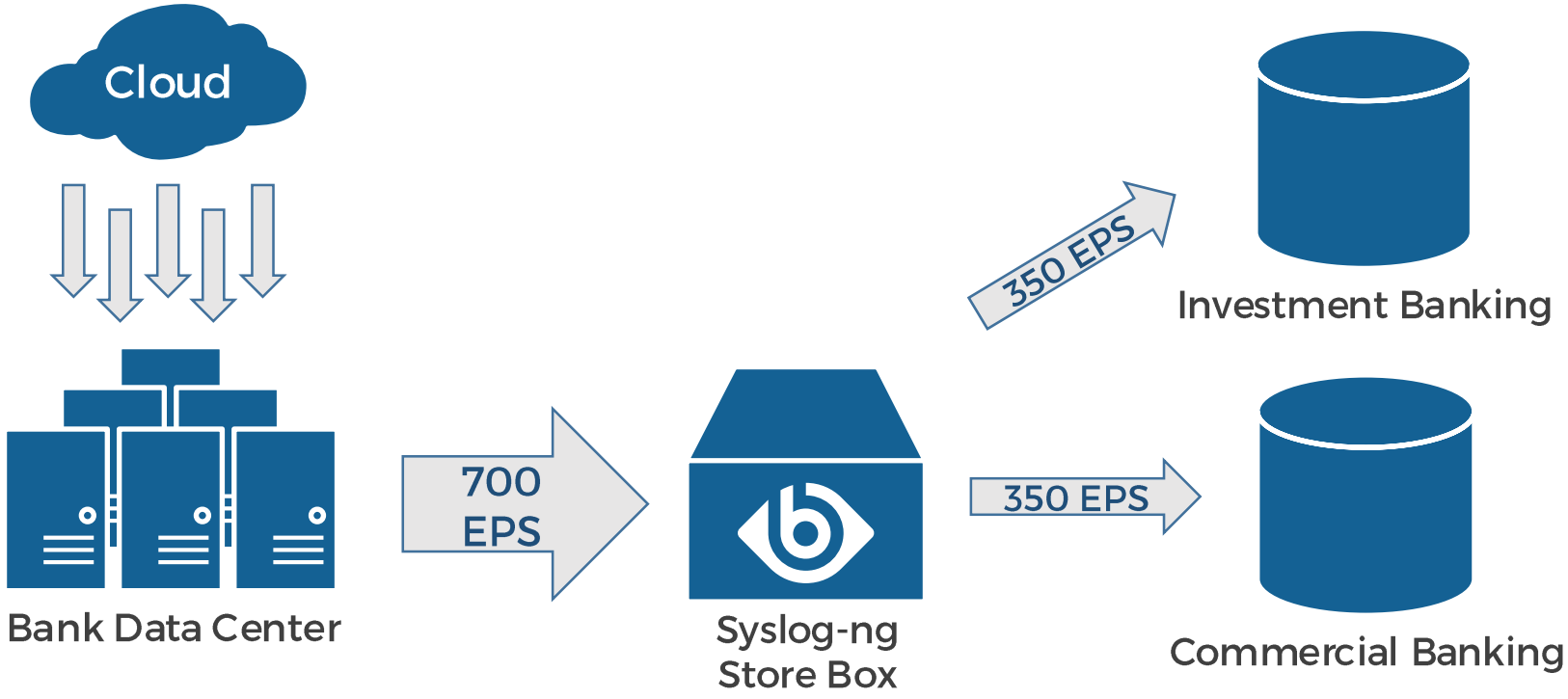
Logically separate content

Data can be filtered further

Different archiving policies

Repository access controls

User-specific log “views”



BALABIT

Use-case #5: Reliable Log Infrastructure

Challenges:

Critical event, logs never sent

Connection saturation

Single-point of failure

Data open to inspection

Solution:

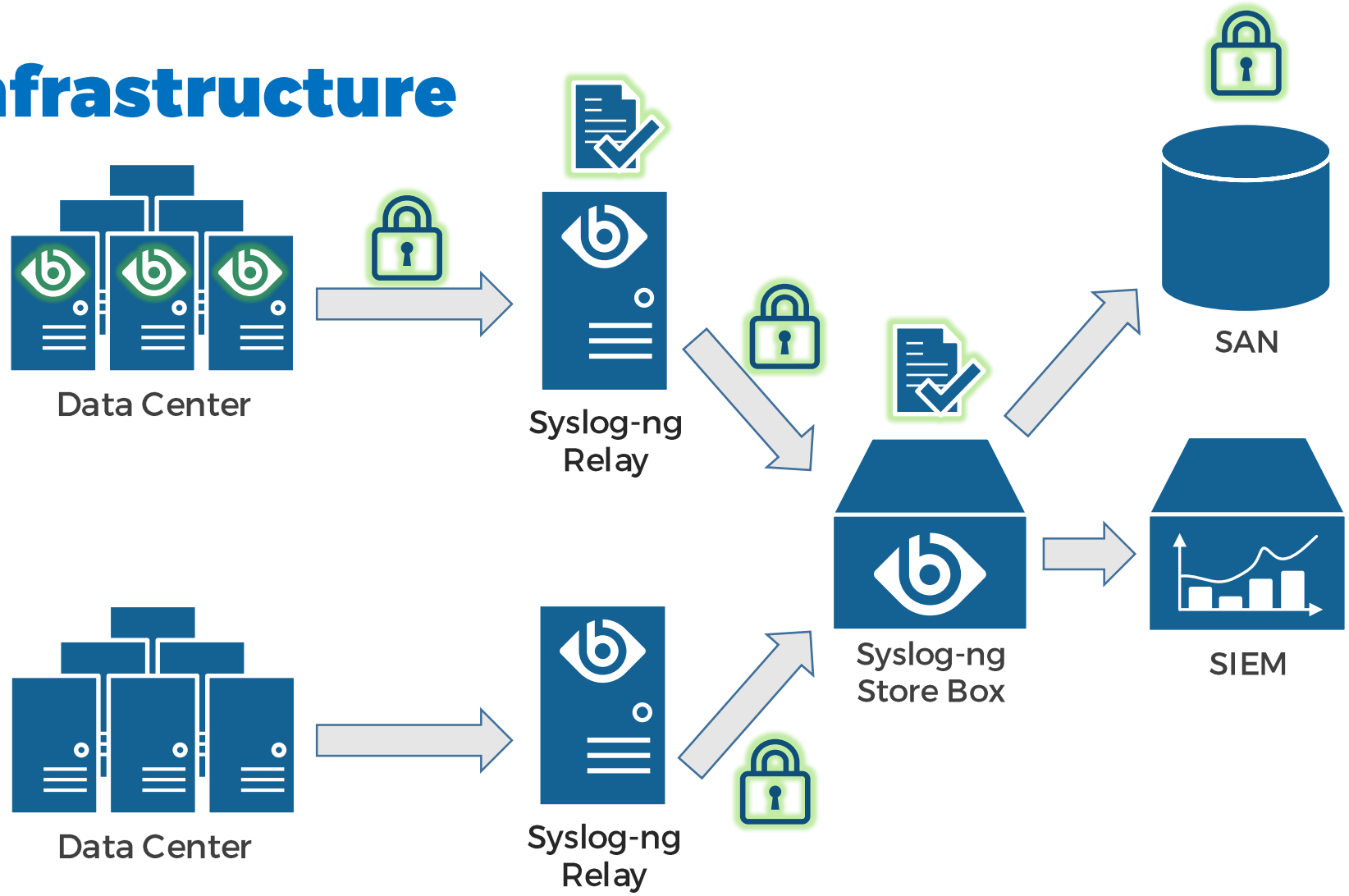
Relays as a local staging post

Consolidate, cache & buffer

Alternate destinations

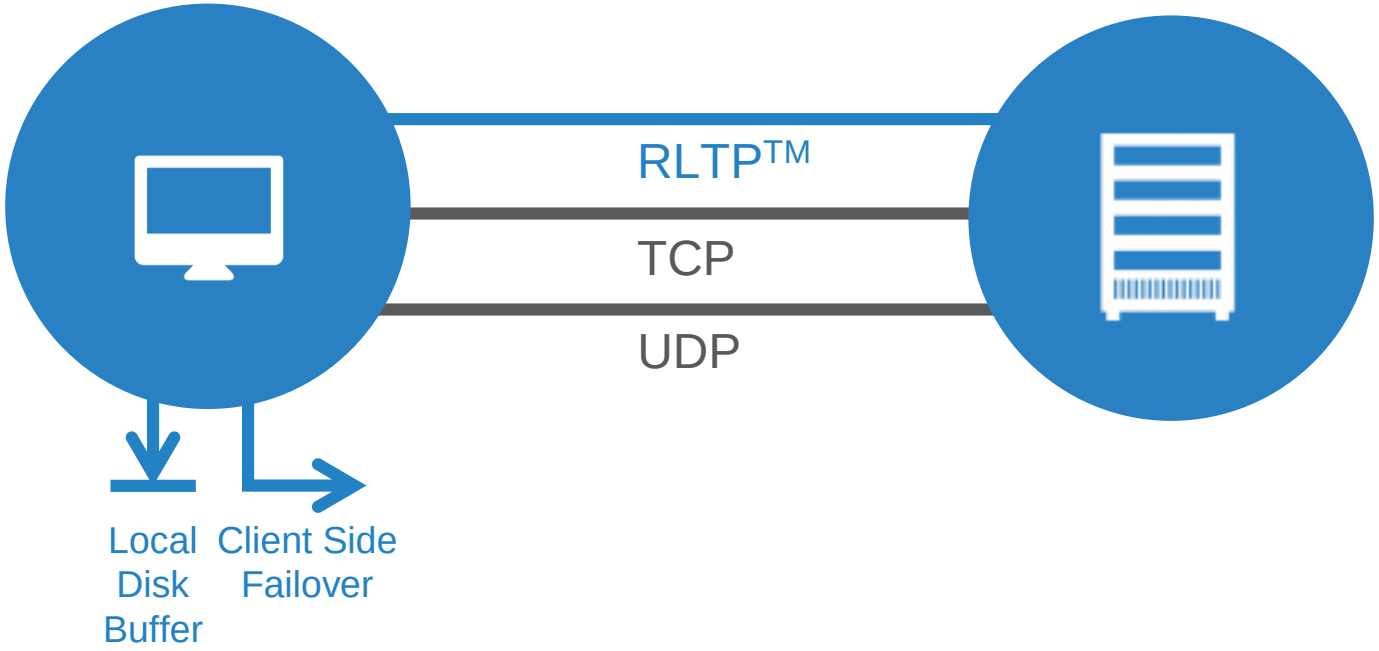
RLTP: received & understood

Encryption & timestamping



BALABIT

RELIABLE LOG TRANSFER



Makes Log Data Complete

BALABIT

STRONG ENCRYPTION

Data in motion

TLS encryption

Mutual authentication
X.509 certificates

Data at rest

Logstore™

Encrypted, Time-stamped,
Compressed
binary files

Makes Log Data Secure

BALABIT

SYSLOG-NG STORE BOX DESCRIPTION

Turnkey solution
Physical / Virtual Appliance

High performance indexing
100,000 logs/sec sustained
35 GB/hr

Web- Based Intuitive GUI
Visualization Statistics

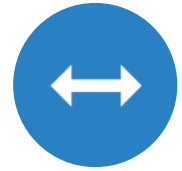
Full text search

Reports

Automated Archiving
Raw storage: 1TB - 10 TB

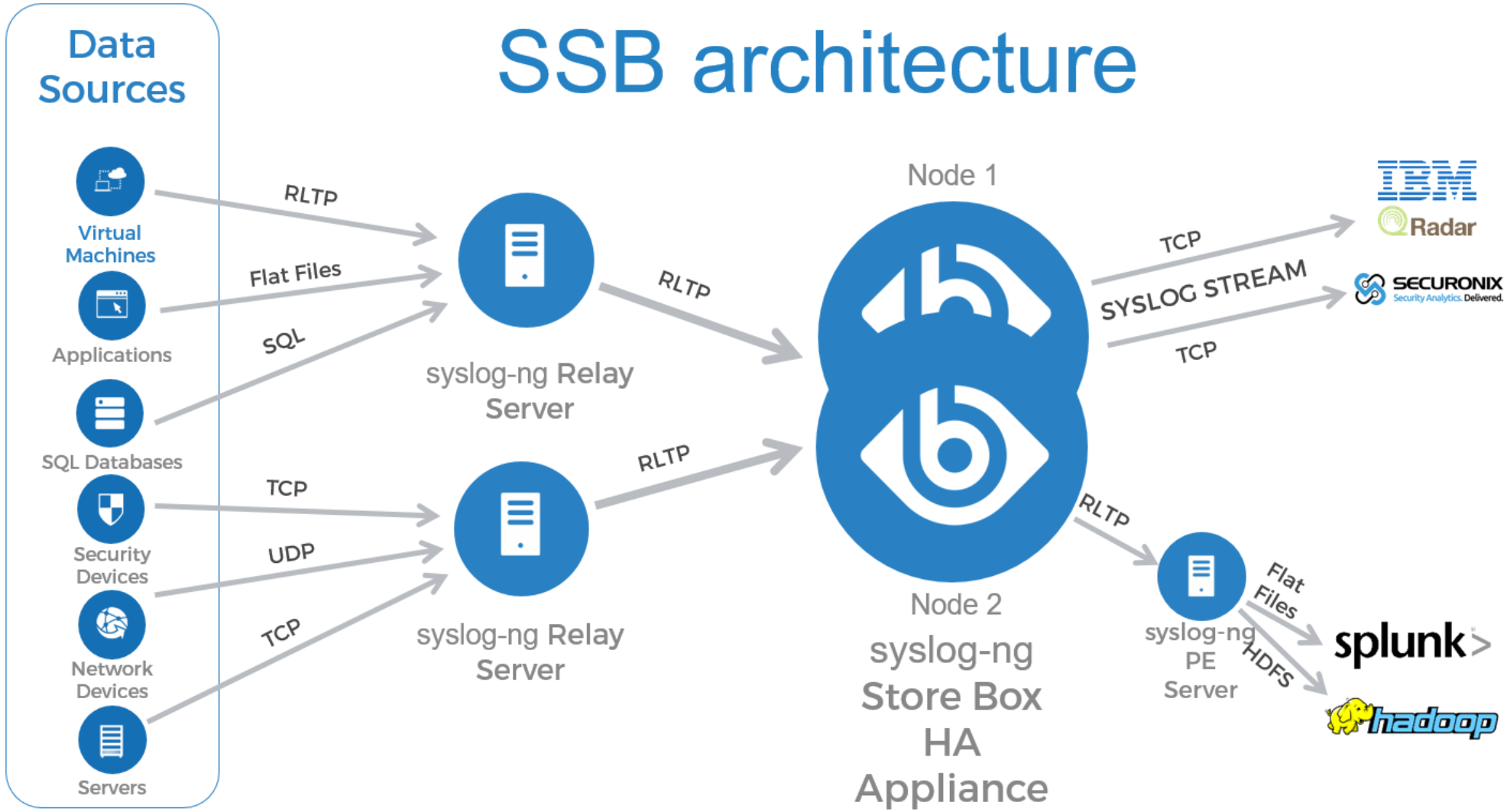
Granular access control
LDAP/Radius Integration

RESTful API

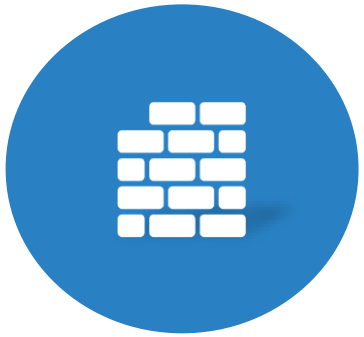


BALABIT

SSB architecture



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

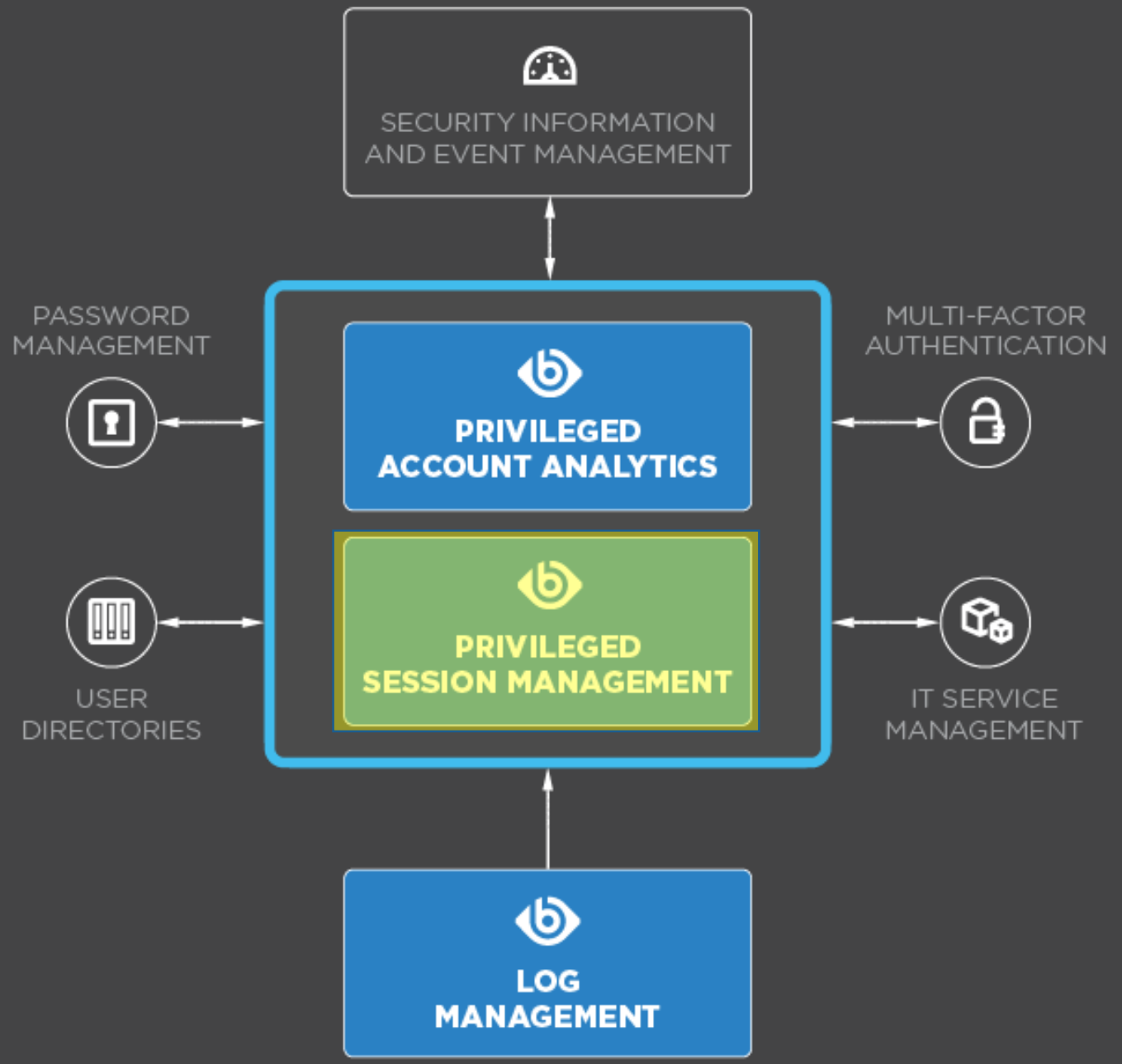
Admins (or attackers) can delete the logs!

PASSWORD MANAGERS

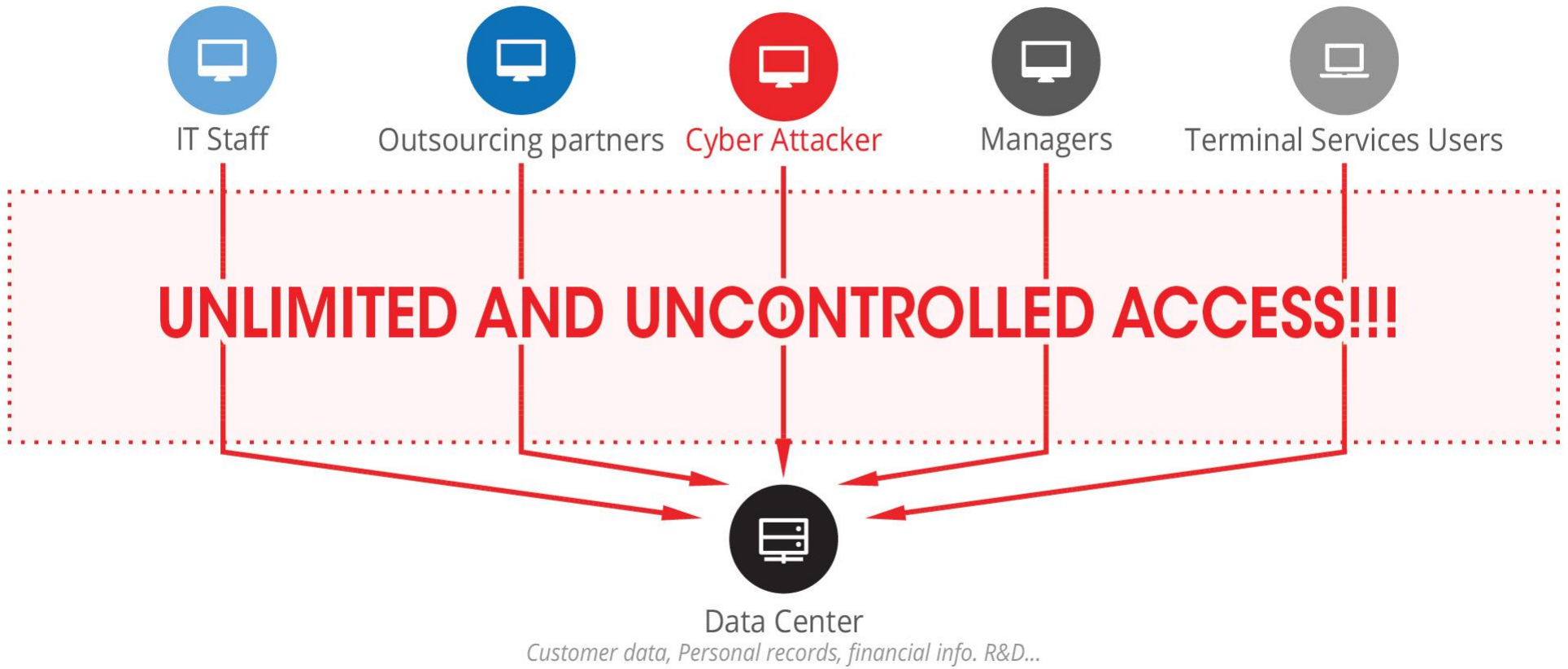
Complex and costly systems

No answer to „who did what?”

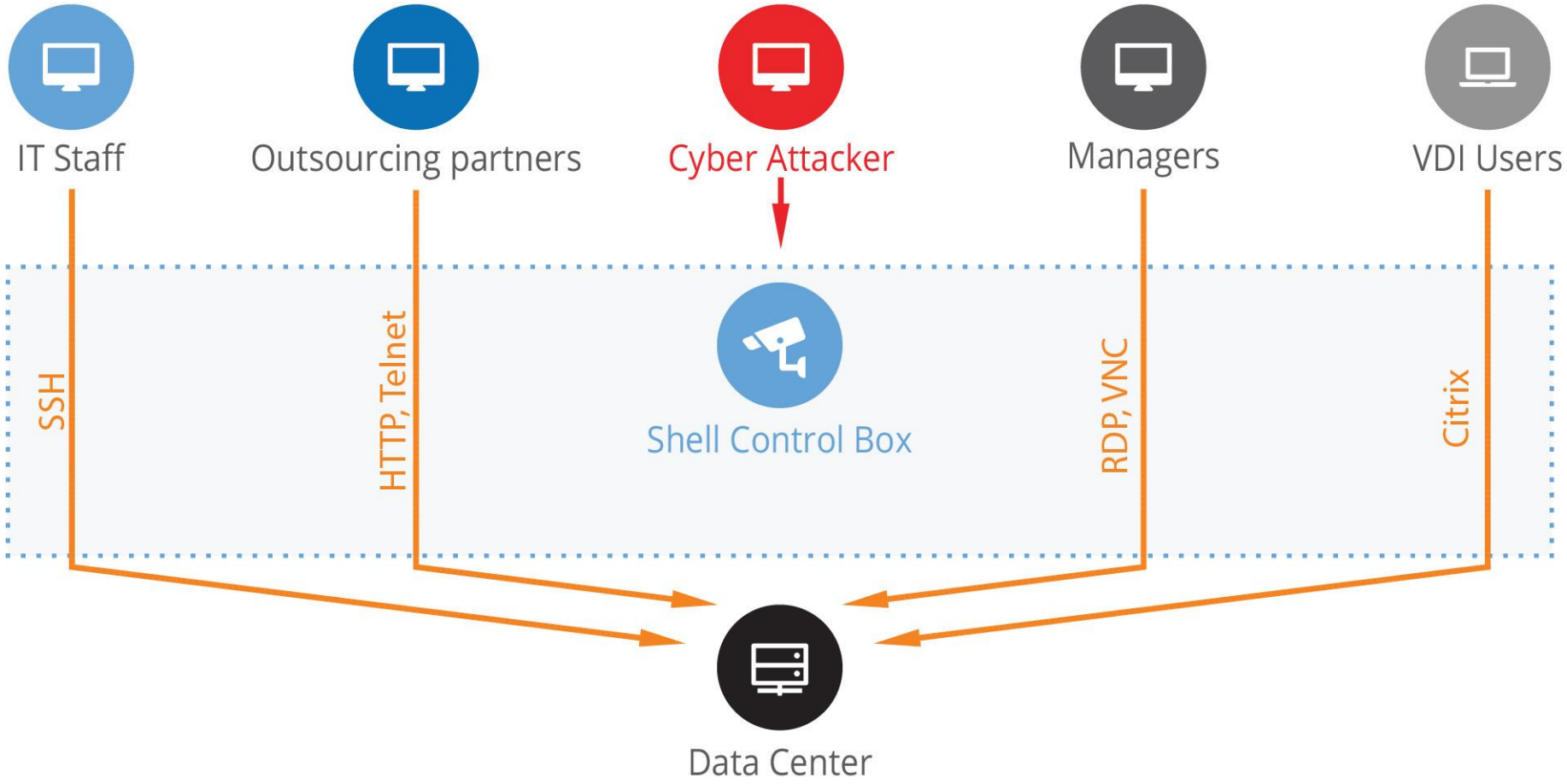
BALABIT PRIVILEGED ACCESS MANAGEMENT



UNFETTERED ACCESS OF PRIVILEGED USERS...

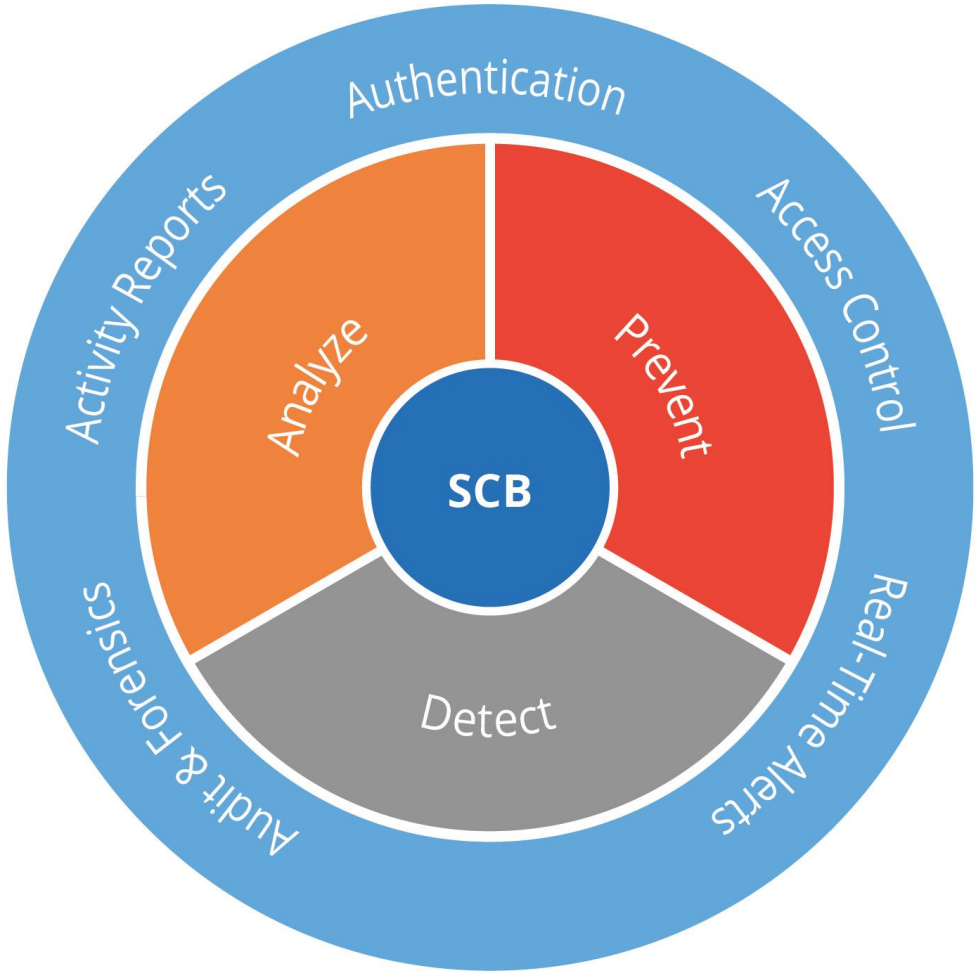


TURNKEY, INDEPENDENT AND TRANSPARENT AUDITING



BALABIT

PRIVILEGED SESSION MANAGEMENT



EASY DEPLOYMENT:

- Widest platform coverage
- Transparent & Independent

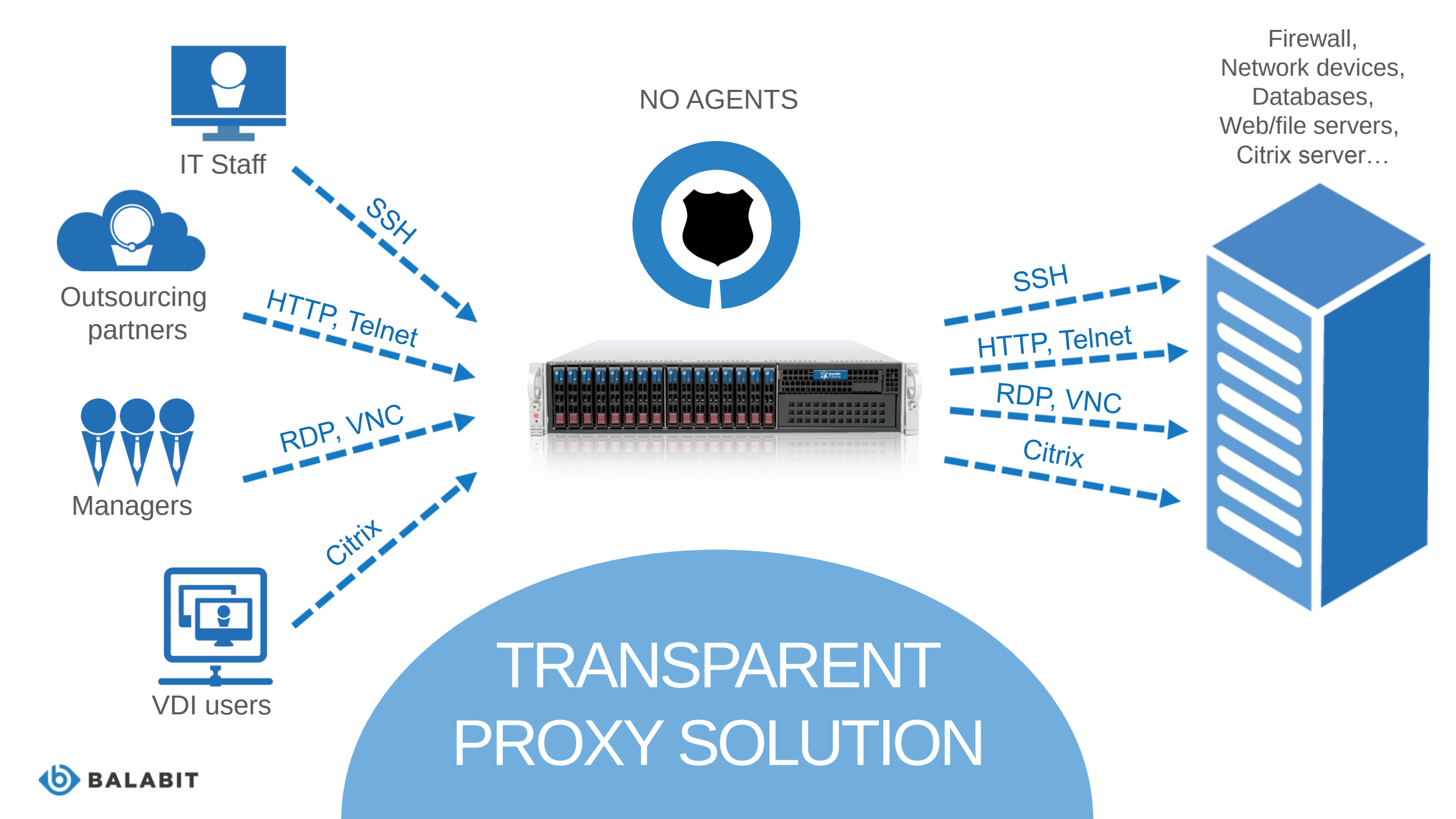
GRANULAR ACCESS CONTROL & PREVENTION:

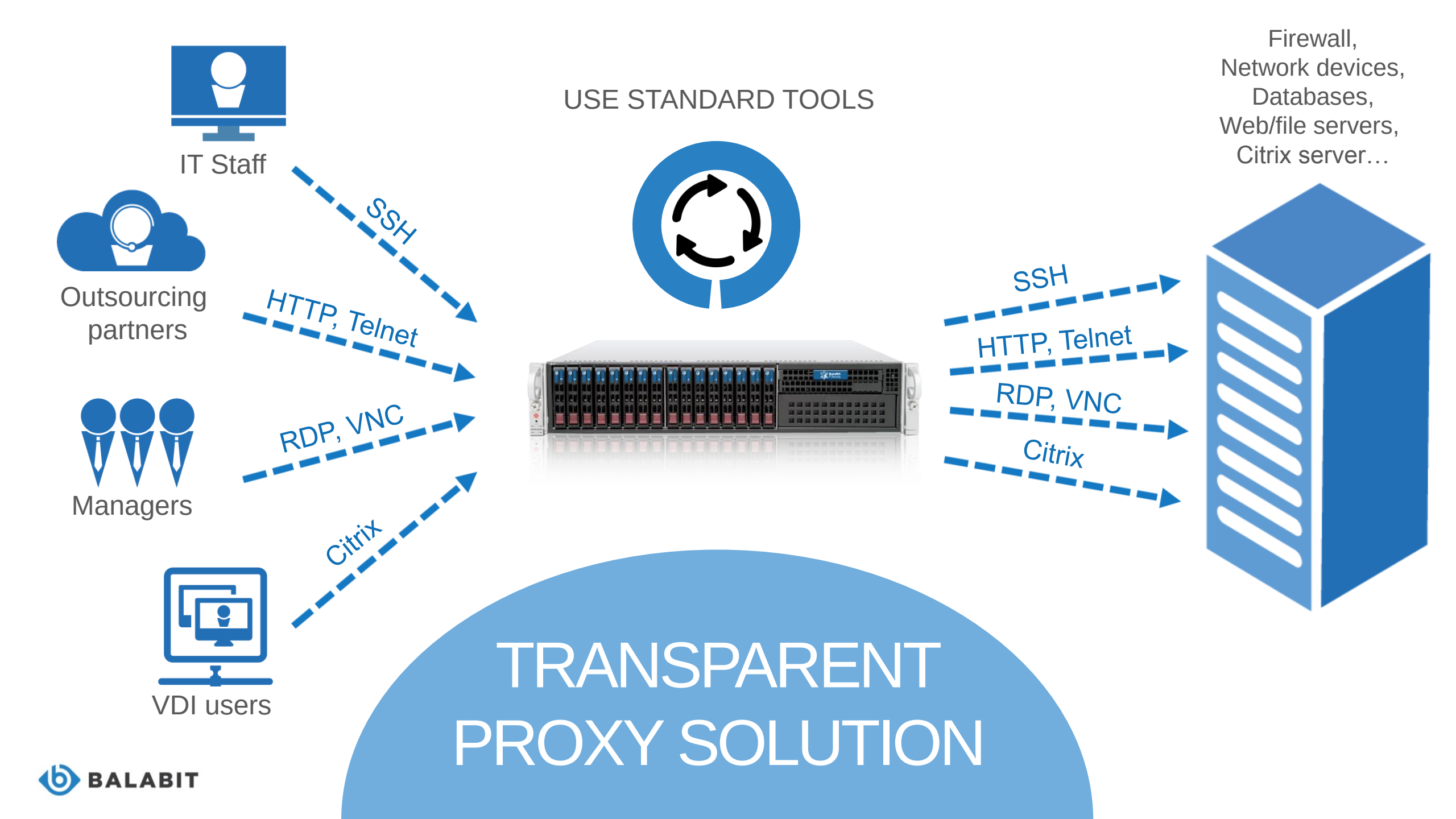
- User directory integration
- Strong authentication & Auto-Logon
- Channel control
- File-transfer control
- 4-eyes authorization
- Real-time blocking of harmful actions

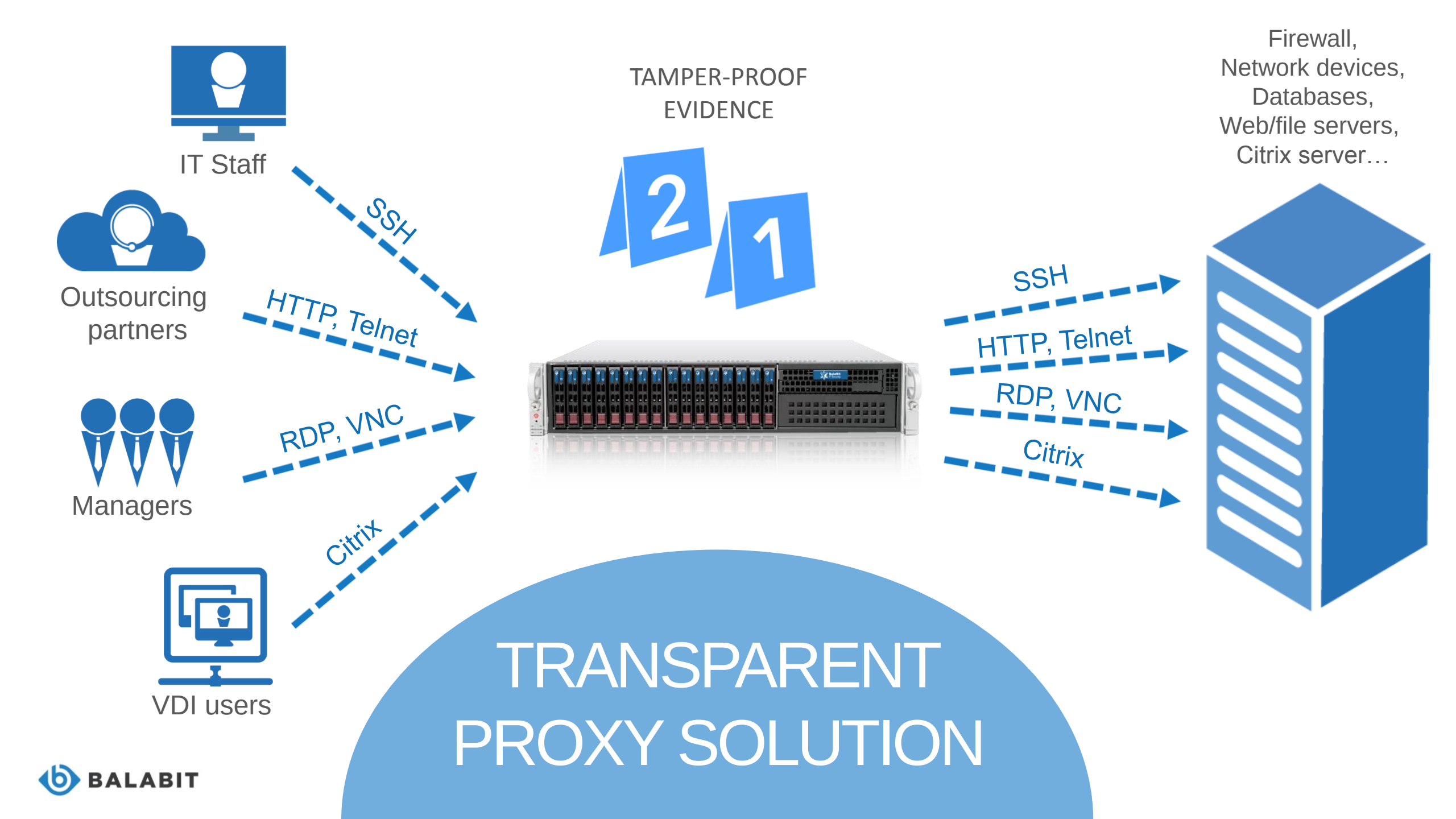
QUALITY AUDIT & REPORTING:

- Fast, free-text search in audit trails
- Movie-like playback
- Tamper-proof audit data
- Alerting to email or SIEM
- Augmented log data & Compliance reports

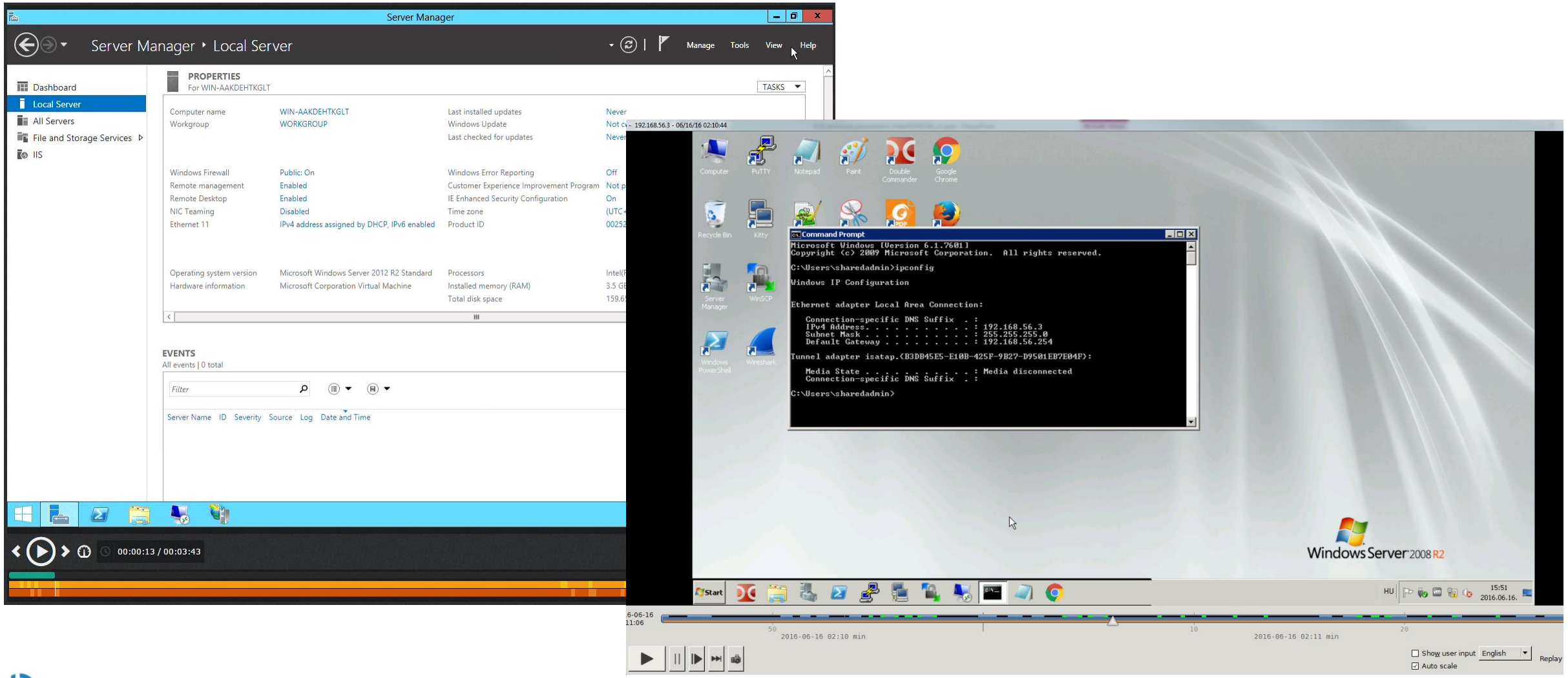
BALABIT


IT Staff
Outsourcing partners
Managers
VDI users
SSH
HTTP, Telnet
RDP, VNC
Citrix
NO AGENTS
SSH
HTTP, Telnet
RDP, VNC
Citrix
Firewall,
Network devices,
Databases,
Web/file servers,
Citrix server…
TRANSPARENT
PROXY SOLUTION
BALABIT


IT Staff
Outsourcing partners
Managers
VDI users
SSH
HTTP, Telnet
RDP, VNC
Citrix
USE STANDARD TOOLS
SSH
HTTP, Telnet
RDP, VNC
Citrix
Firewall,
Network devices,
Databases,
Web/file servers,
Citrix server…
TRANSPARENT
PROXY SOLUTION
BALABIT

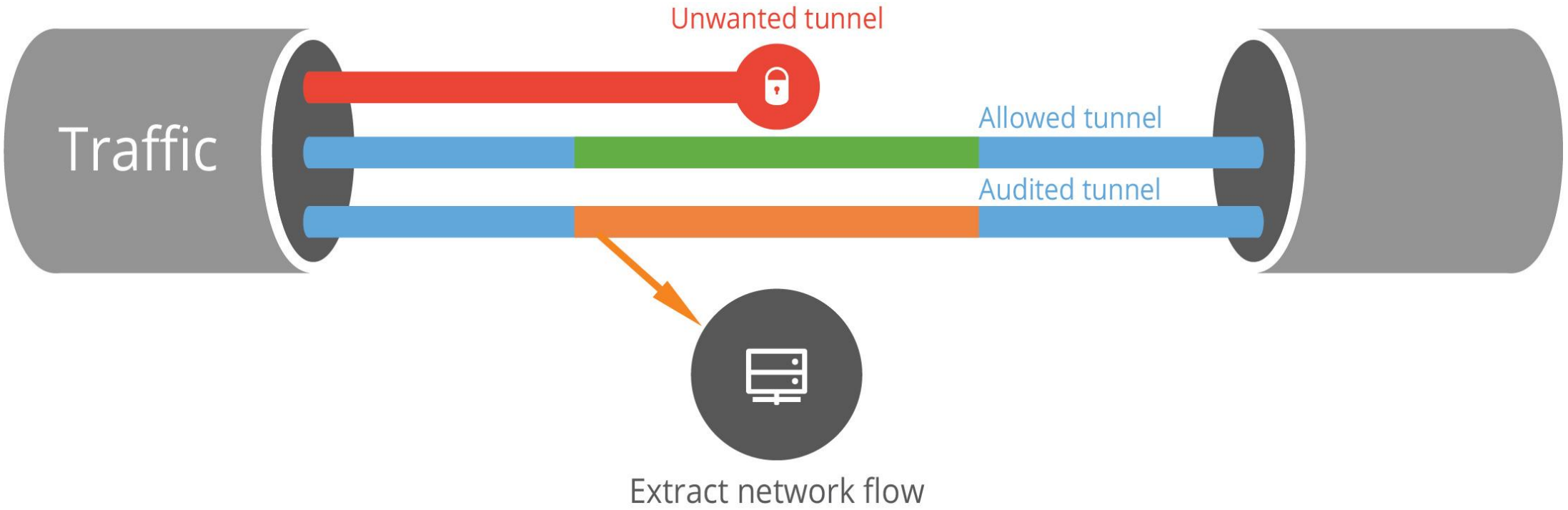

IT Staff
Outsourcing partners
Managers
VDI users
SSH
HTTP, Telnet
RDP, VNC
Citrix
TAMPER-PROOF EVIDENCE
2
1
SSH
HTTP, Telnet
RDP, VNC
Citrix
Firewall,
Network devices,
Databases,
Web/file servers,
Citrix server…
TRANSPARENT PROXY SOLUTION
BALABIT

HIGH-QUALITY AUDIT TRAILS



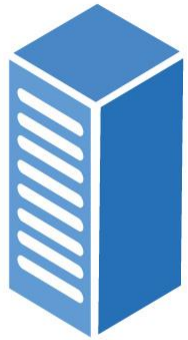
BALABIT

GRANULAR ACCESS CONTROL



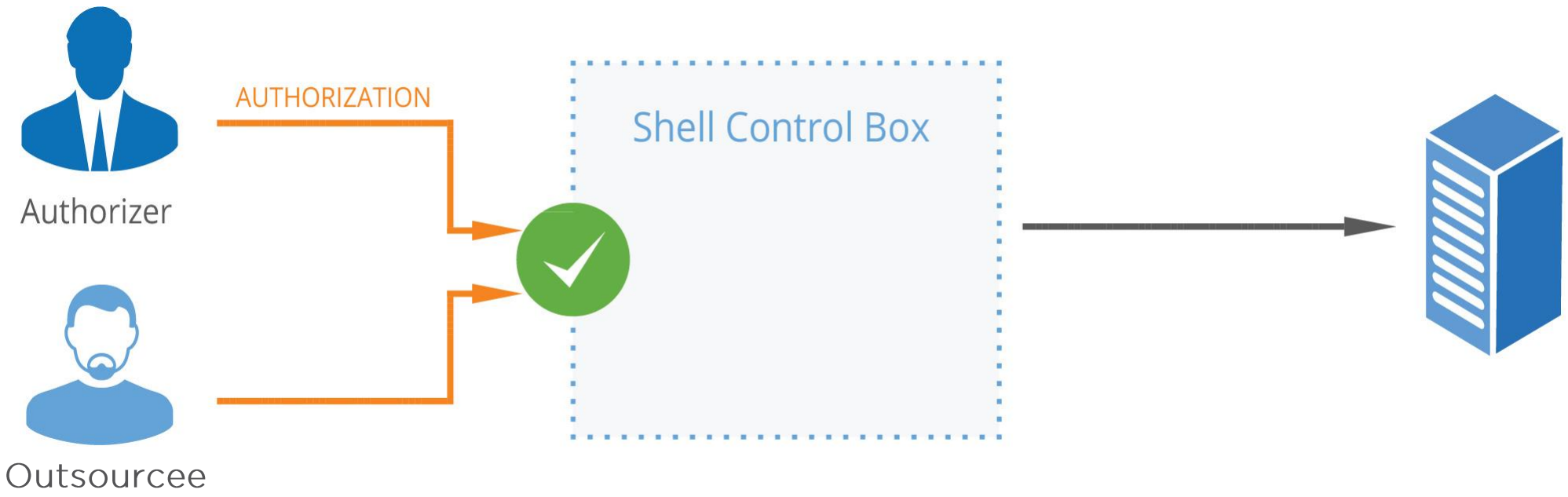
4-EYES AUTHORIZATION & REAL-TIME MONITORING

Outsourcee



4-EYES AUTHORIZATION & REAL-TIME MONITORING

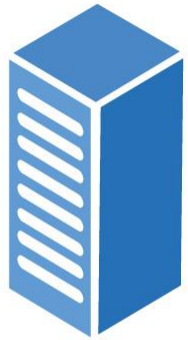
4-EYES AUTHORIZATION & REAL-TIME MONITORING



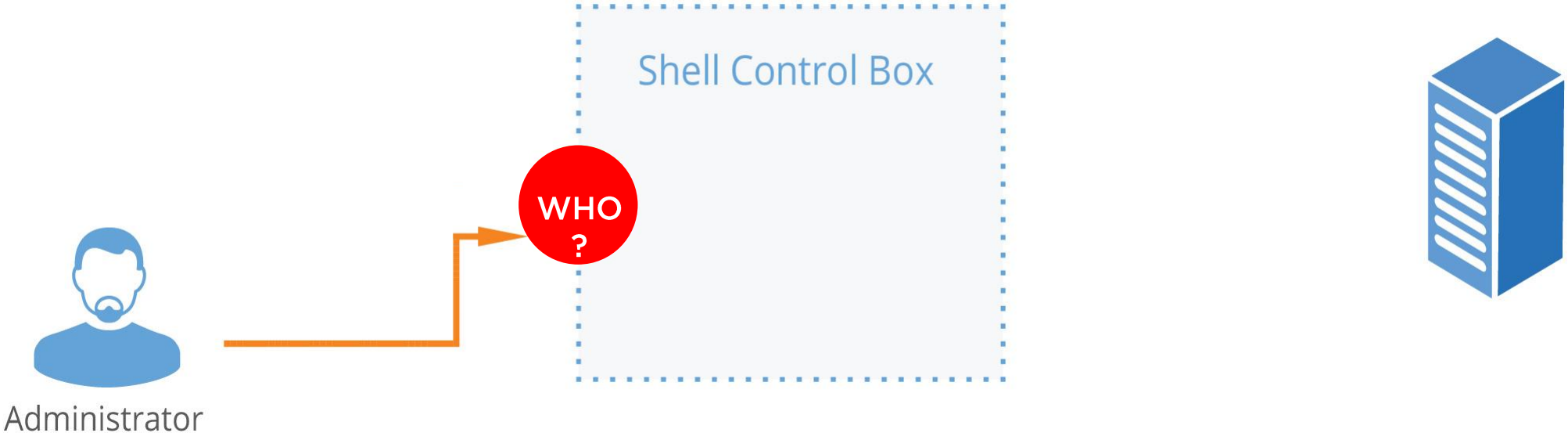
4-EYES AUTHORIZATION & REAL-TIME MONITORING

SHARED ACCOUNT PERSONALIZATION

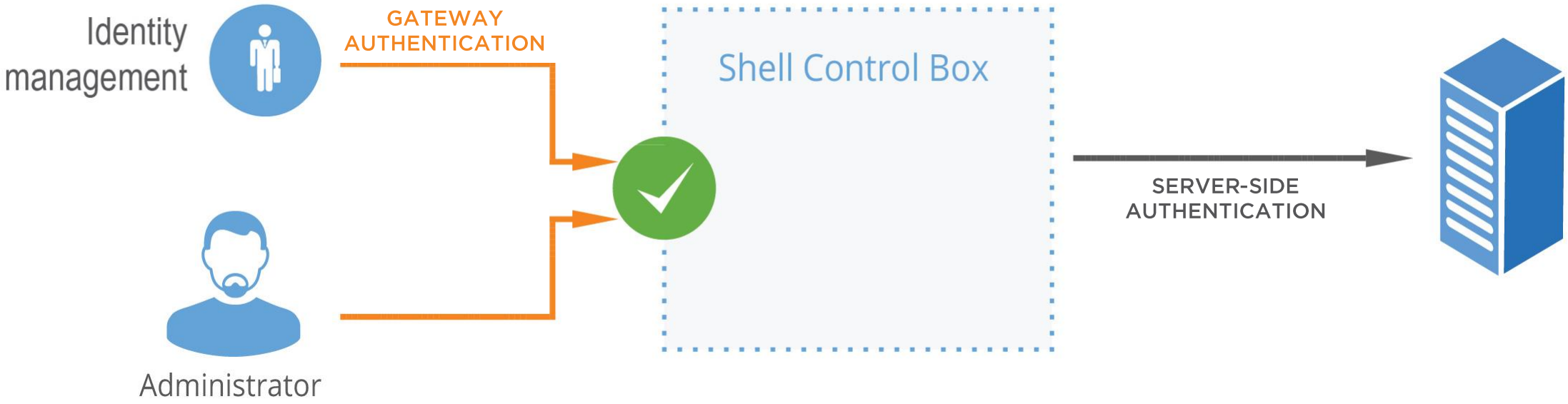
Administrator



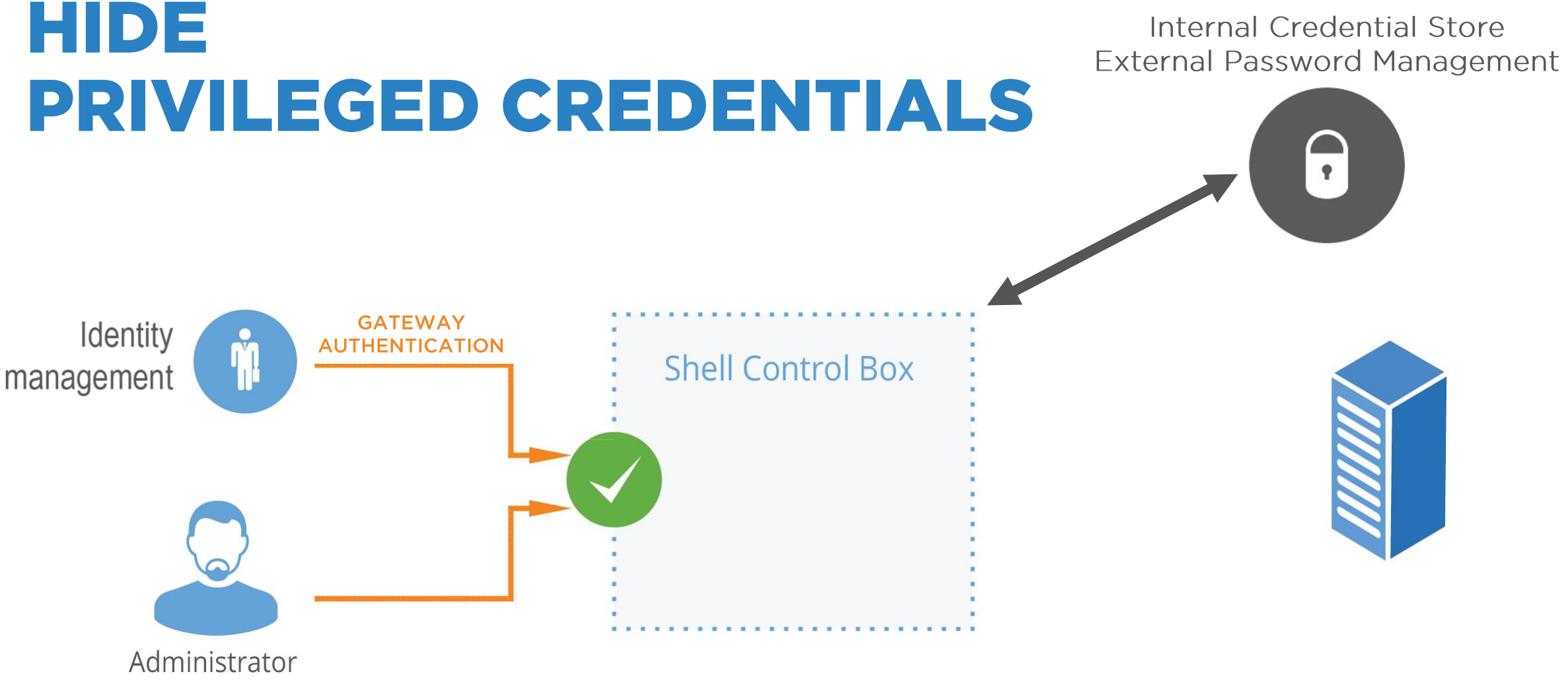
SHARED ACCOUNT PERSONALIZATION



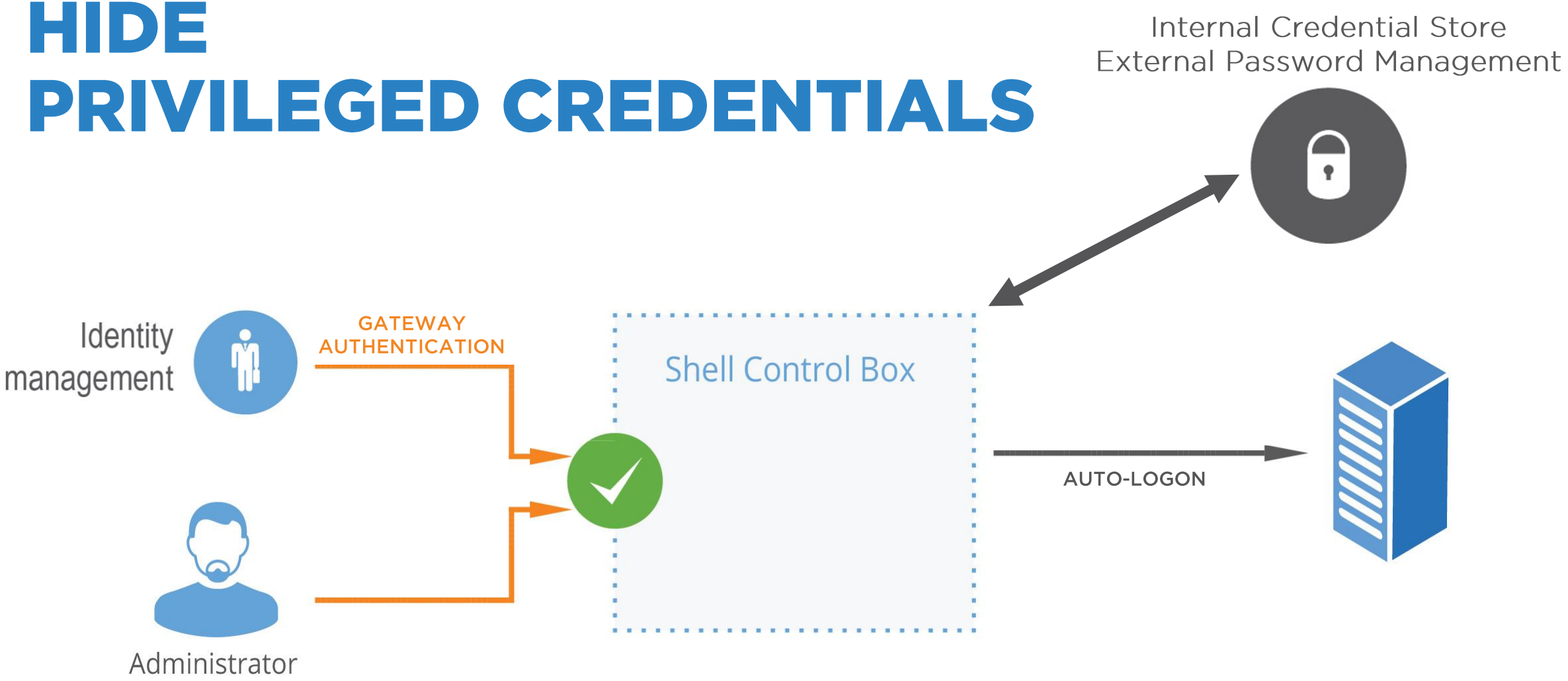
SHARED ACCOUNT PERSONALIZATION



HIDE PRIVILEGED CREDENTIALS



HIDE PRIVILEGED CREDENTIALS

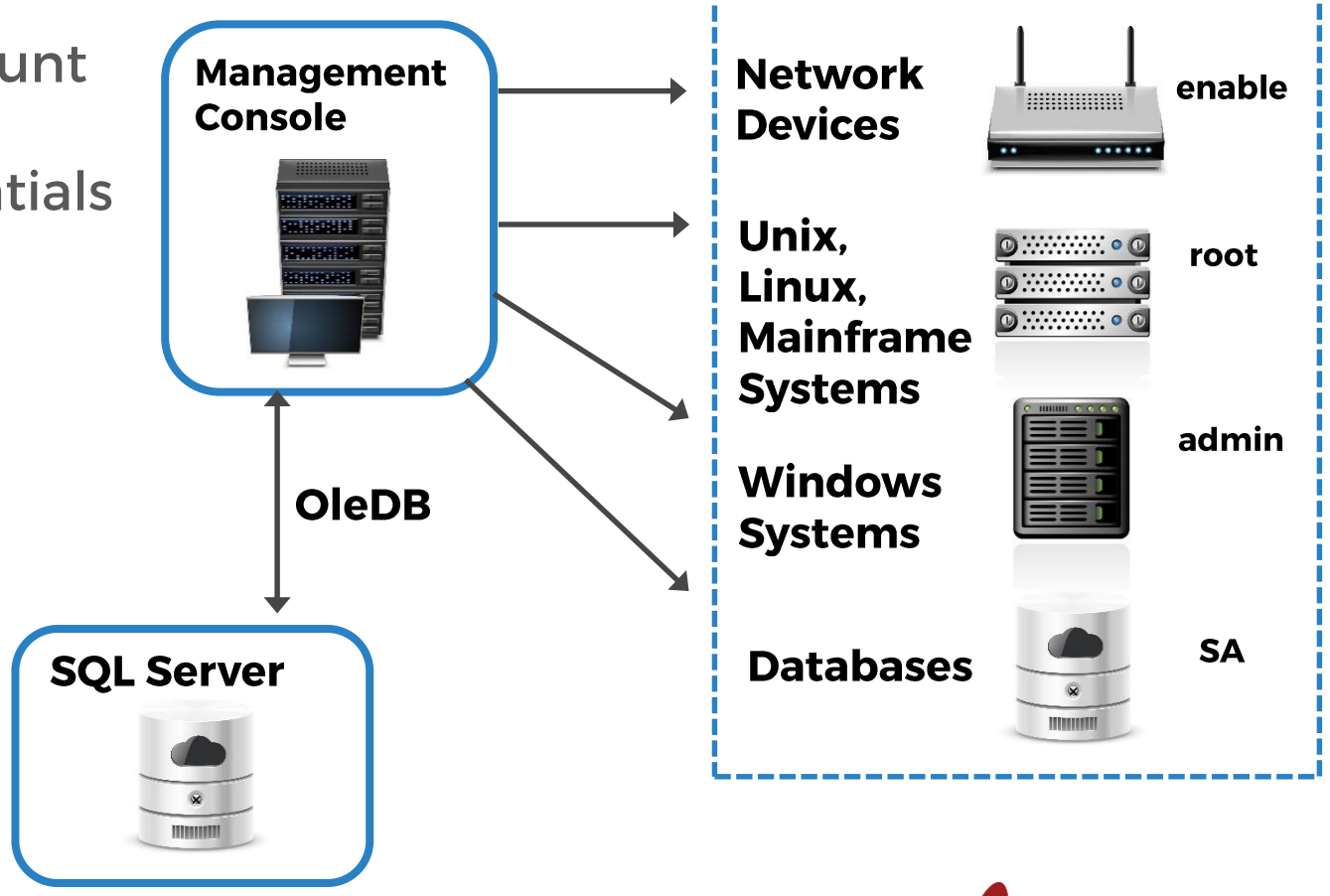


RED IDENTITY MANAGEMENT (ERPM)

PRIVILEGED PASSWORD MANAGEMENT

- Auto-discover systems, accounts, account usage
- Remediate Privileged Account Credentials

Asset	Account	Password
Router	enable	W<g2%$124jnq\ q\
Linux	root	Ab#59bh?M<f9+TTd3
Windows	Admin	,id<94b<LE2=]3&hq23mn 6
Database	SA	a)]$123gjR992

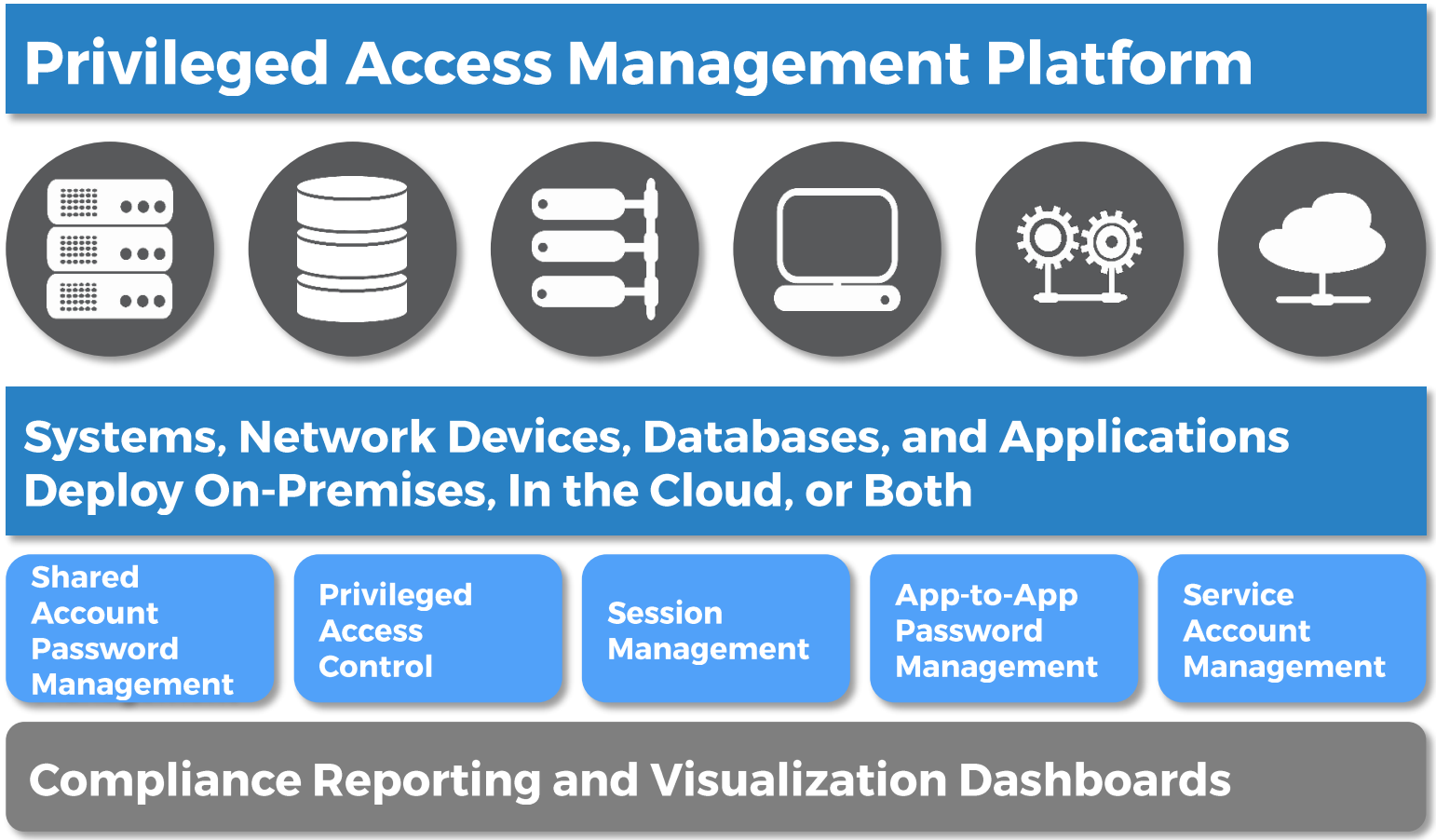


BALABIT

LIEBERMANSOFTWARE

JOINT SOLUTION

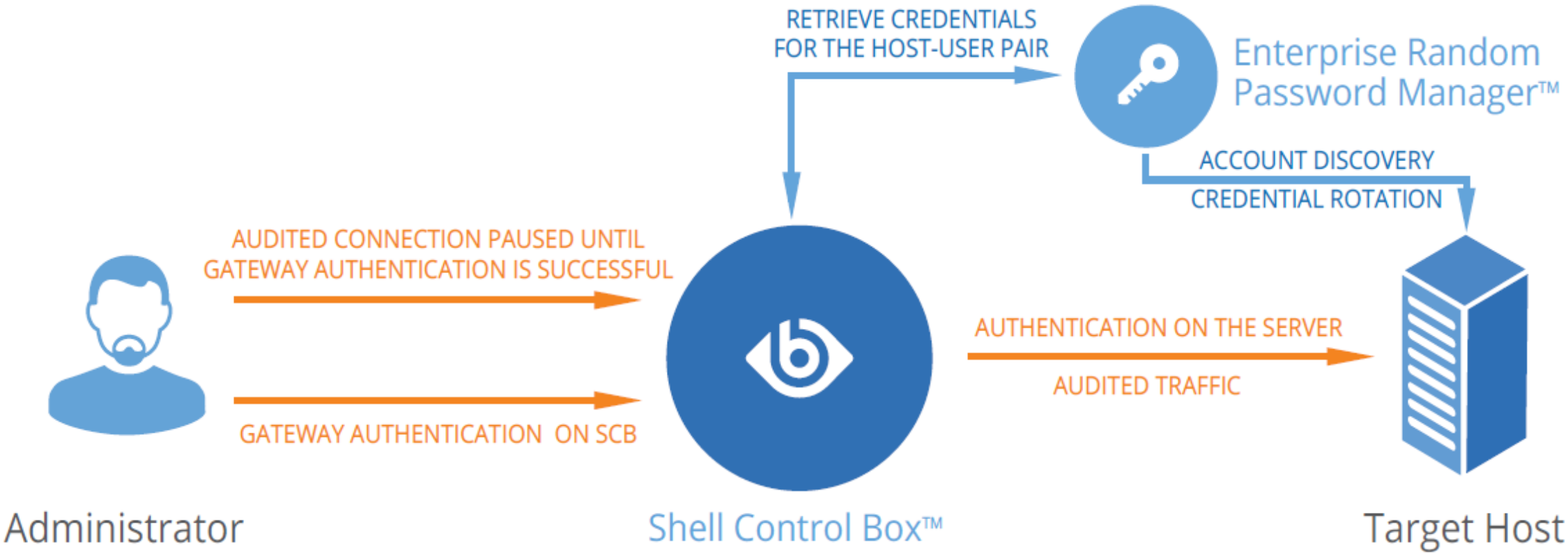
A COMPREHENSIVE PLATFORM



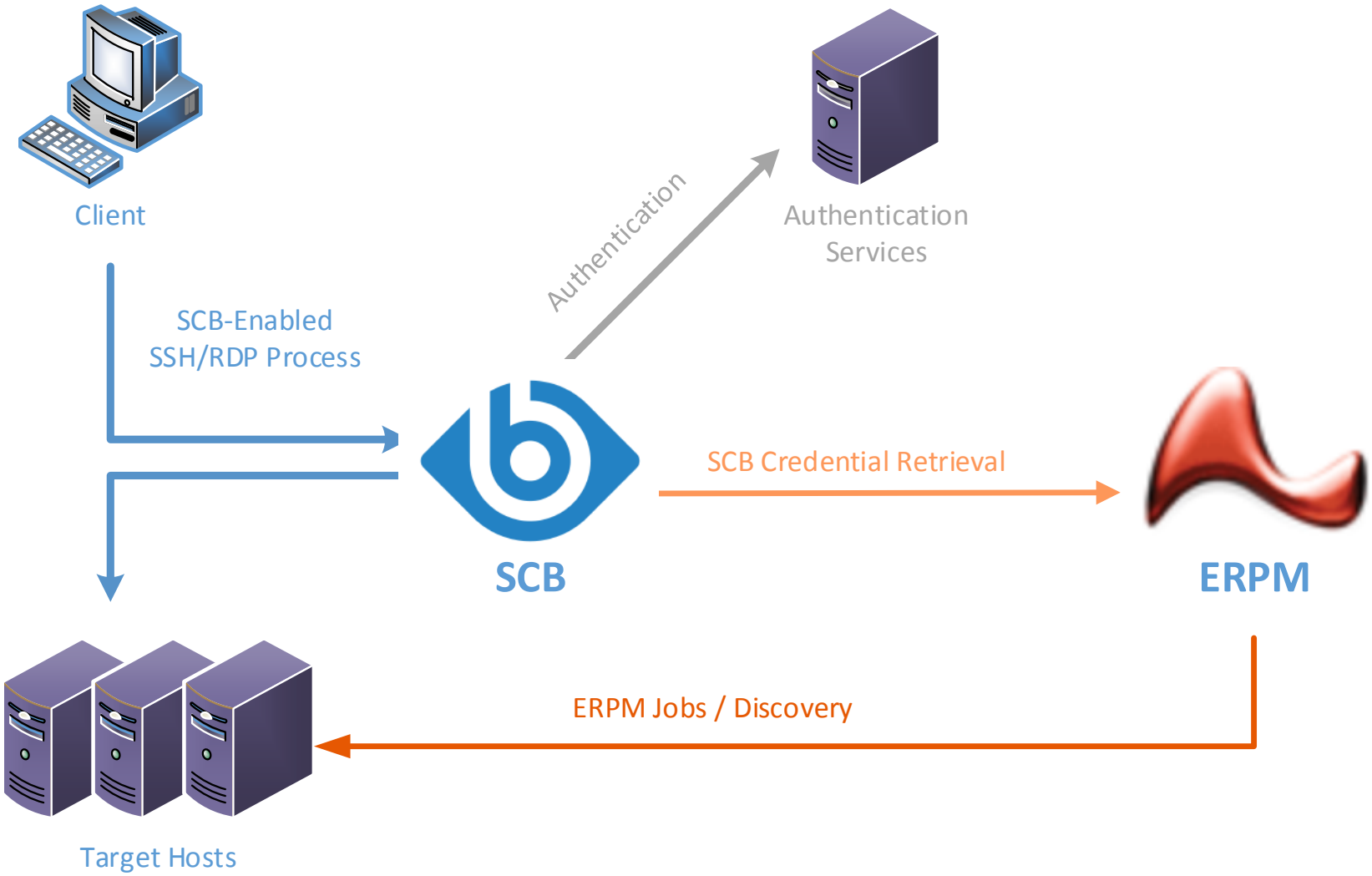
BALABIT

LIEBERMANSOFTWARE

PSM-RED IM INTEGRATION



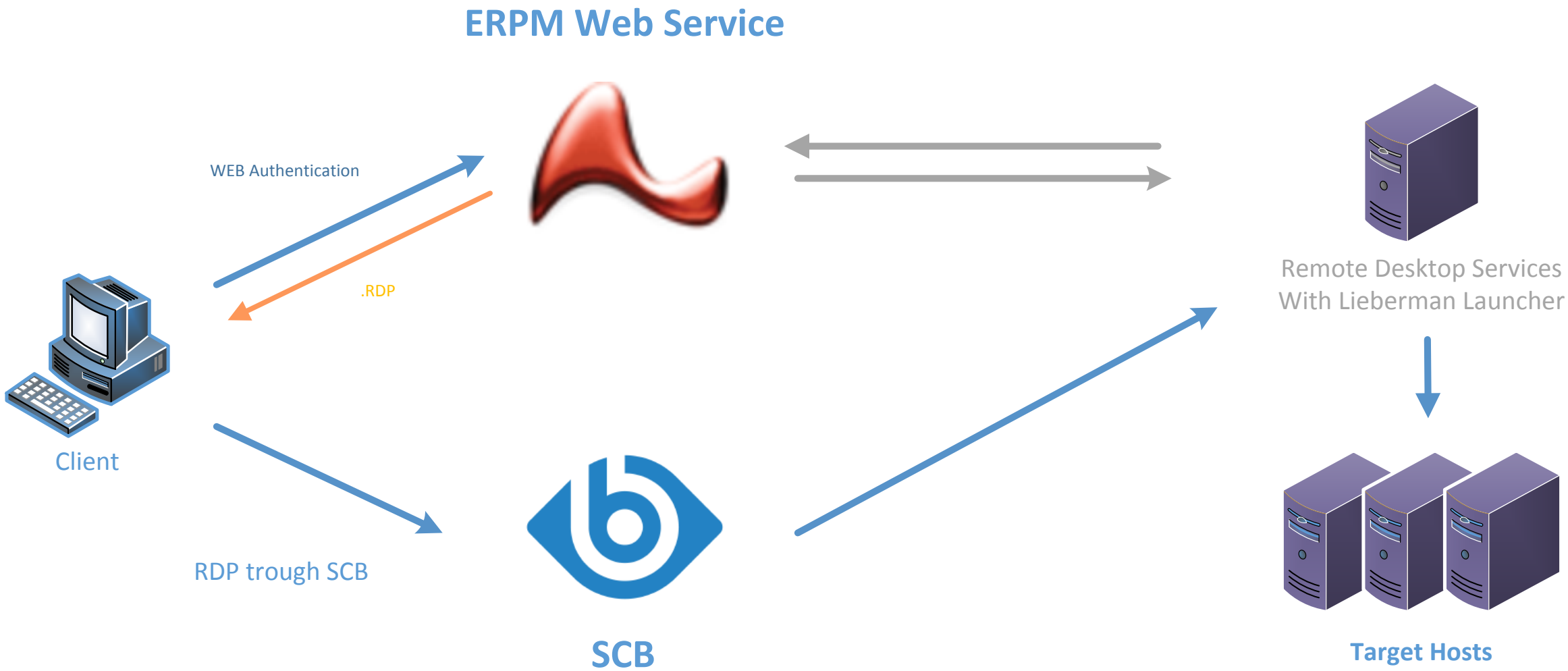
PSM-RED IM INTEGRATED SOLUTION



BALABIT

LIEBERMANSOFTWARE

PSM + RED IM APPLICATION LAUNCHER



PRIVILEGED ACCESS MANAGEMENT

Application Access Control

- Launch on-premises, cloud, and Web applications on your machine or Bastion hosts, without disclosing passwords

Privileged Access Management

REAL-TIME PREVENTION OF MALICIOUS ACTIVITIES

telnet

SSH

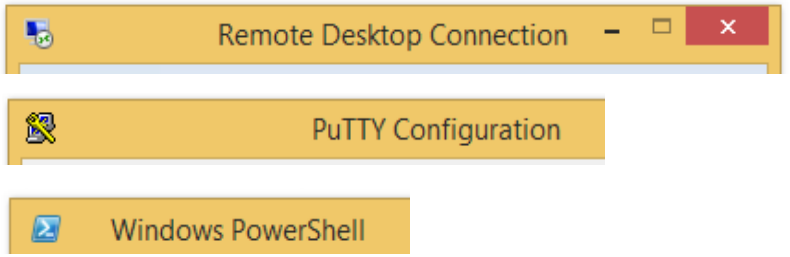
> scp financial.db

Command detection

> cat credit-cards
> 1234 5678 9123 4567

Screen-content detection

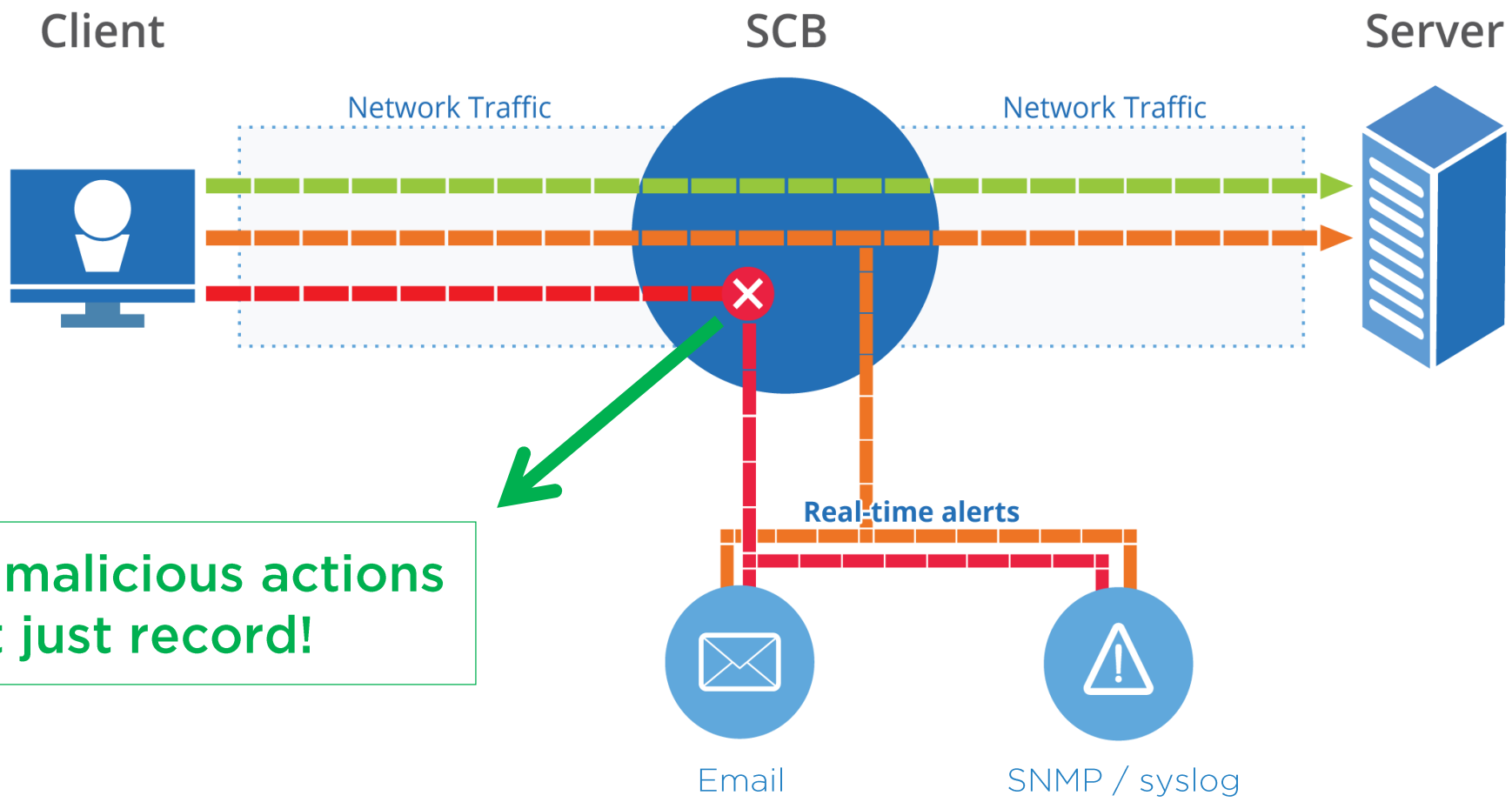
CITRIX



Window-title detection

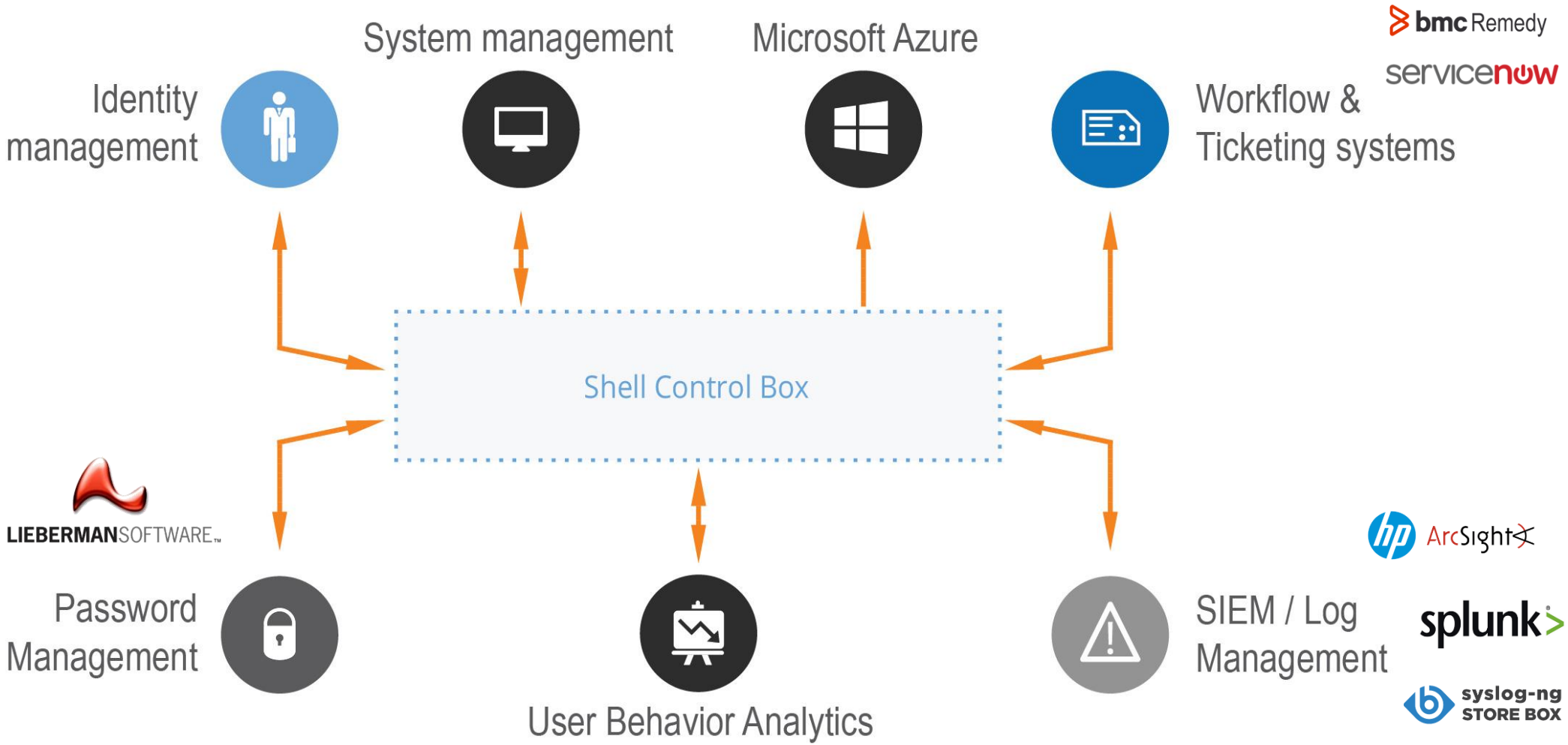
BALABIT

REAL-TIME PREVENTION OF MALICIOUS ACTIVITIES



Prevent malicious actions not just record!

SEAMLESS ENTERPRISE INTEGRATION

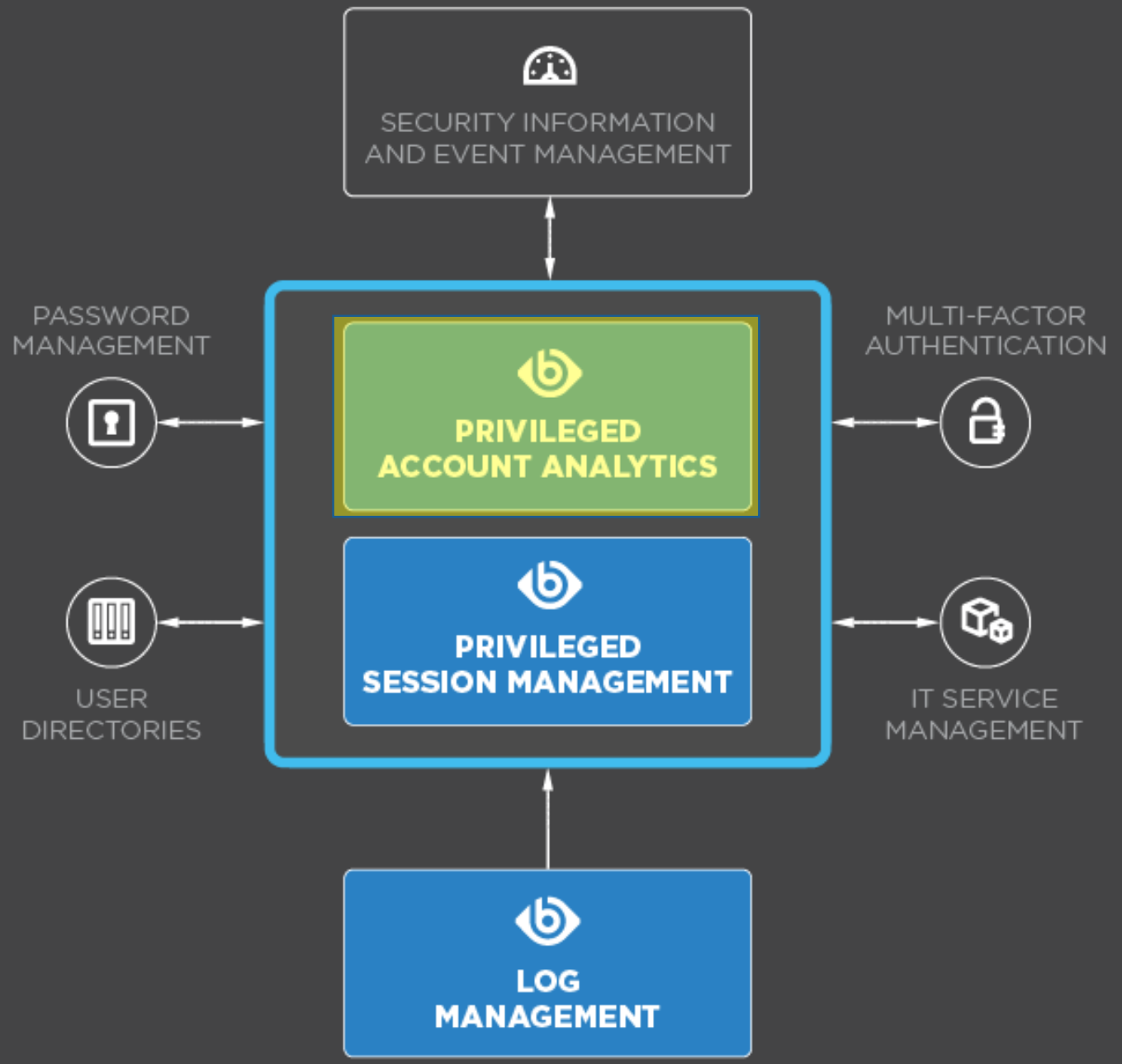


BALABIT

HARDWARE SPECIFICATIONS

T1	T4	T10	VM
1x QuadCore CPU	1x QuadCore CPU	2x 6-Core CPU	n/a
8 GB RAM	8 GB RAM	32 GB RAM	n/a
1 TB Software RAID	4 TB Hardware RAID	10 TB Hardware RAID + spare disk	n/a
	Redundant PSU	Redundant PSU	n/a
HA	HA	HA	ESXi / HyperV / KVM / Azure

BALABIT PRIVILEGED ACCESS MANAGEMENT



FOCUS ON PEOPLE

”Only amateurs attack machines; professionals target people. And any solutions will have to target the people problem, not the math problem”

75% of IT security experts consider insider threats and insiders' account misuse more risky than outsider threats.[9]

83% of IT security experts assume that attackers use social engineering methods – e.g. phishing – when they want to get sensitive data in the shortest time.[10]

What is digital behavior?

Time of login

Accessed servers

Typing dynamics

Used apps

Screen resolution

Typical commands

BALABIT

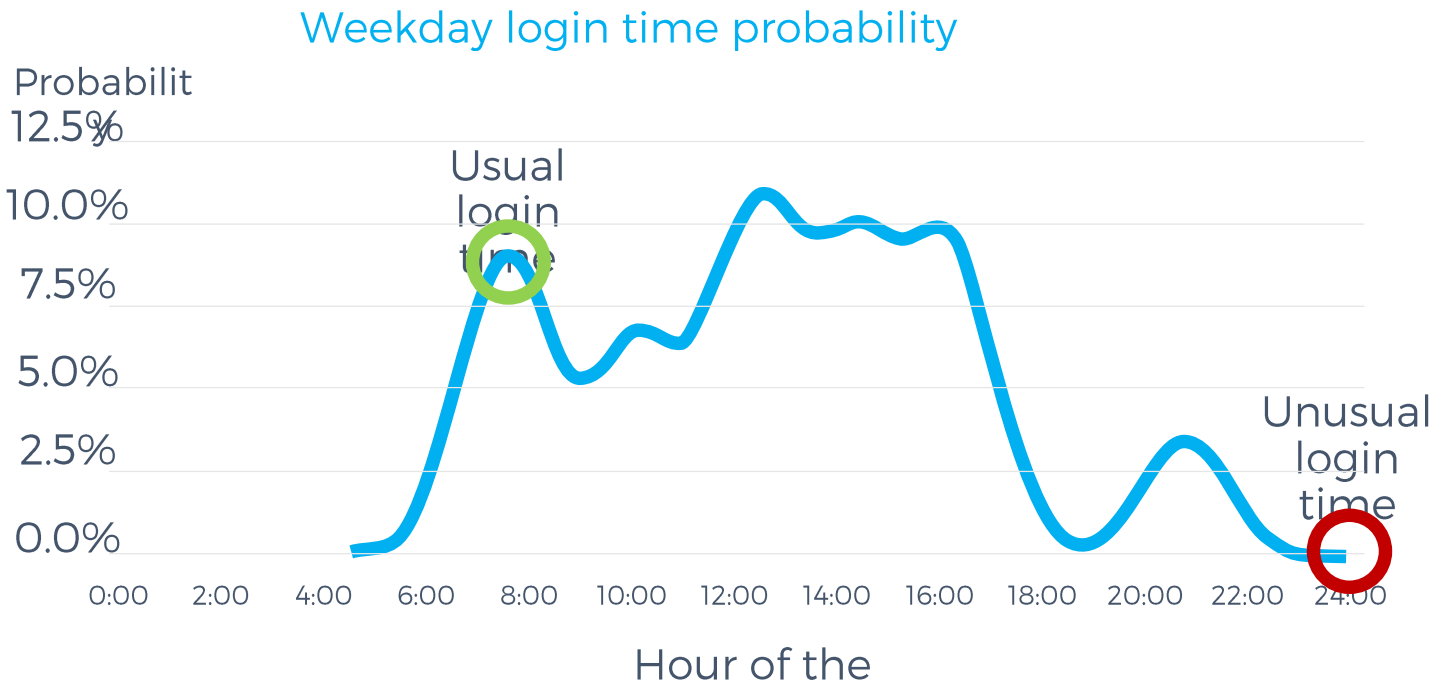
Behavior is the new authentication!

Habits
Something you do

Typical time of working

Typical activities performed (Commands in CLI, Applications in GUIs, Transaction types)

Range of accessed servers and applications



Behavior is the new authentication!

Possession
Something you have

Screen resolution

Mouse vs trackpad vs touchscreen

Type and version of the operating system, browser & client apps

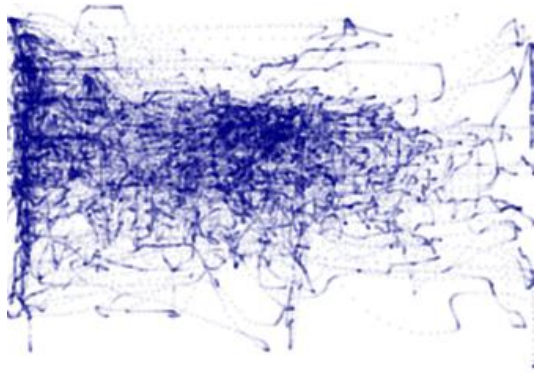
Browser settings (Language, Time zone)

Behavior is the new authentication!

Inherence
Something you are

Mouse movement analysis

Keystroke dynamics analysis



Behavior is the new authentication!

Context
Something that surrounds you

Location (GeoIP, ISP, GPS data)

Network traffic counters

IP address reputation

How can behavior analysis prevent attacks?

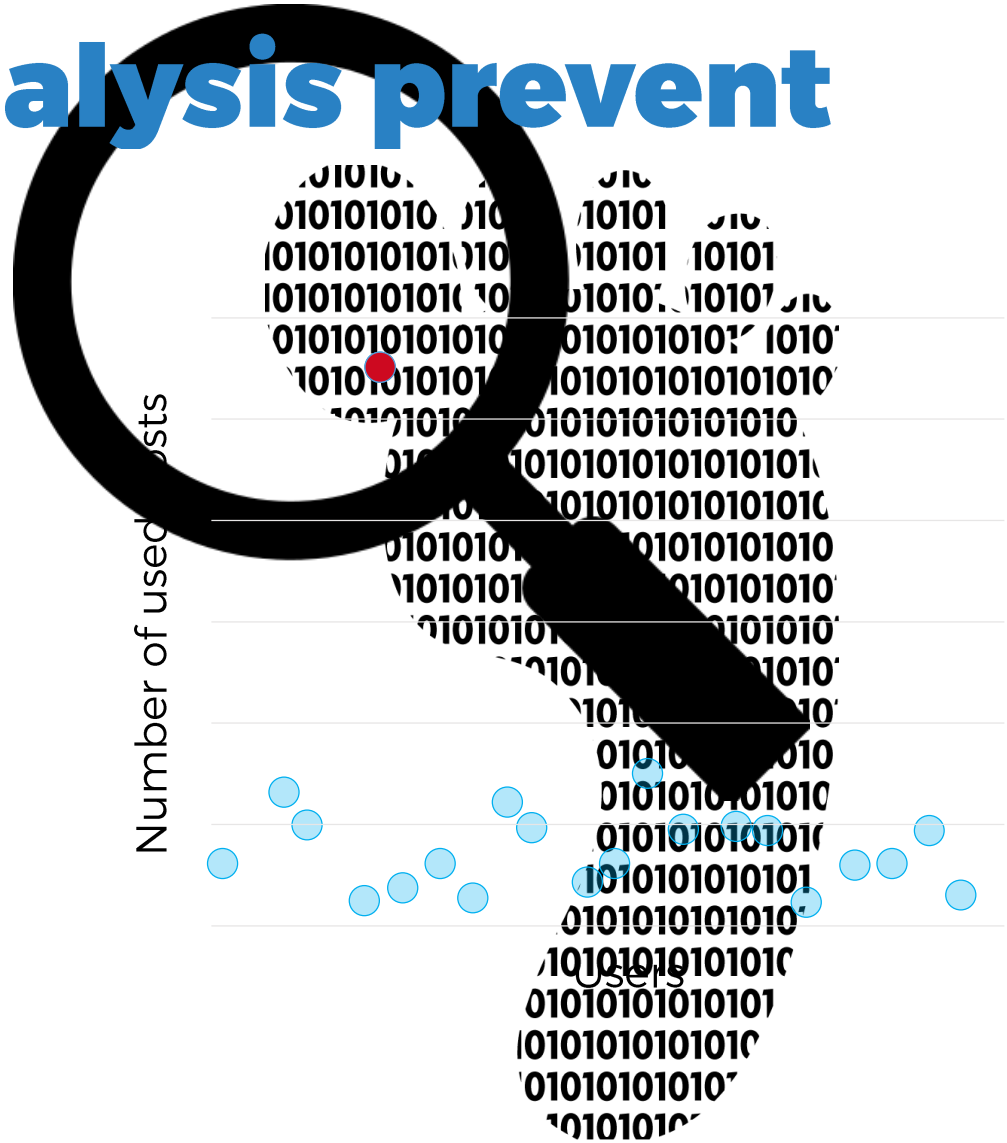
GATHER users' DIGITAL FOOTPRINTS

DEFINE what is NORMAL, build user baselines

Identify UNUSUAL EVENTS in real-time

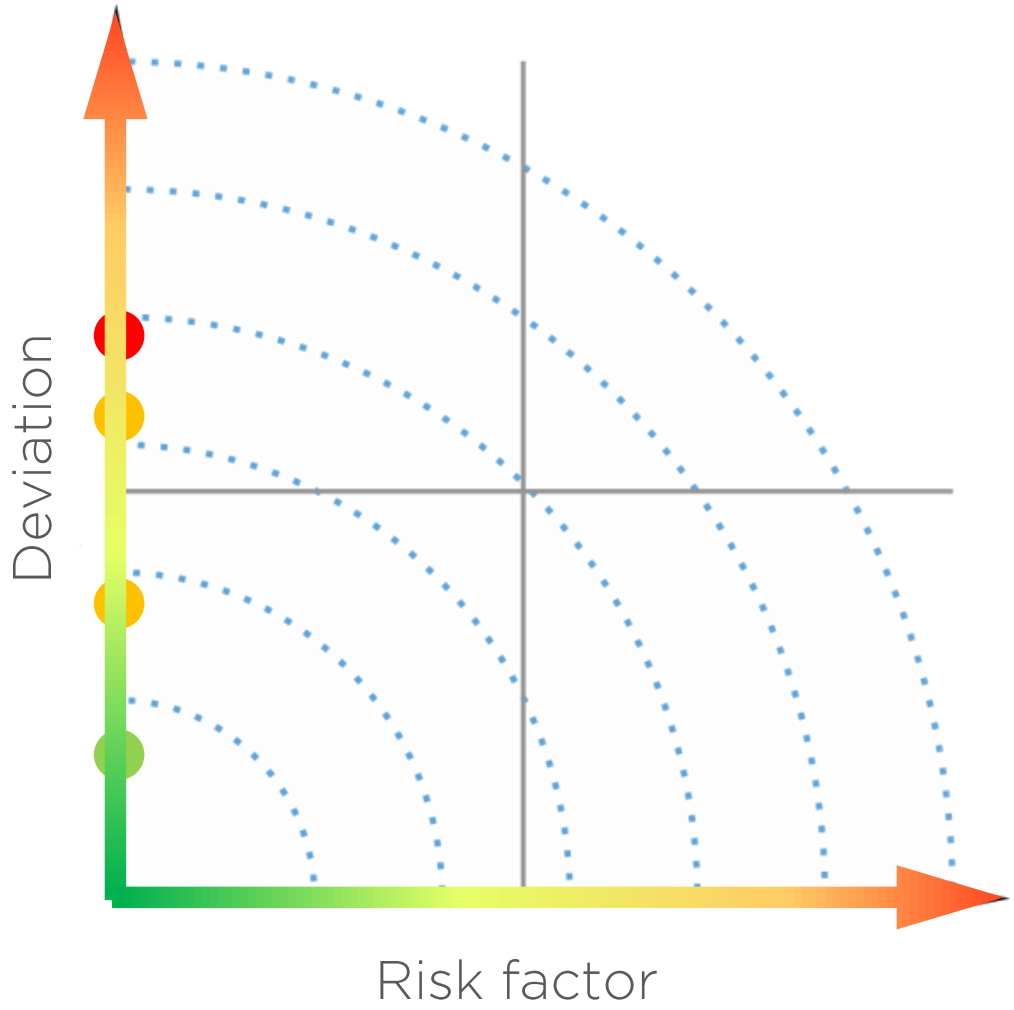
Identify EXTERNAL attackers

Identify malicious INSIDERS



BALABIT

FOCUS ON THE IMPORTANT



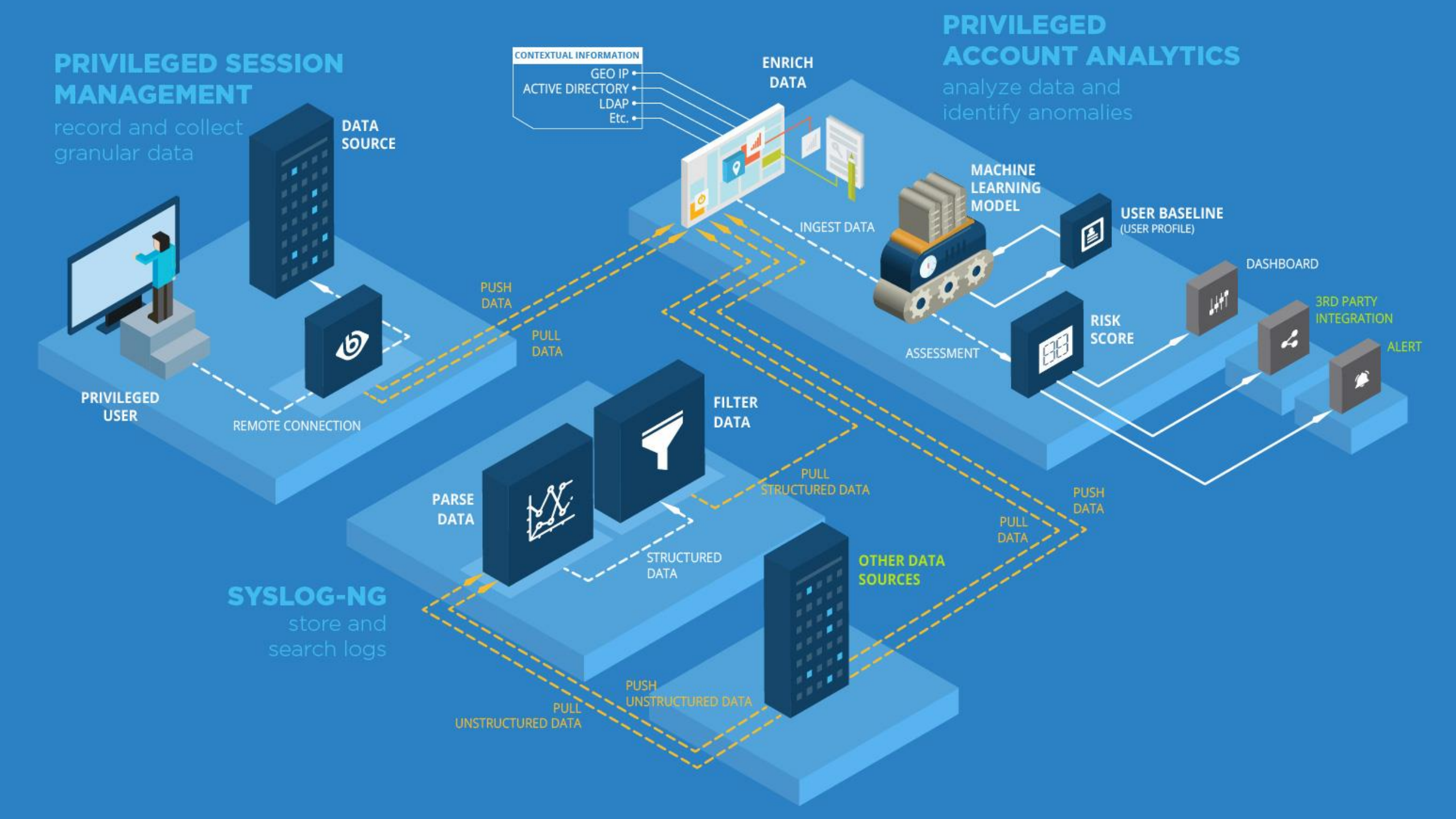
- DBA runs a query on the customers' table
- DBA restarts Oracle
- Trainee logs in at 11PM
- Trainee logs in at 9AM

Priority list based on risk factor and deviation

WHY BALABIT PRIVILEGED ACCESS MANAGEMENT?

Our proxy-based technology enables:

- Fastest deployment time – no agents required
- Most granular access control (command level policy enforcement)
- Real-time alerts
- Real-time shadowing
- No change to workflows
- Full text search of session content, not just metadata
- Behavioral biometrics
- Automated session termination


PRIVILEGED SESSION MANAGEMENT
record and collect granular data
DATA SOURCE
PRIVILEGED USER
REMOTE CONNECTION
CONTEXTUAL INFORMATION
GEO IP
ACTIVE DIRECTORY
LDAP
Etc.
ENRICH DATA
PUSH DATA
PULL DATA
INGEST DATA
PRIVILEGED ACCOUNT ANALYTICS
analyze data and identify anomalies
MACHINE LEARNING MODEL
USER BASELINE
(USER PROFILE)
DASHBOARD
3RD PARTY INTEGRATION
ALERT
RISK SCORE
ASSESSMENT
FILTER DATA
PARSE DATA
PULL STRUCTURED DATA
PUSH DATA
PULL DATA
STRUCTURED DATA
OTHER DATA SOURCES
SYSLOG-NG
store and search logs
PUSH UNSTRUCTURED DATA
PULL UNSTRUCTURED DATA

BALABIT

THANK YOU.
QUESTIONS?

Péter SOPRONI | Pre-Sales Engineer | peter.soproni@balabit.com