BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

SHELL CONTROL BOX

Best-of-breed Privileged User Monitoring

AGENDA

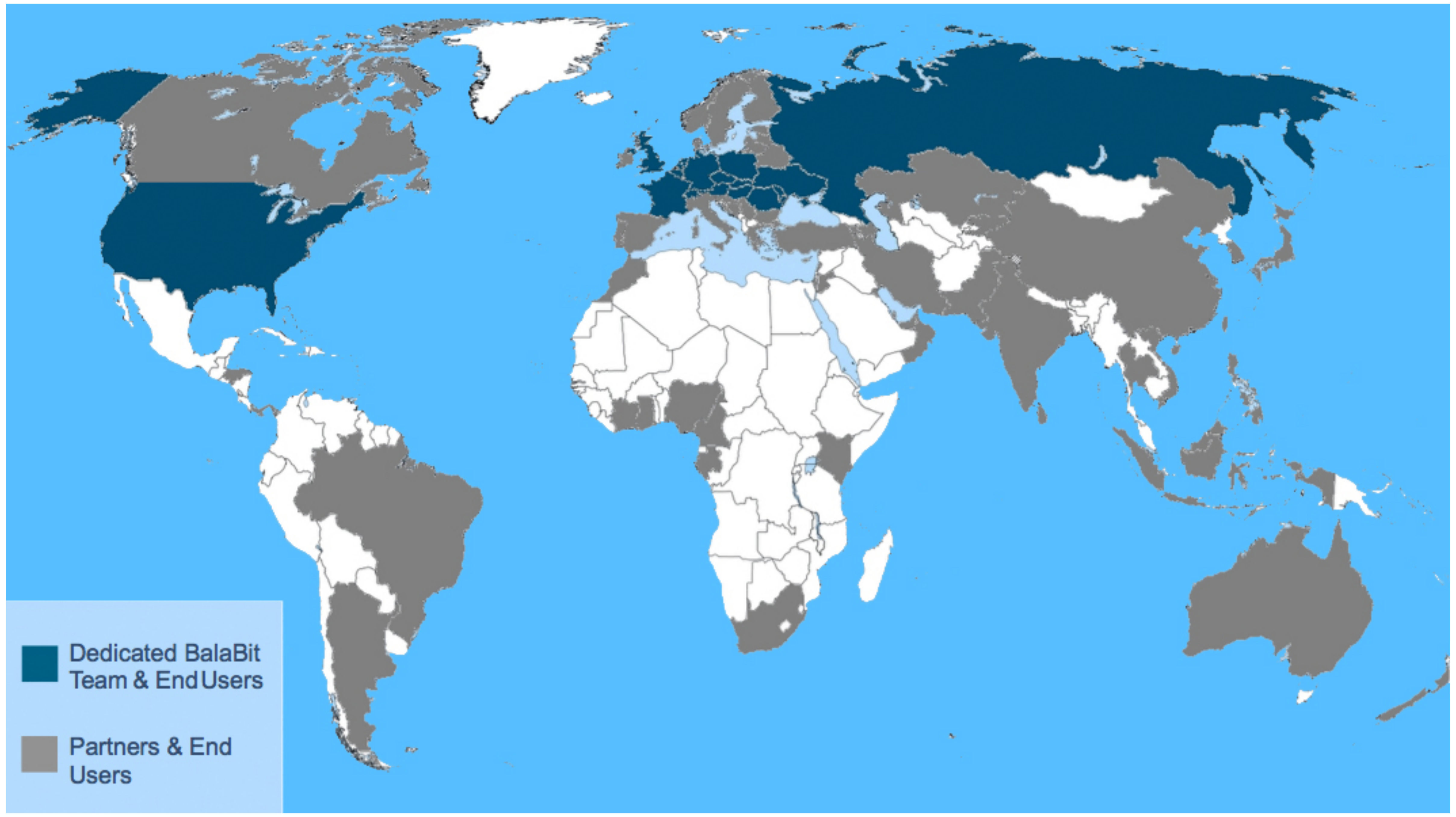
- ABOUT BALABIT
- SECURITY THREATS BY HUMANS
- USER MONITORING BY BALABIT
- USE CASES
- TARGET CUSTOMERS
- BENEFITS

BALABIT

Leading Provider of Contextual Security Intelligence

Global technology lead in

- Log Management
  syslog-ng
- Privileged User Monitoring
  Shell Control Box
- User Behavior Analytics
  Blindspotter



BALABIT

Key Facts

EXPERTISE

- 15 years in IT security

GROWTH

- 30% avg. revenue increase

RECOGNITION

- More than 1 Million installations

CLIENTS

- More than 1300 clients

REFERENCES

- 23 of Fortune100

CHANNEL

- More than 100 partners

REFERENCE CUSTOMERS

TELCO

T-Mobile

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

KMF

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
Les territoriaux solidaires

APRIA HEALTHCARE®

UNIVERSITY OF EXETER

LEEKIE ENTERPRISES INCORPORATED

PARTNERSHIPS

vmware® PARTNER
TECHNOLOGY ALLIANCE

SailPoint™

MAPR®

Microsoft

thycotic

AllianceONE Partner / hp

redhat®

CITRIX® READY

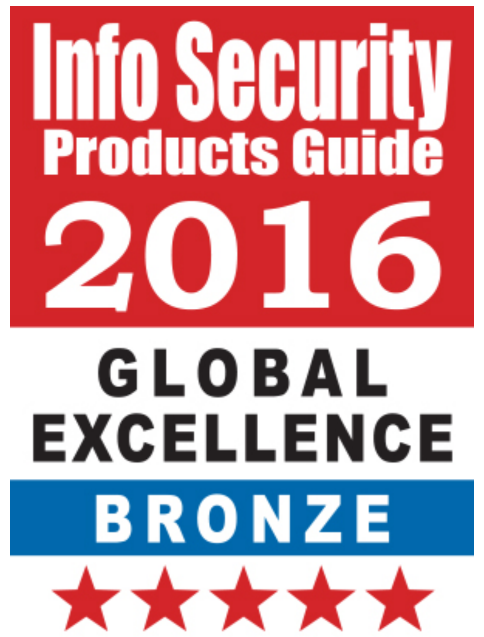
LIEBERMANSOFTWARE™

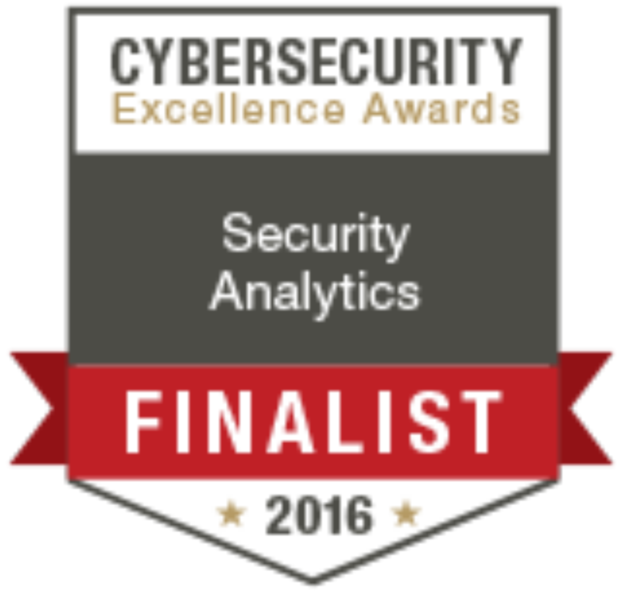
Omada

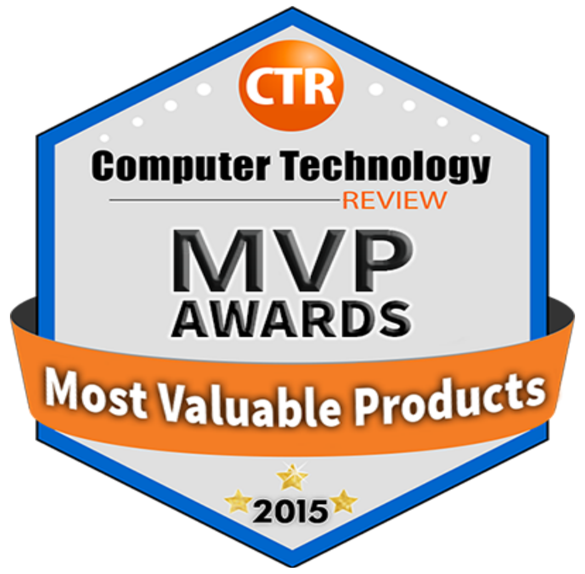
Hortonworks

AWARDS & CERTIFICATIONS

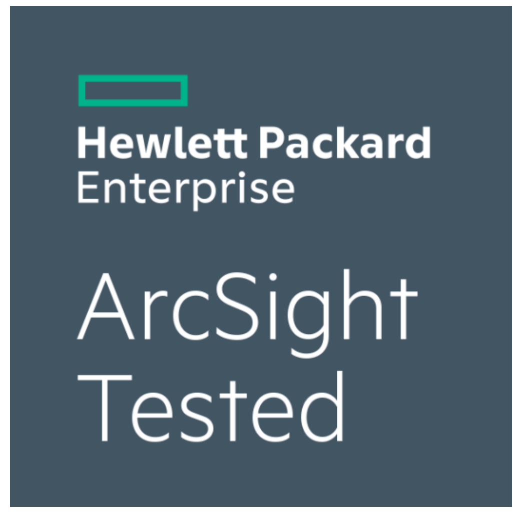
Blindspotter

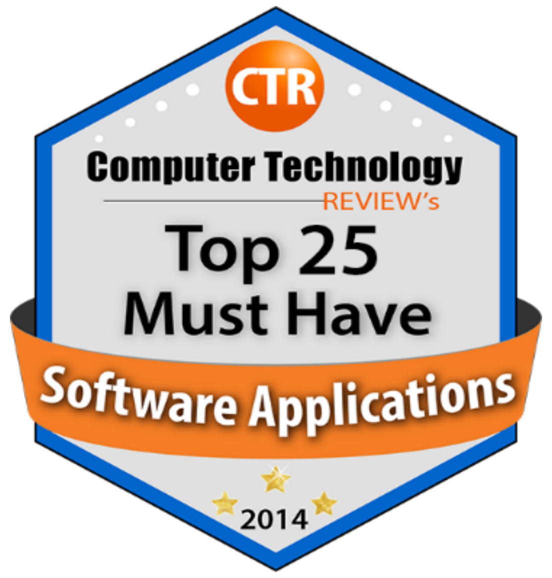


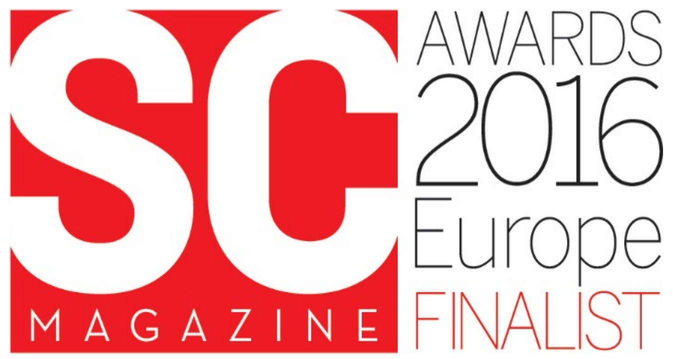


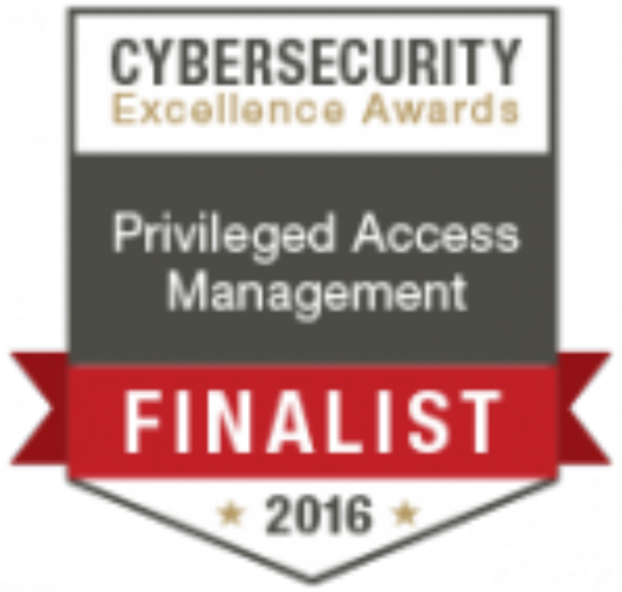


Shell Control Box





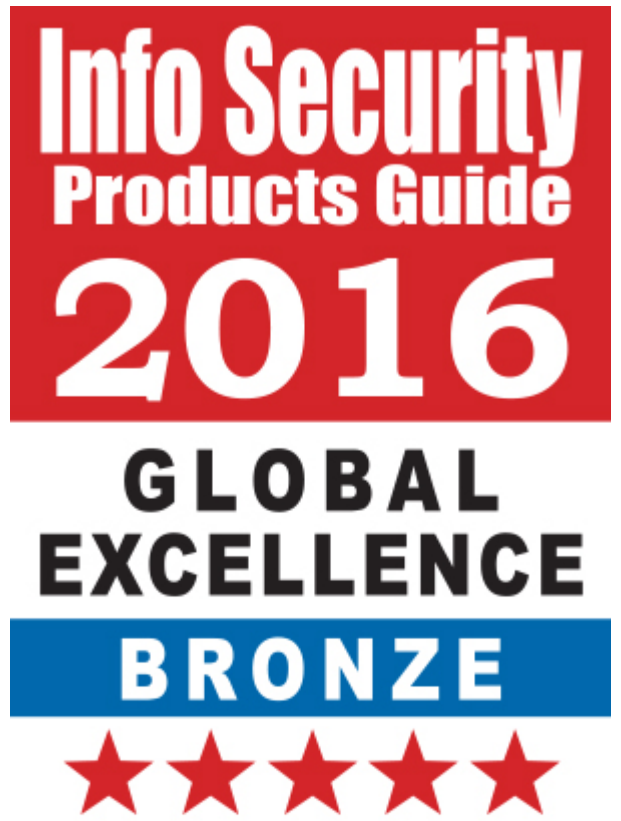


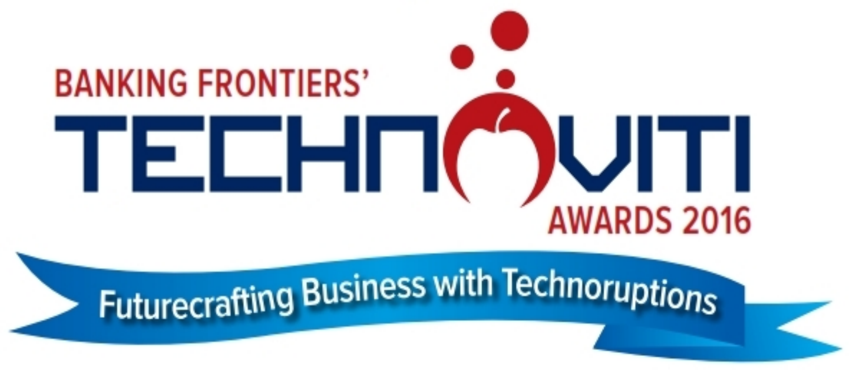


infosecurity
RUSSIA

westcoast labs
PERFORMANCE VALIDATED

CSI Suite





ENTERPRISES IN INCREASING TROUBLE

Cyber-threats Caused by Humans

BREACHES CONTINUE…

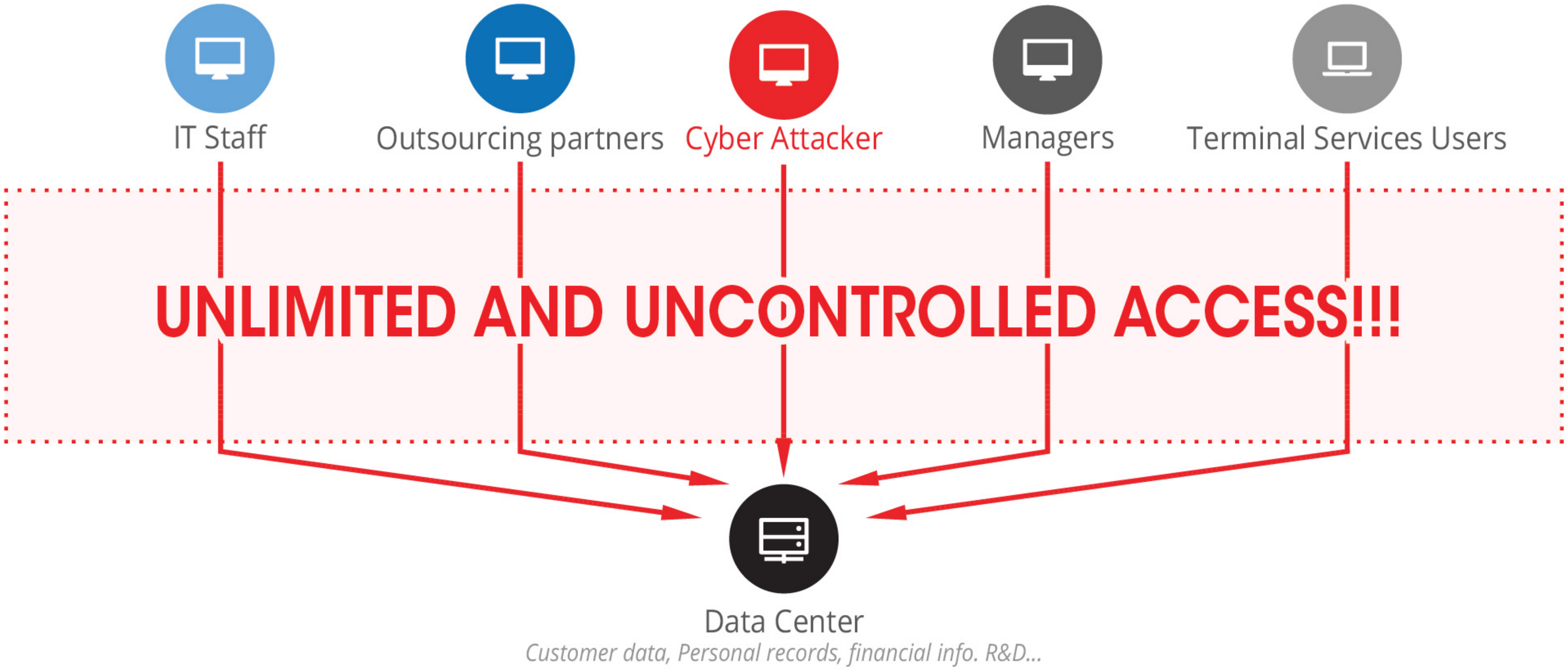
Sucess for APT depends on privileged account hijacking

Retail giant Target confirmed that credit and debit card information for 40 million of its customers had been compromised. ” – New York Times
The CEO and CIO left the company

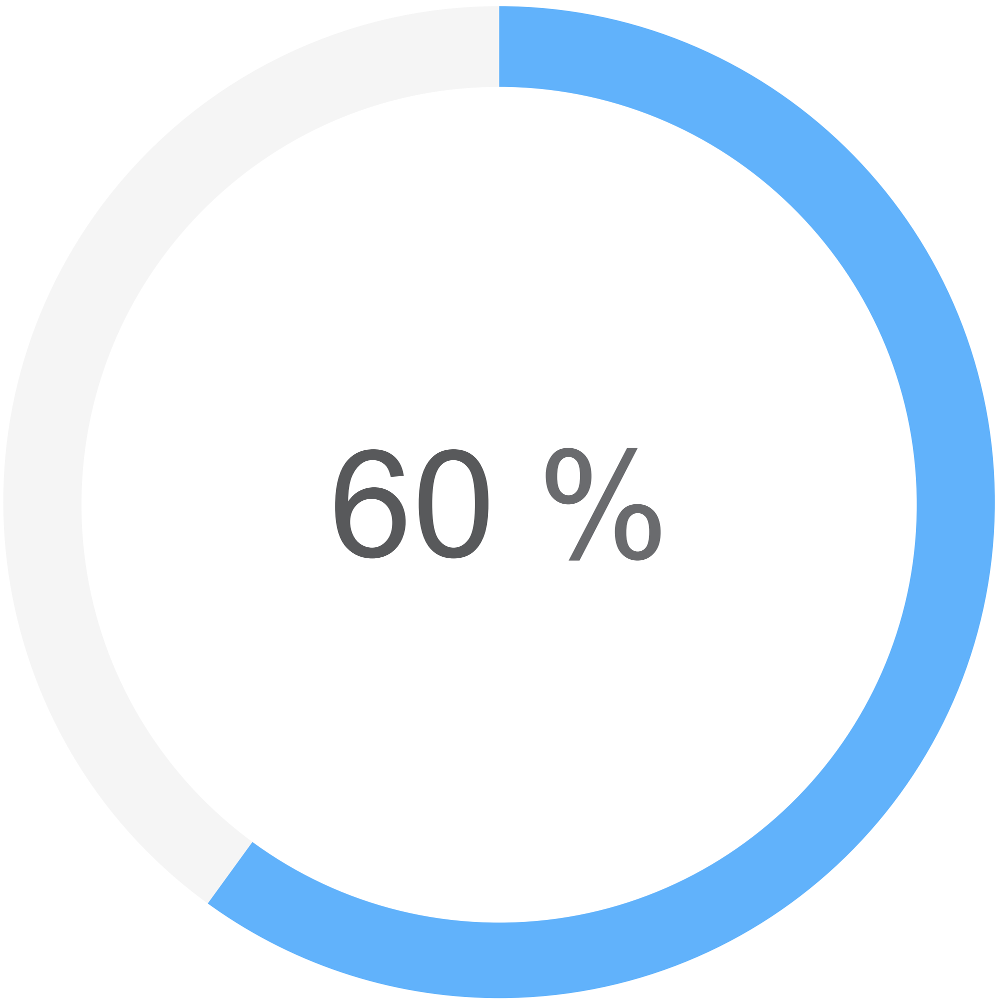
Sony Pictures Entertainment has been targeted by computer hackers in an attack which reports say forced it shut down its systems… – BBC
Costs estimated at $15-35 M and growing

Office on Personnel Management government data breach impacted 21.5 million people – CNN
Director resigned

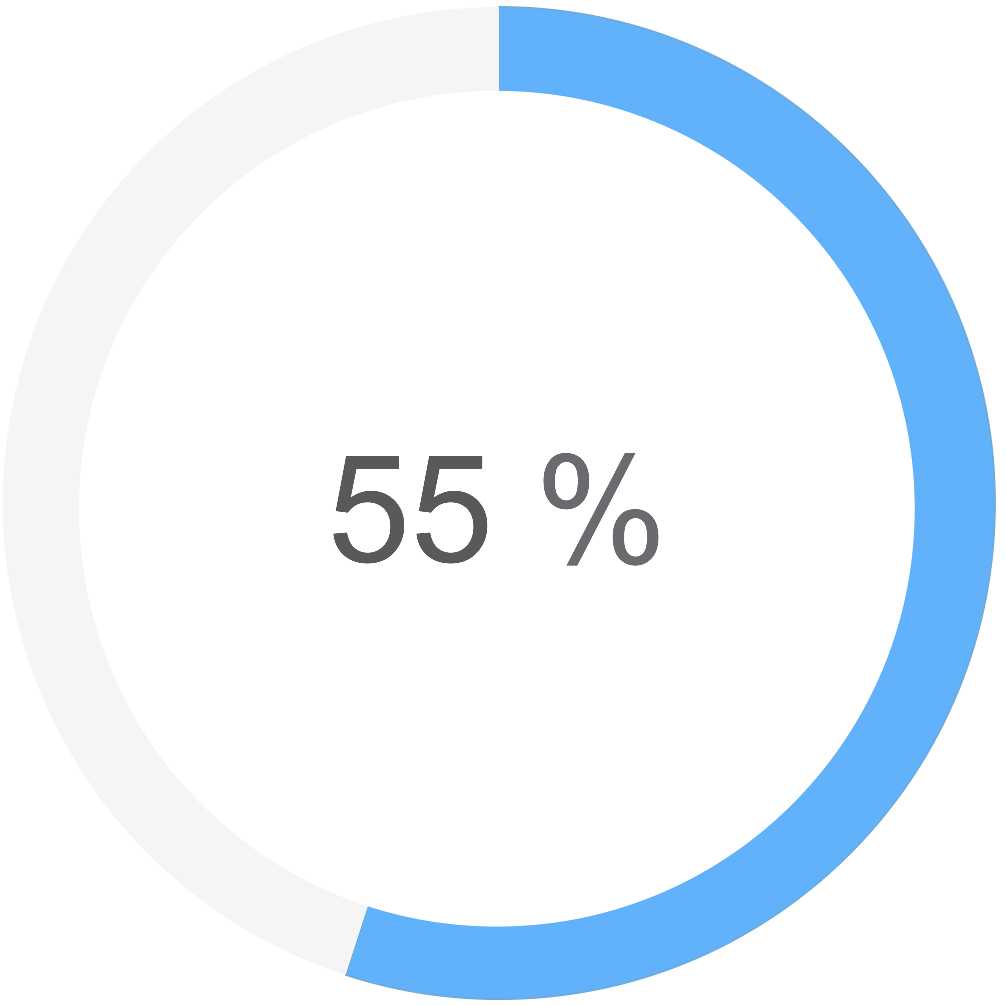
UNFETTERED ACCESS OF PRIVILEGED USERS…


IT Staff
Outsourcing partners
Cyber Attacker
Managers
Terminal Services Users
UNLIMITED AND UNCONTROLLED ACCESS!!!
Data Center
Customer data, Personal records, financial info. R&D…

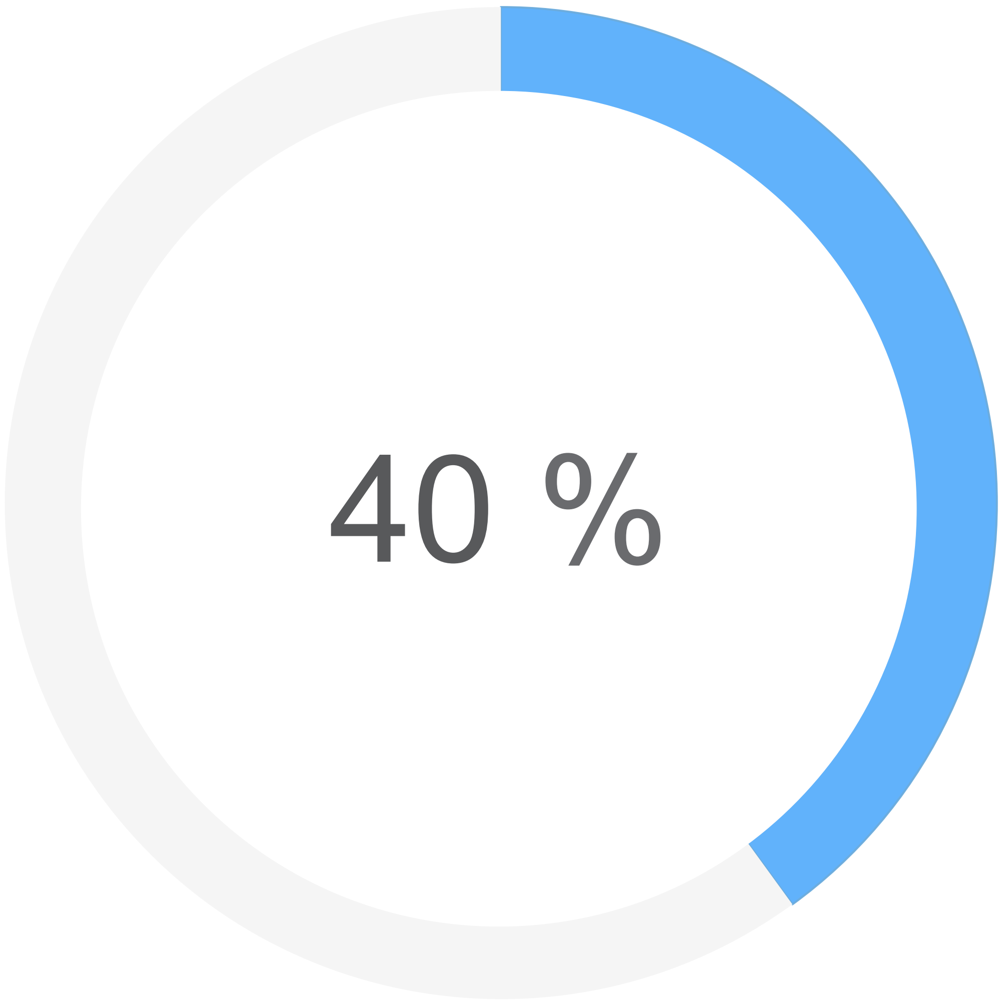
PRIVILEGED ACCOUNT MISUSE



Incidents
by
SYSTEM ADMINS



Internal misuse
by
PRIVILEGE ABUSE



Top threat actions
by
STOLEN CREDENTIALS

BALABIT

** Source: Verizon 2015 Data Breach Investigations Report*

verizon 2015 DATA BREACH INVESTIGATIONS REPORT

COMPLIANCE PRESSURE FOR MONITORING USERS

ISO 2700X

PCI DSS

SOX/ COBIT

ISAE 3402 / SAS 70

LOCAL LAWS

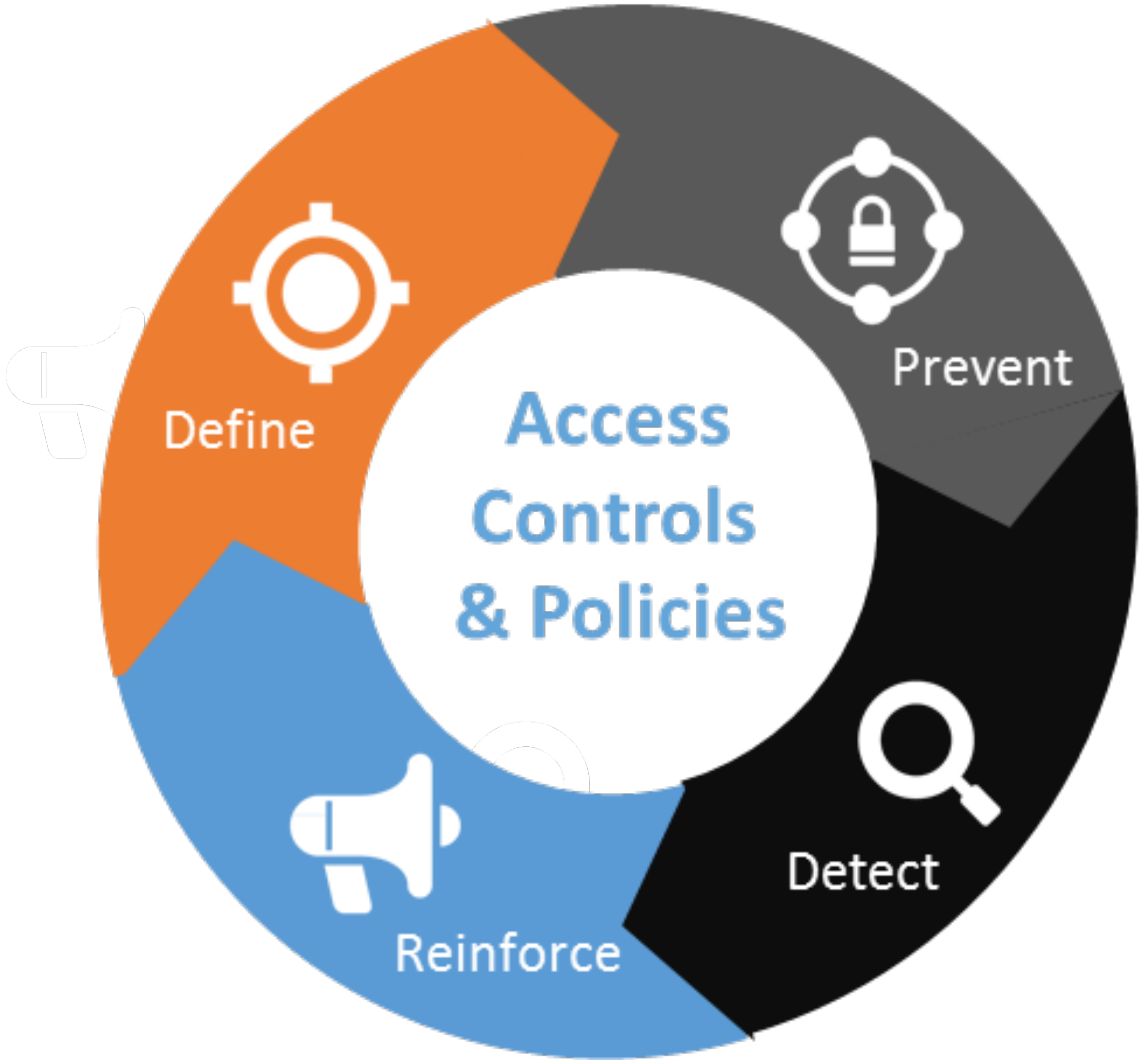
EU DIRECTIVES

GPG, FISMA, HIPAA, JSOX, etc

LIMITATIONS OF „TRADITIONAL” APPROACHES

CONVENTIONAL APPROACHES TO IT SECURITY

- Build layers of access controls, policies and walls
- Use predefined patterns and rules to prevent access
- Restrict users and business agility



BALABIT

TRADITIONAL SOLUTIONS' BOTTLENECKS

1

FIREWALLS

No granular access control

Admins & APTs* can bypass FWs

2

LOGGING/SIEM* PRODUCTS

Several types of events are not logged!

Difficult to understand

Admins (or attackers) can delete the logs!

3

Password managers

Complex and costly systems

No answer to „who did what?”

…These solutions are NOT Enough!

**APT: Advanced Persitent Threat*

**SIEM: Security Information & Event Management*

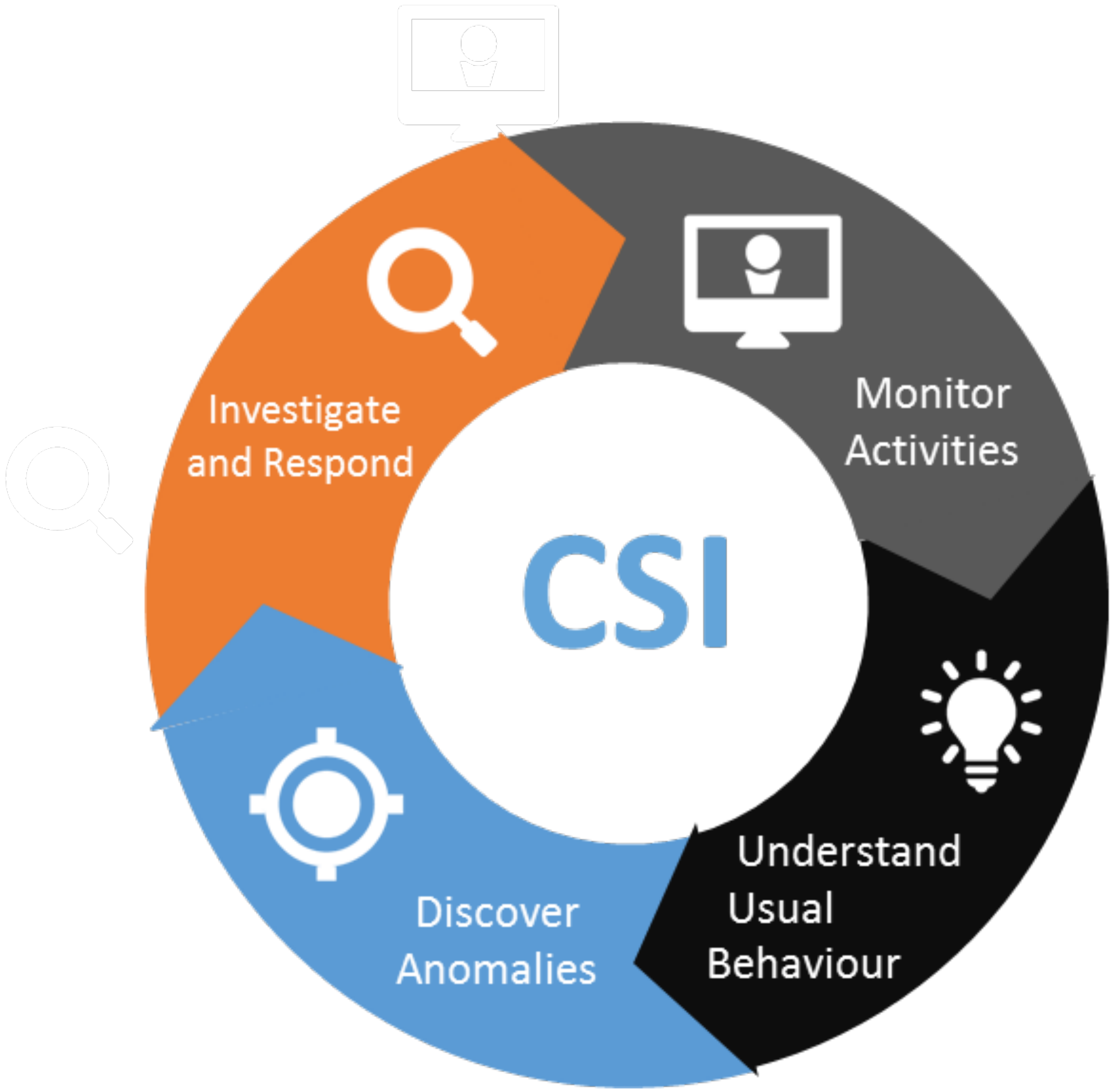
CONTEXTUAL SECURITY INTELLIGENCE (CSI)

Prevent data breaches without constraining business

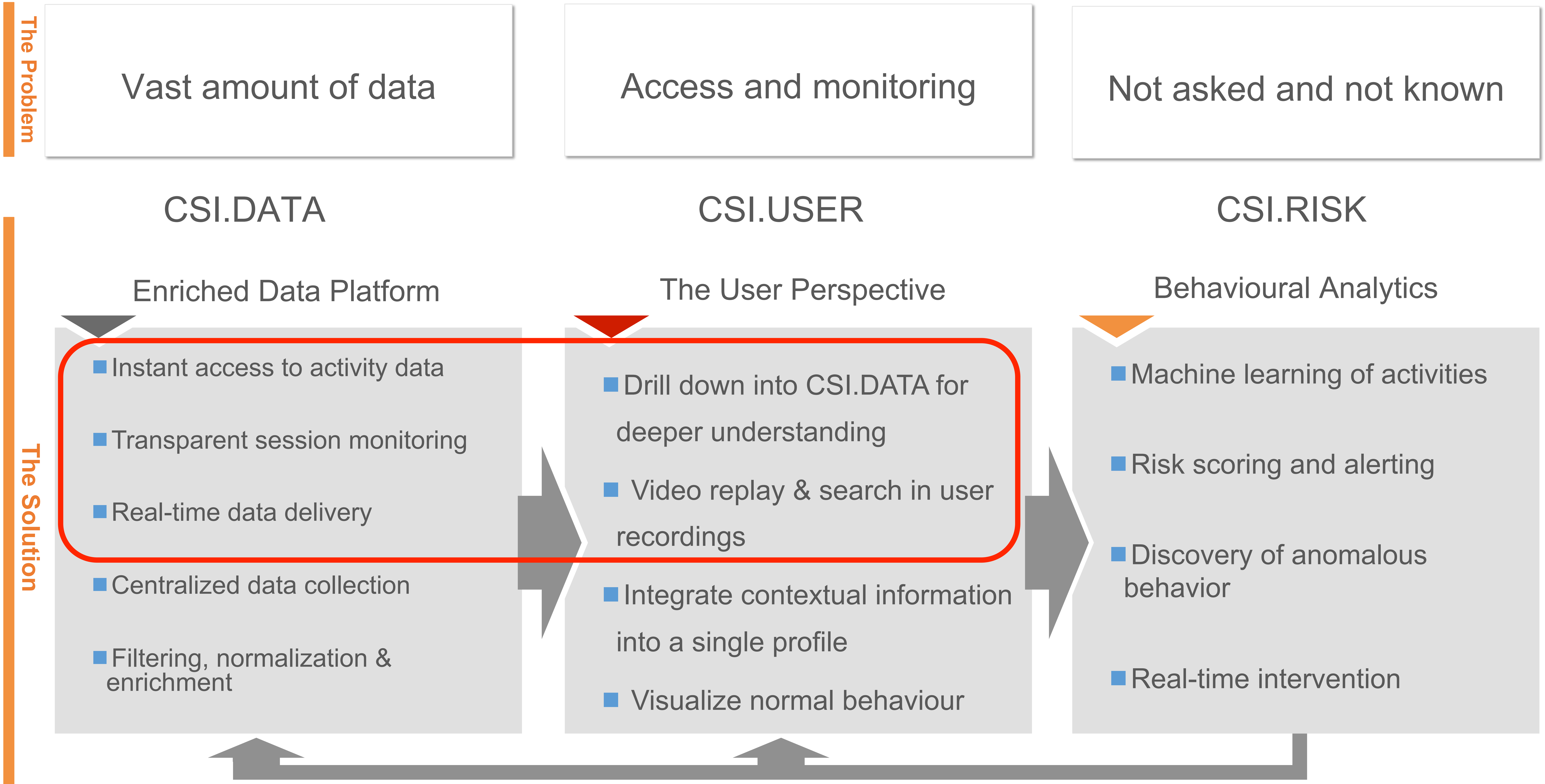
MOVE FROM PREVENTATIVE TO CONTEXTUAL SECURITY

- Monitor User Activity
- Baseline business-as-usual using machine learning
- Discover unknown threats based on deviation from the norm and risk in real-time
- Investigate and Respond immediately

Trust, but verify!



CONTEXTUAL SECURITY INTELLIGENCE SUITE



The Problem

Vast amount of data

Access and monitoring

Not asked and not known

The Solution

CSI.DATA

Enriched Data Platform

- Instant access to activity data
- Transparent session monitoring
- Real-time data delivery
- Centralized data collection
- Filtering, normalization & enrichment

CSI.USER

The User Perspective

- Drill down into CSI.DATA for deeper understanding
- Video replay & search in user recordings
- Integrate contextual information into a single profile
- Visualize normal behaviour

CSI.RISK

Behavioural Analytics

- Machine learning of activities
- Risk scoring and alerting
- Discovery of anomalous behavior
- Real-time intervention

BALABIT
SHELL CONTROL BOX

Best-of-breed Solution for Privileged User Monitoring

SHELL CONTROL BOX

Privileged User Activity Monitoring

Controls

privileged access to remote servers

Prevents

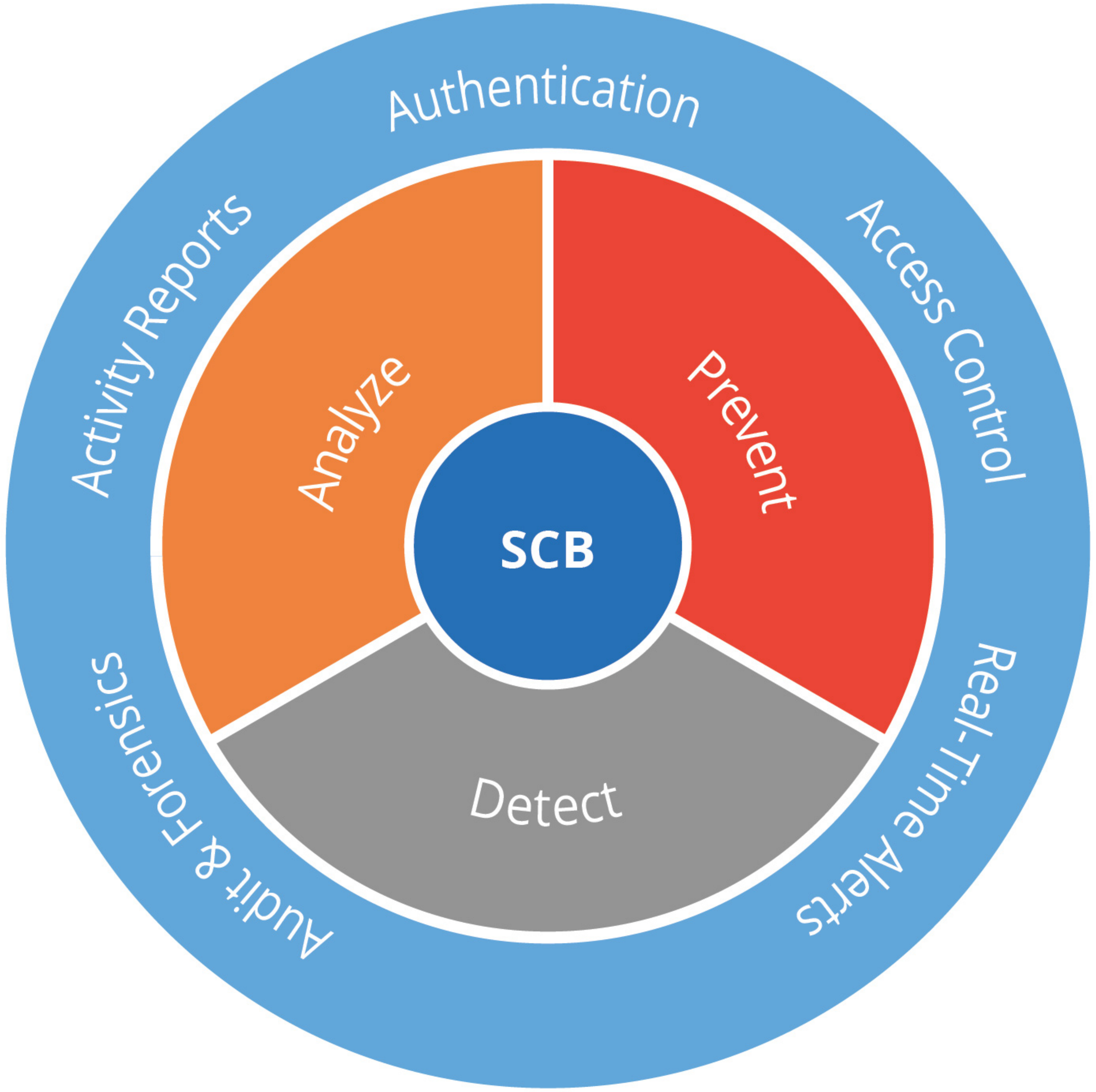
malicious actions

Records

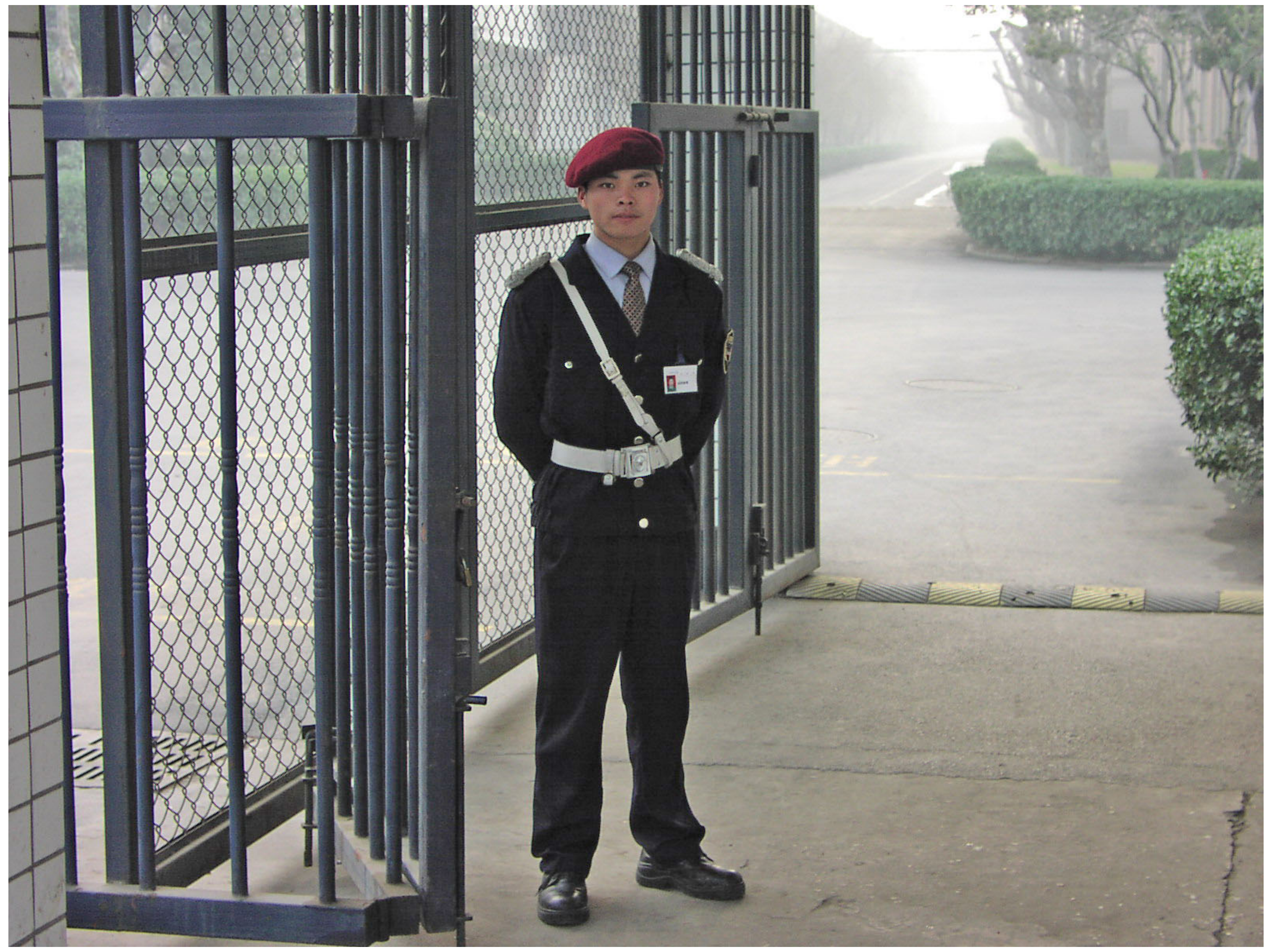
activities into movie-like audit trails

Reports

actions for compliance and/or decision support reasons



„REAL-LIFE” EXAMPLES

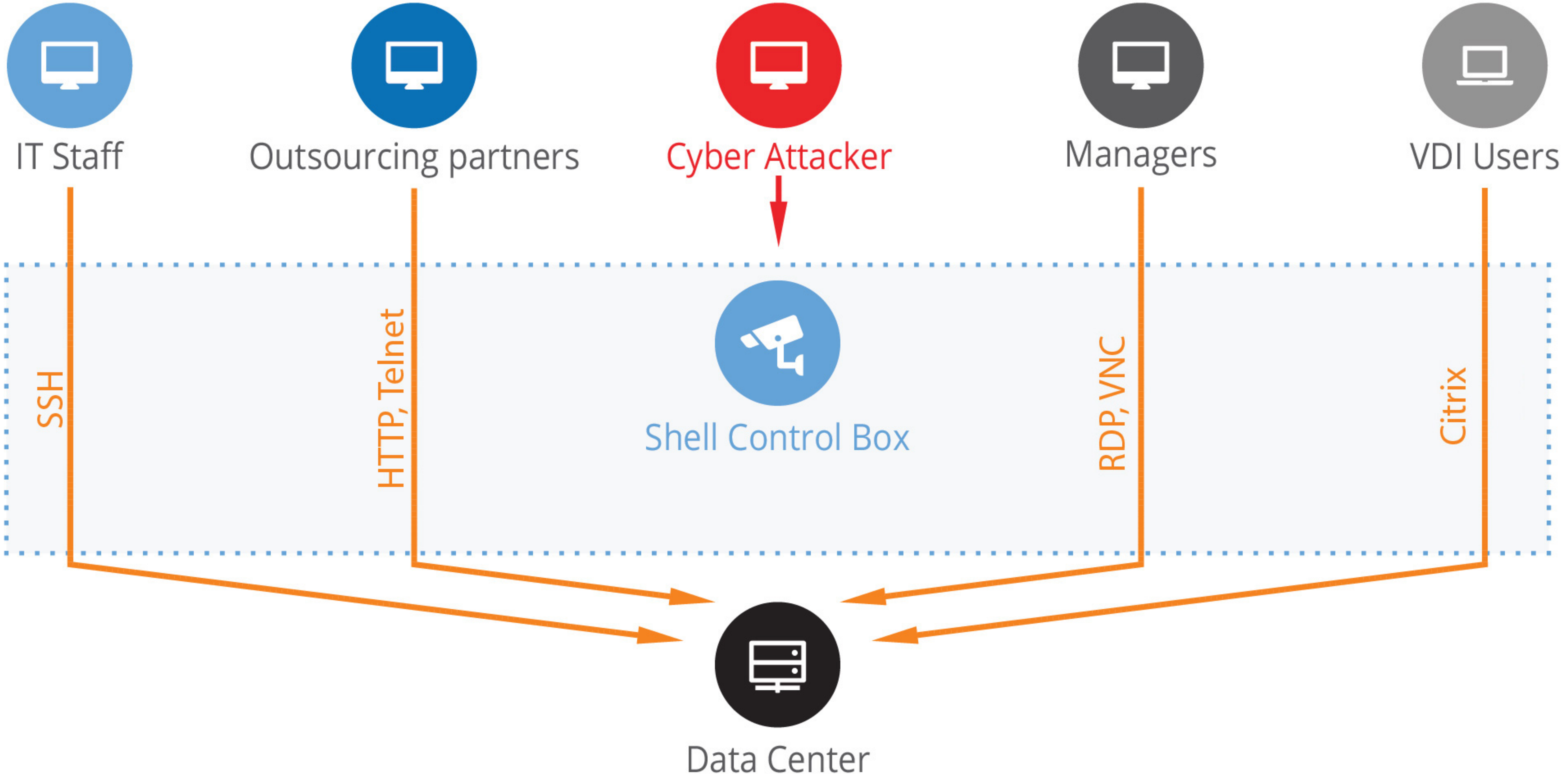


Access Control

Monitoring

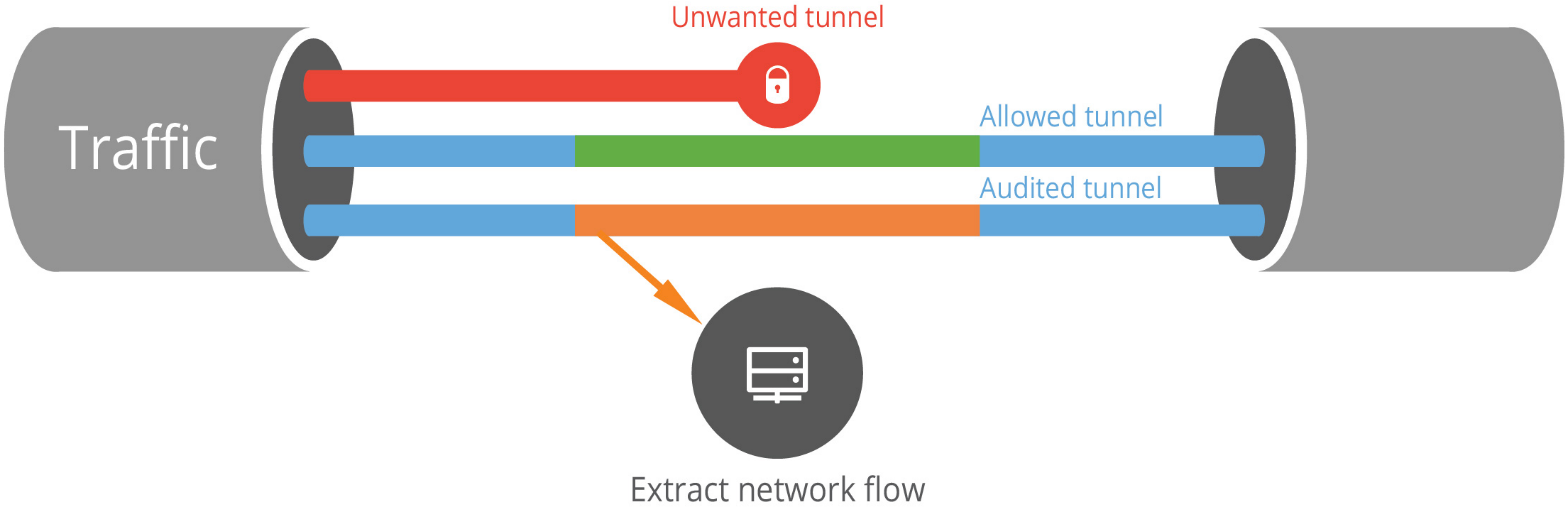
Tamper-proof Recording

TURNKEY, INDEPENDENT AND TRANSPARENT AUDITING

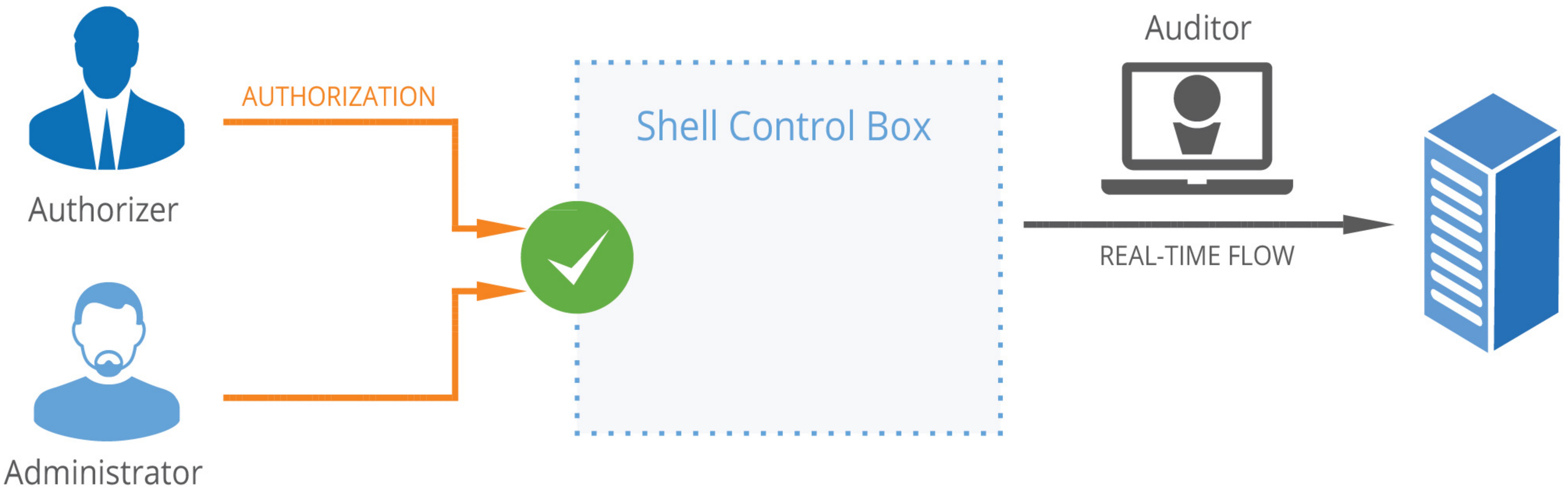


BALABIT

GRANULAR ACCESS CONTROL

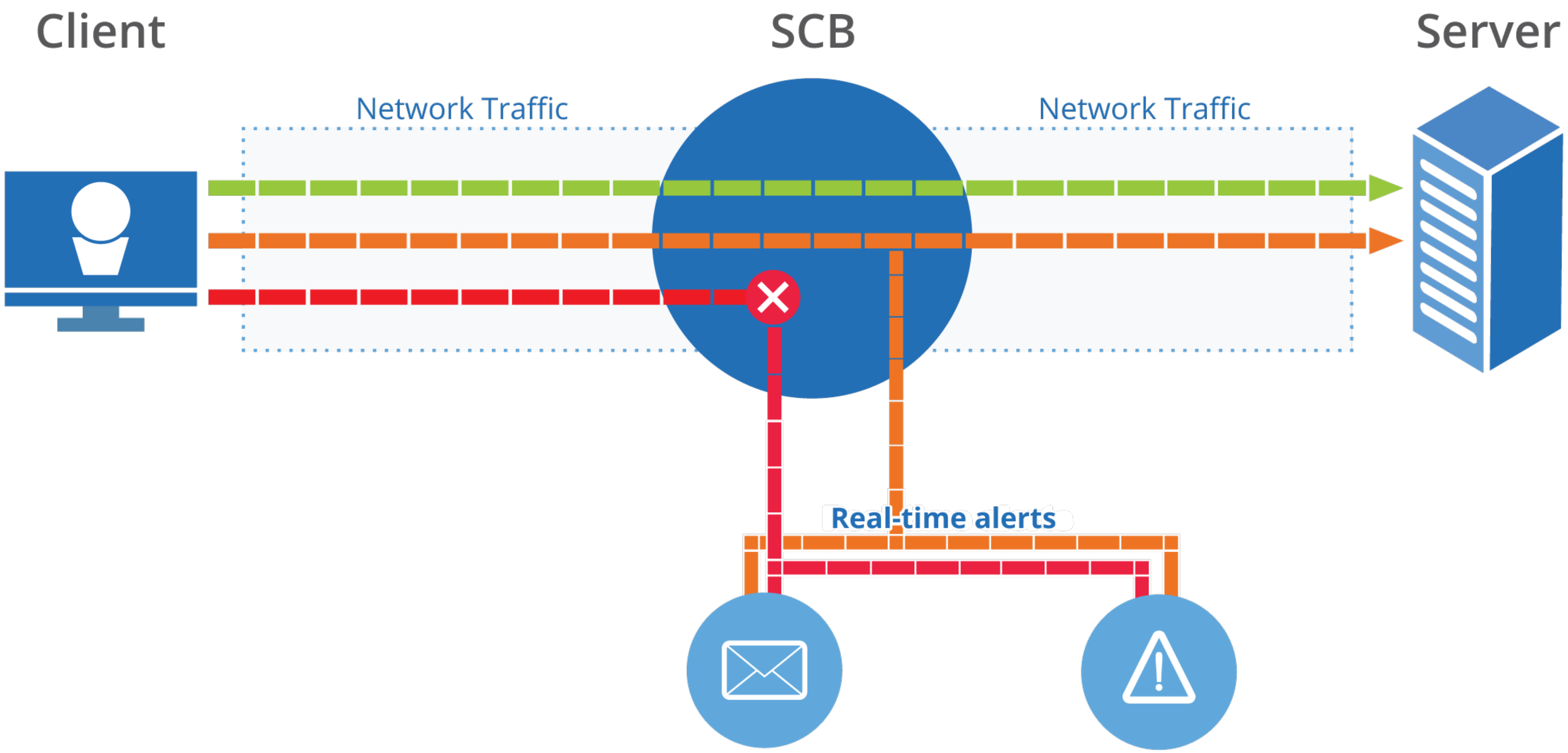


4-EYES AUTHORIZATION & REAL-TIME MONITORING



BALABIT

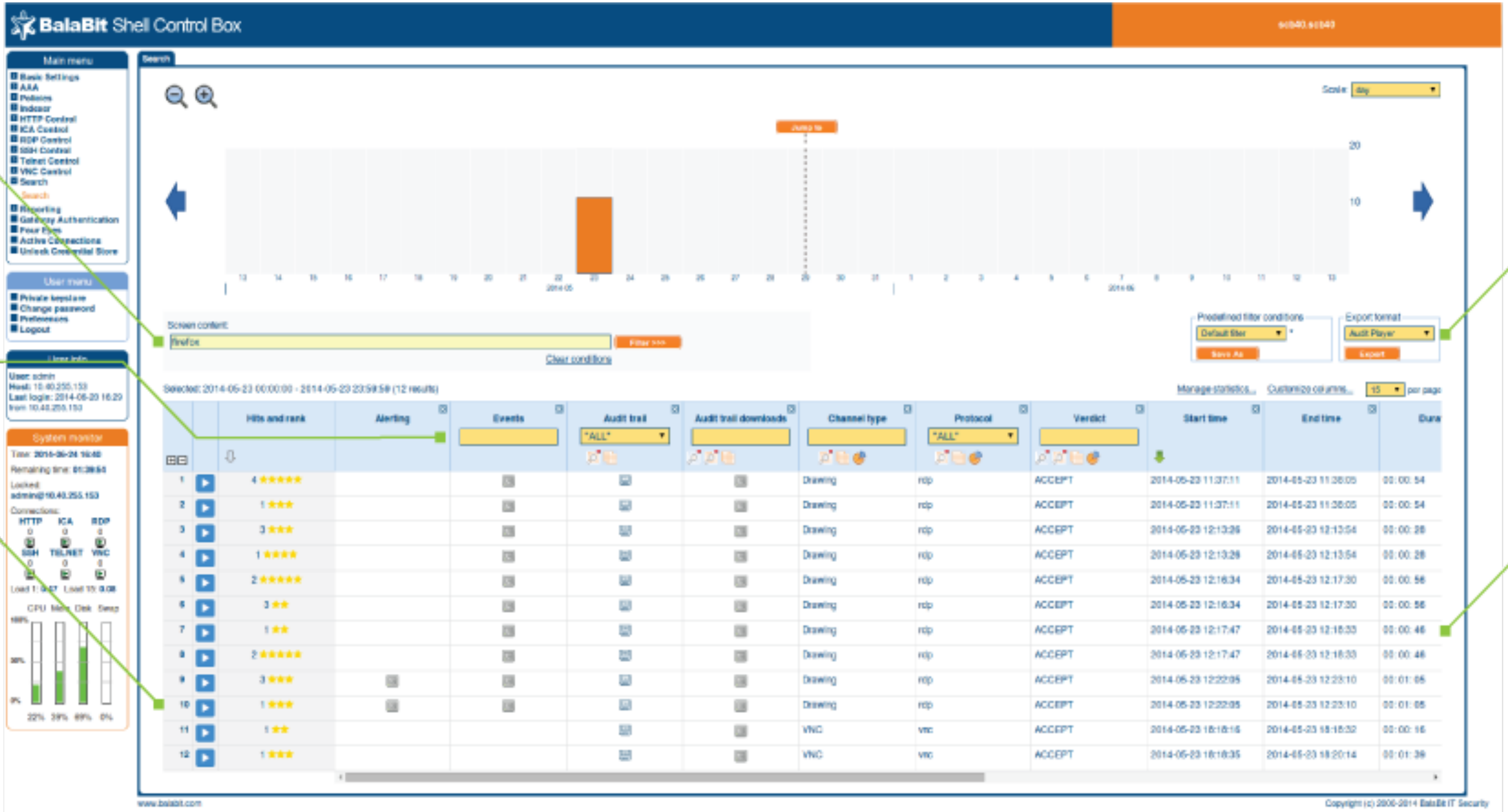
REAL-TIME PREVENTION OF MALICIOUS ACTIVITIES



Prevent malicious actions not just record!

BALABIT

FAST IT TROUBLESHOOTING & FORENSICS



User: admin
Host: 10.40.255.153
Last login: 2014-05-20 16:29 from 10.40.255.153

Time: 2015-06-24 16:40
Remaining time: 01:39:54
Locked: admin@10.40.255.153

Screen content: firefox

Clear conditions

Selected: 2014-05-23 00:00:00 - 2014-05-23 23:59:59 (12 results)

		Hits and rank	Alerting	Events	Audit trail	Audit trail downloads	Channel type	Protocol	Verdict	Start time	End time	Dura
					"ALL"			"ALL"				
1	▶	4 ★★★★★		▣	▣	▣	Drawing	rdp	ACCEPT	2014-05-23 11:37:11	2014-05-23 11:38:05	00:00:54
2	▶	1 ★★★		▣	▣	▣	Drawing	rdp	ACCEPT	2014-05-23 11:37:11	2014-05-23 11:38:05	00:00:54
3	▶	3 ★★★		▣	▣	▣	Drawing	rdp	ACCEPT	2014-05-23 12:13:26	2014-05-23 12:13:54	00:00:28
4	▶	1 ★★★★		▣	▣	▣	Drawing	rdp	ACCEPT	2014-05-23 12:13:26	2014-05-23 12:13:54	00:00:28
5	▶	2 ★★★★★		▣	▣	▣	Drawing	rdp	ACCEPT	2014-05-23 12:16:34	2014-05-23 12:17:30	00:00:56
6	▶	3 ★★		▣	▣	▣	Drawing	rdp	ACCEPT	2014-05-23 12:16:34	2014-05-23 12:17:30	00:00:56
7	▶	1 ★★		▣	▣	▣	Drawing	rdp	ACCEPT	2014-05-23 12:17:47	2014-05-23 12:18:33	00:00:46
8	▶	2 ★★★★★		▣	▣	▣	Drawing	rdp	ACCEPT	2014-05-23 12:17:47	2014-05-23 12:18:33	00:00:46
9	▶	3 ★★★	▣	▣	▣	▣	Drawing	rdp	ACCEPT	2014-05-23 12:22:05	2014-05-23 12:23:10	00:01:05
10	▶	1 ★★★	▣	▣	▣	▣	Drawing	rdp	ACCEPT	2014-05-23 12:22:05	2014-05-23 12:23:10	00:01:05
11	▶	1 ★★			▣	▣	VNC	vnc	ACCEPT	2014-05-23 18:18:16	2014-05-23 18:18:32	00:00:16
12	▶	1 ★★★			▣	▣	VNC	vnc	ACCEPT	2014-05-23 18:18:35	2014-05-23 18:20:14	00:01:39

Free-text search in audited data

Quick Filtering to find incidents

Hits count & ranking

Export data for further analysis

Full metadata about connections

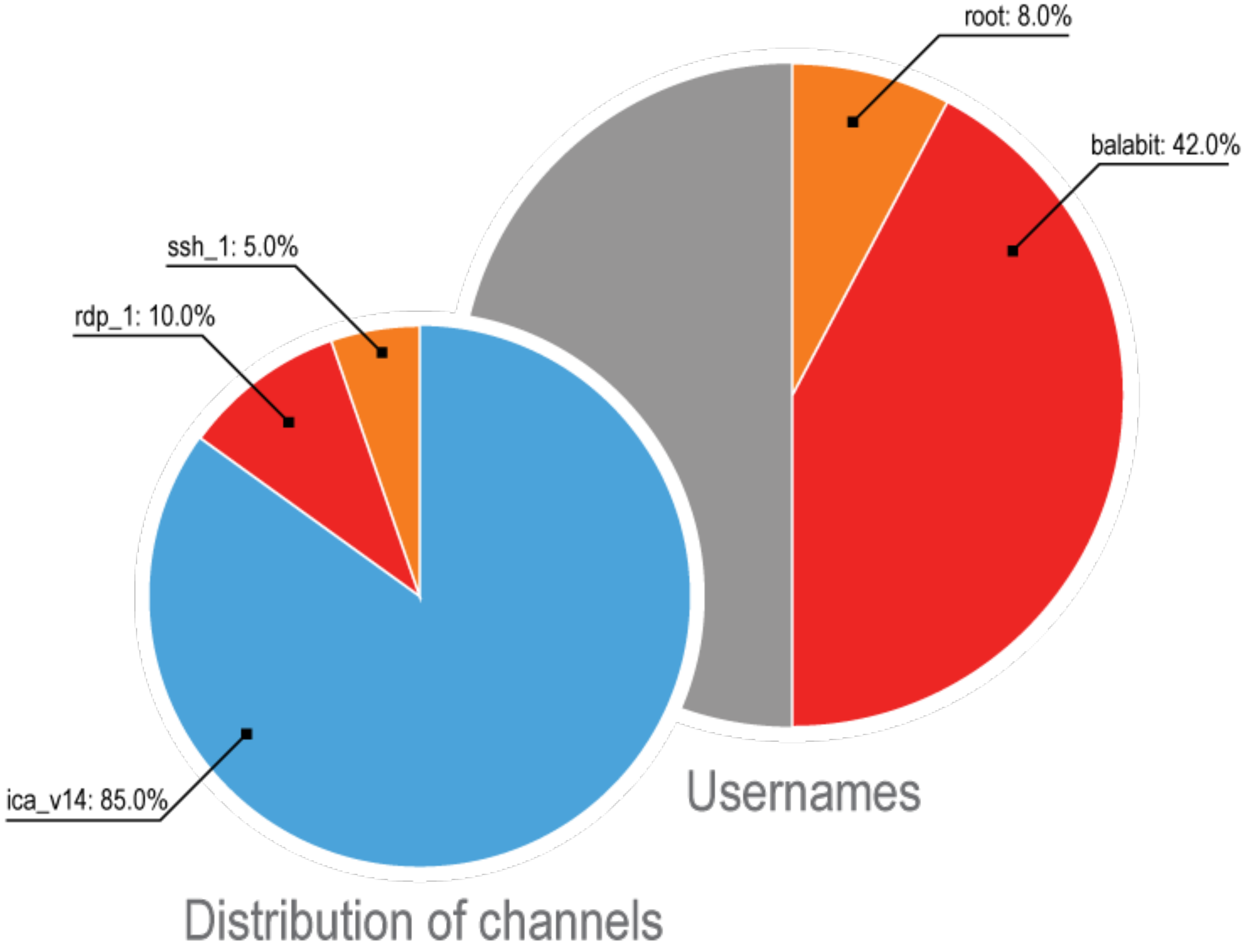
MOVIE-LIKE PLAYBACK OF RECORDED SESSIONS

BALABIT

HOST INDEPENDENT REPORTING

REPORTS ON:

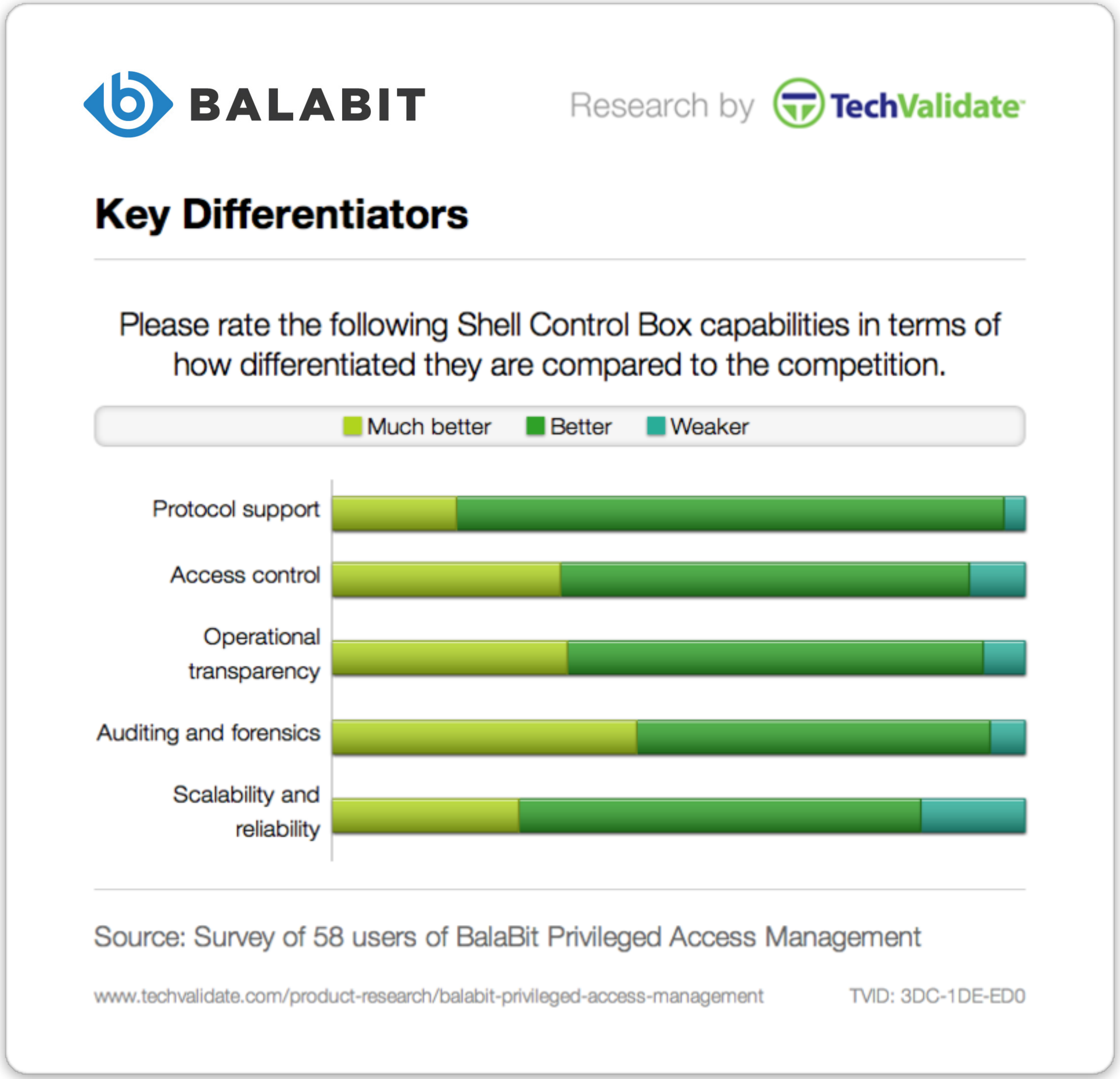
- Usernames,
- Configuration changes,
- Most used commands,
- Privilege escalations,
- Source & destination hosts,
- Access channels,
- Failed logins,
- PCI DSS status, etc.



SEAMLESS ENTERPRISE INTEGRATION

Microsoft Azure
System management
Microsoft Azure
Identity management
Workflow & Ticketing systems
Shell Control Box
Password Management
User Behavior Analytics
SIEM / Log Management
SailPoint
Omada
LIEBERMANSOFTWARE
DELL Software
thycotic
BALABIT
bmc Remedy
servicenow
hp ArcSight
splunk>
syslog-ng STORE BOX
BLINDSPOTTER

UNIQUE CAPABILITIES



BALABIT Research by TechValidate

Key Differentiators

Please rate the following Shell Control Box capabilities in terms of how differentiated they are compared to the competition.

Source: Survey of 58 users of BalaBit Privileged Access Management

www.techvalidate.com/product-research/balabit-privileged-access-management TVID: 3DC-1DE-ED0

BALABIT
SHELL CONTROL BOX

Appliances

LICENSING AND IMPLEMENTATION

- **Pricing based on the number of protected hosts**
- **Provided as an appliance, or a virtual image** (Support of Vmware, MS Hyper-V and Azure)
- **3 HW configurations** (Scalable up to 10TB for auditing „unlimited” hosts)
- **Fast deployment, low OPEX** (Implementation and training: 3-5 days)
- **High Availability option**
- **3 support packages** (Base, Extended, Privileged)
- **Direct, 7/24 vendor support** (option)

APPLIANCES

T1	T4	T10	VA VMware / HyperV
Single QuadCore CPU	Single QuadCore CPU	Dual 6-Core CPU	n/a
8 GB	8 GB	32 GB	n/a
1 TB Software RAID	4 TB Hardware RAID	10 TB Hardware RAID	n/a
	Redundant PSU	Redundant PSU Spare disk	n/a
HA	HA	HA	by virtual infrastructure
10 → 500 Protected Host	10 → 5000 Protected Host	100 → Unlimited Protected Host	10 → Unlimited Protected Host

BALABIT
SHELL CONTROL BOX

Use Cases

MARKET DRIVERS

1

COMPLIANCE

International standards

Local legislation

Company policy

2

SECURITY

Monitor IT staff

Control outsource & cloud admins

Audit terminal services users

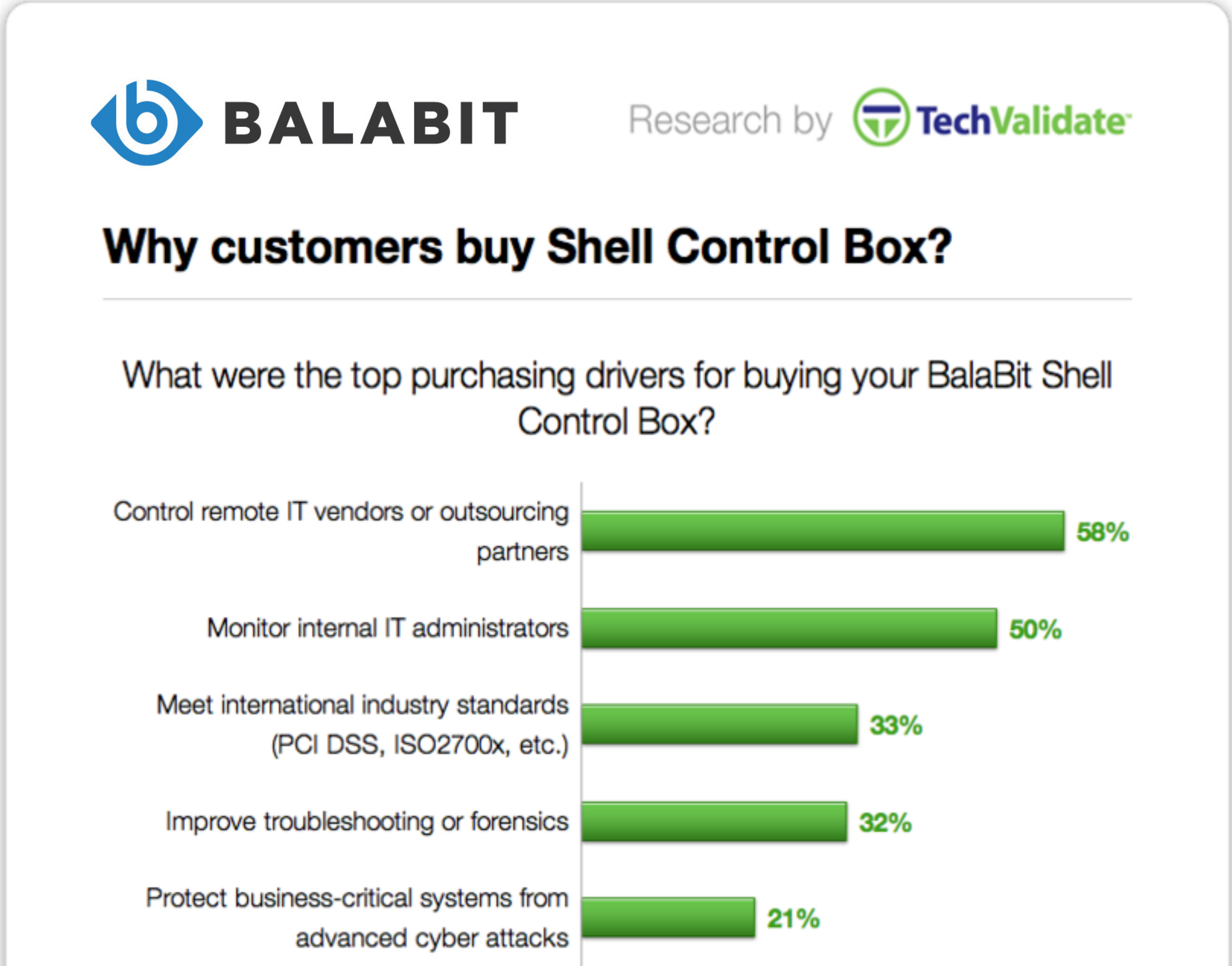
3

OPERATIONAL EFFICIENCY

Fast Troubleshooting & Forensics

Quick audits

KEY CUSTOMER DRIVERS



BALABIT Research by TechValidate

Why customers buy Shell Control Box?

What were the top purchasing drivers for buying your BalaBit Shell Control Box?

USE CASES - COMPLIANCE

Fiducia IT AG

financial IT services provider, Germany

CHALLENGE

Audit admins' access to private banking information to comply with BaFin requirements

SOLUTION

SCB monitors all internal & external administrative access to data center (8,000 UNIX/ Linux servers)

BENEFITS

Smoothly passing supervisory audits

SIA SSB Group

financial provider, Italy

CHALLENGE

Audit access of 200 administrators' to credit card data for PCI DSS compliance

SOLUTION

SCB controls and monitors the administrators' sessions to sensitive servers

BENEFITS

Full compliance with PCI DSS w/o business disruption

Major telecom provider

Major telecommunication provider, Taiwan

CHALLENGE

Audit remote accesses to the 3G network infrastructure for ISO 27011 compliance

SOLUTION

SCB monitors remote access of internal and external network operators

BENEFITS

Full compliance with ISO 27011 and with company access policies.

USE CASES - SECURITY

Bouygues Telecom

CHALLENGE

Centralize & secure administrative access to 18,000 network devices

SOLUTION

Control and monitor SSH and RDP sessions by SCB

BENEFITS

Advanced security of privileged access to critical asstes

Central Bank of Hungary

CHALLENGE

Enhancing the protection of the mission-critical currency-system

SOLUTION

SCB to audit IT operators working in VMware View (thin-client) environment

BENEFITS

Increased accountability of the banking IT staff

Ankara University

Turkey

CHALLENGE

Prevent another data loss on externally managed servers

SOLUTION

SCB to control and monitor remote desktop (RDP) and SSH connections of externally supported servers

BENEFITS

Mitigated risk of data loss in IT outsourcing processes

USE CASES - OPERATIONAL EFFICIENCY

Leading IT services provider

Germany

CHALLENGE

Database update failed due to wrong IT vendor instructions

SOLUTION

Record all actions of database admins by SCB

BENEFITS

By searching & replaying the relevant working session, the provider identified and troubleshooted the problem in hours.

Major mobile provider

Russia

CHALLENGE

The provider's mobile network partially stopped after a junior operator restarted a critical network server

SOLUTION

Record all actions of network operators by SCB

BENEFITS

By replaying the relevant session, the provider identified the problem and restored the network rapidly.

SCB minimized business disruption, revenue loss and reputation damage!

BALABIT
SHELL CONTROL BOX

Target Customers

KEY QUESTIONS TO ANSWER…

01 Are you sure you’d pass audits concerning user monitoring?

02 Can you reliably control your outsourcing partners?

03 Can you monitor the actions of your „superusers”?

04 Can you ensure the accountability of your staff?

05 Do you really know „who did what” on your key servers?

TELECOMMUNICATIONS

Protecting client and billing data

Several types of sensitive data (e.g. call data records or web traffic)

Great need for business continuity

Thousands of networking devices managed by countless operators

Fast resolution of network problems and accountability issues

Security Risk of Third-parties

Nation-wide impact of cyber-attacks

Critical national infrastructure, as targets of cyber-terrorists

CLOUD- AND MANAGED SERVICE PROVIDERS

Strict measures to keep reputation

Proactive, special security precautions

Accountability issues

Transparent and auditable IT mgt. to prevent „blame-games”

SLA verification

Justify KPIs and billable actions

Compliance challenges

Client data protection - PCI DSS (Cloud Computing Guides), CSA, ISAE 3402, etc.

FINANCE

Increasing risk of fraud & cyber-attacks

Banks as largest targets for cyber-criminals

Great regulatory pressure

Strict internal IT security policies,
Basel III, MiFID II, SOX, PCI DSS…

Complex IT organizations

Large, distributed data centers managed by hundreds of admins

Difficulties of controlling 3rd parties

GOVERNMENT

Cyber espionage & APT attacks

Advanced security to prevent national security incidents

Regulatory pressure

National laws and acts, such as HIPAA or NIST SP 800-53

Managing 3rd parties

Protection of personal records from external providers

OTHER INDUSTRIES

Public utility services

Manufacturing firms

Large retailers

Enterprises with extensive network

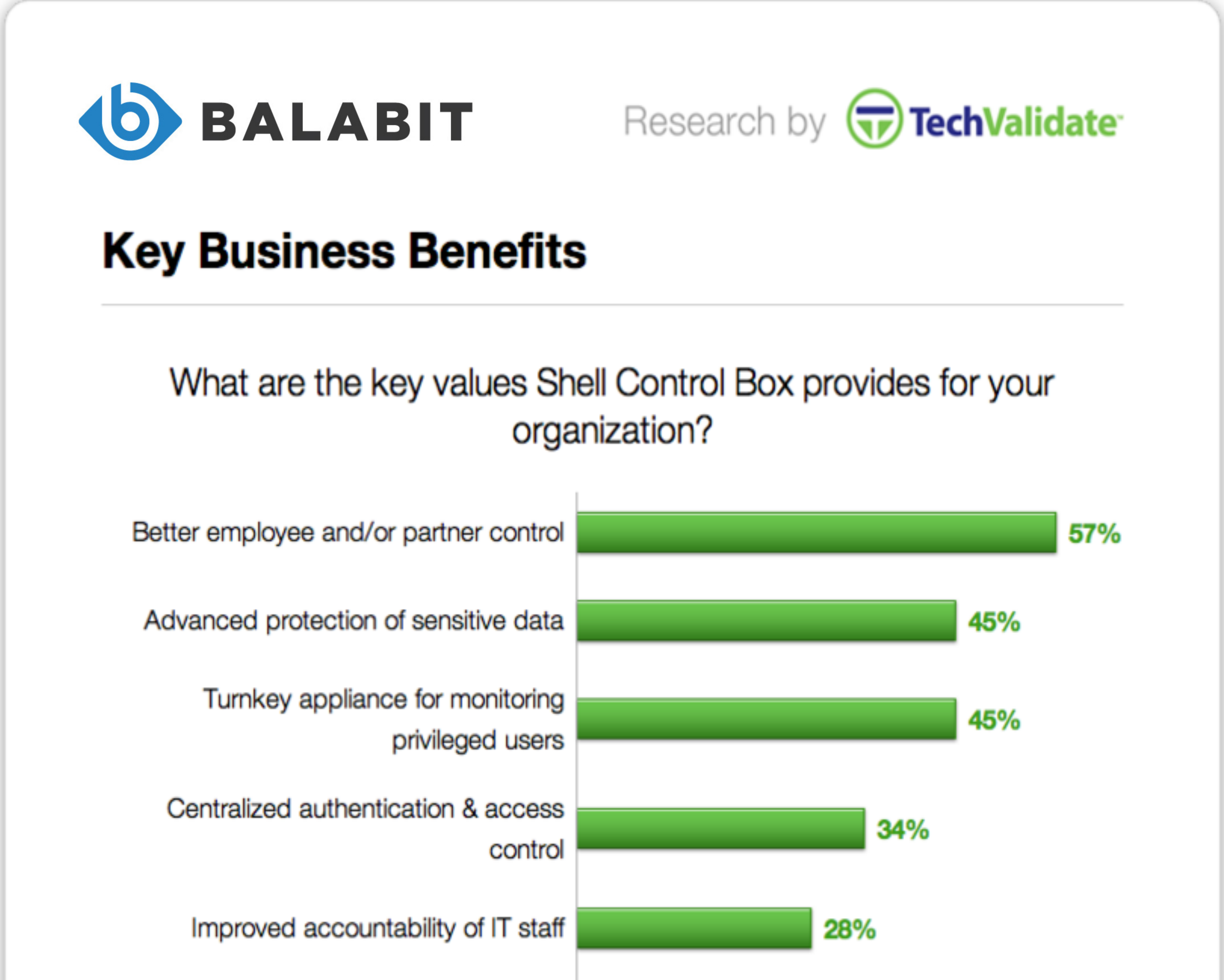
Enterprises using IT outsourcing

Enterprises with high security standards

BALABIT SHELL CONTROL BOX

Customer Benefits

BENEFITS



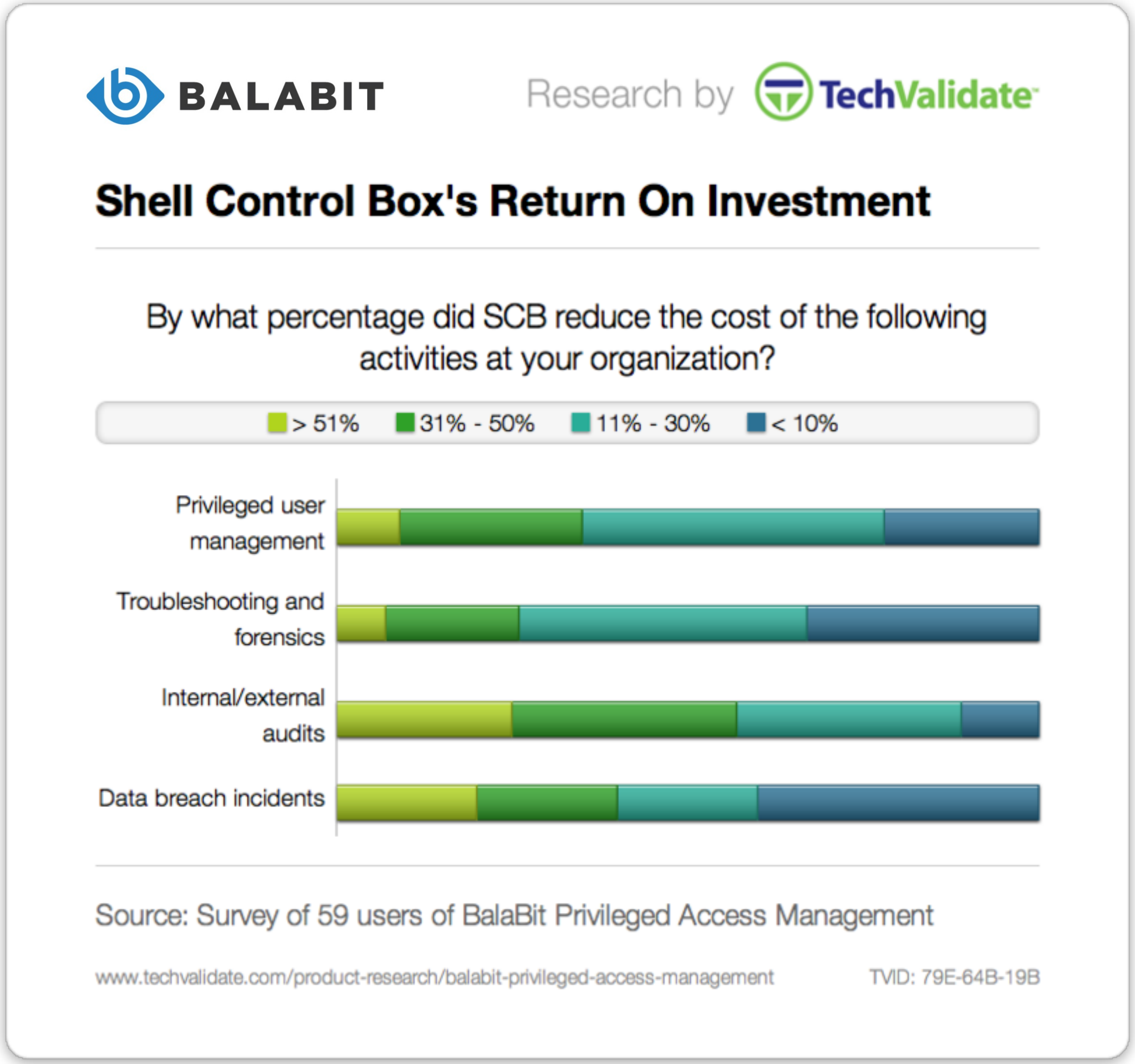
BALABIT

Research by TechValidate

Key Business Benefits

What are the key values Shell Control Box provides for your organization?

ROI



BALABIT Research by TechValidate

Shell Control Box's Return On Investment

By what percentage did SCB reduce the cost of the following activities at your organization?

Source: Survey of 59 users of BalaBit Privileged Access Management

www.techvalidate.com/product-research/balabit-privileged-access-management TVID: 79E-64B-19B

TESTIMONIALS

„Balabit SCB is the only serious product on the market that is capable of securely monitoring SSH sessions”

Øyvind Gielink, IT security Officer, Telenor

„ Balabit is the first company in IT business, which provided a solution in promised time...”

Michael Fendt, System & Network Engineer, Fiducia IT

„ SCB is a core component of Alfa Bank’s new Information Security Strategy.“

Andrey Fedotov, Head of IT Security, Alfa Bank

ANALYST QUOTES

„ Balabit offers industrial strength session monitoring and recording.”

Andras Cser, Vice President, Principal Analyst, Forrester Research

„ Adding third party capabilities such as privileged session management (PSM) can sometimes offer a more suitable solution at a lower price than a suite offering.”

Felix Gaehtgens, Research Director, Gartner

„ Bringing together [user] monitoring and recording is very important to have the context of when did someone do what.”

Martin Kuppinger, Founder and Principal Analyst, KuppingerCole

BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

Thank you for your attention!

Contextual security today

More information: www.balabit.com