Securing Privileged Access Across the Hybrid Enterprise

Vedran Pauk

29.03.2017

Your organization can't afford a large-scale cyber-attack

28,070

Number of attacks the average US company had in 2015

38%

Increase in # of security incidents from 2014 to 2015

3.9B

Number of records lost since 2013

What's the common thread in most if not all breaches?

Compromised accounts and credentials of ….

Privileged Users

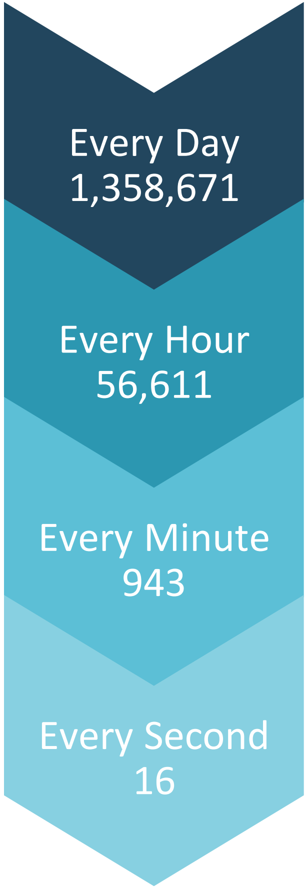
94%

Percentage of CxOs believing their company will experience a breach in two years

$3.79M

Average cost of a data breach

Data records were lost or stolen with the following frequency



Every Day
1,358,671

Every Hour
56,611

Every Minute
943

Every Second
16

http://breachlevelindex.com/#sthash.RZhGQkVZ.dpbs
https://securityintelligence.com/cost-of-a-data-breach-2015/
http://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03074usen/SEL03074USEN.PDF
http://www.vormetric.com/campaigns/datathreat/2016/
http://www.verizonenterprise.com/resources/report/rp_pci-report-2015_en_xg.pdf

But the reality is … The risks are greater than ever

CYBERCRIME

- Experian —15 million individuals' records stolen
- Home Depot—56 million credit cards stolen
- JP Morgan Chase—76 million account records stolen
- Ashley-Madison – 37 million customer records stolen
- OPM – 22 million government employee records stolen

CYBERESPIONAGE

- Anthem—80 million personal records stolen
- Forbes.com and unidentified health insurer—targeted (defense contractors, government workers) information gathering of individual data

BUSINESS IMPACT

- Sony Pictures—extensive disruption
- German Steel Mill—physical damage
- Saudi Aramco—physical systems damage and business disruption

And the financial impact is staggering

$300 Billion

GDP of Singapore

$3 Trillion

Global Economic Impact of Cybercrime in 10 Years

- McKinsey, World Economic Forum

$300 Billion

Global Drug Trafficking Revenue

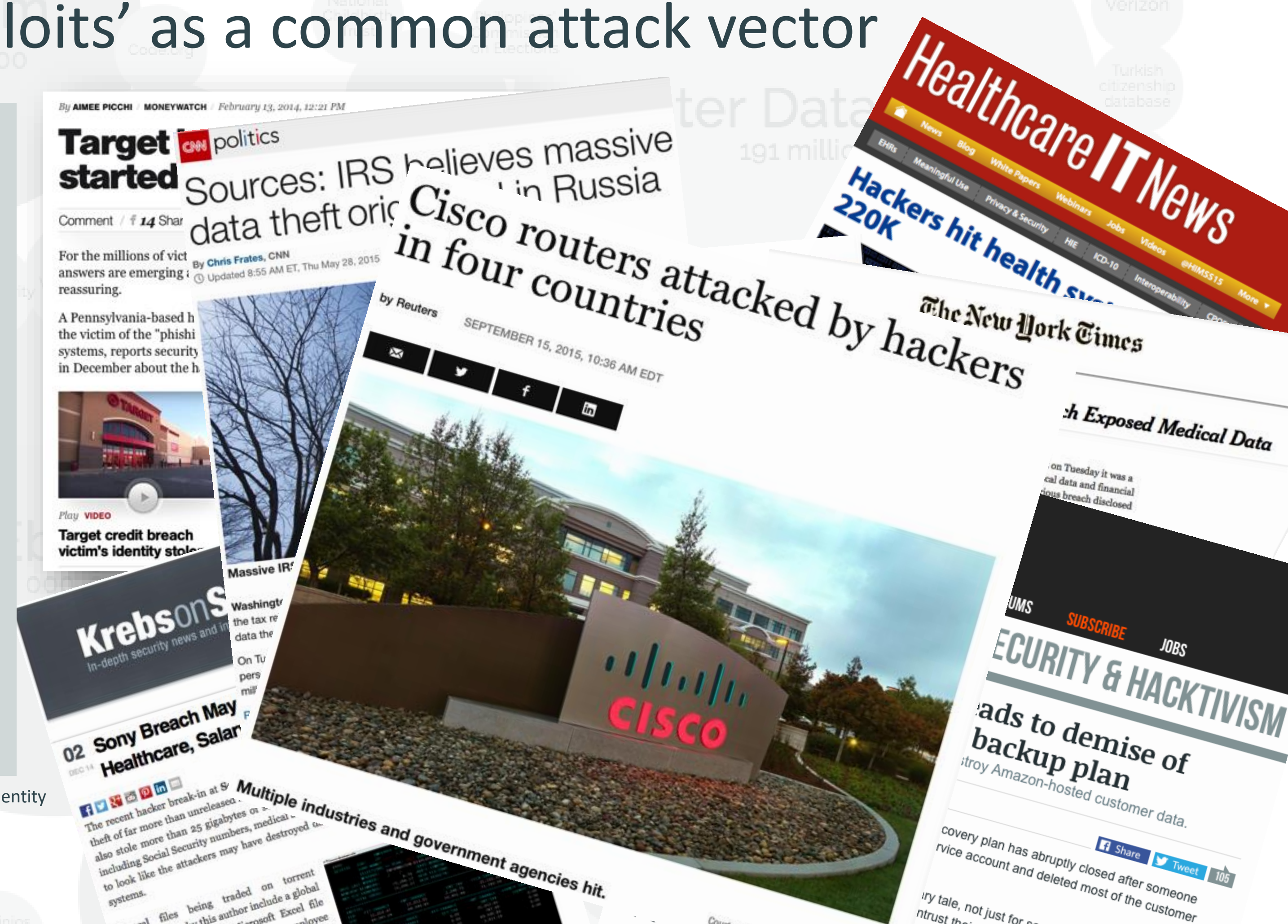
Net Losses: Estimating the Global Loss of Cybercrime (Intel Security – June 2014). Cybercrime is a growth industry. The returns are great, and the risks are low. We estimate that the annual cost to the global economy from cybercrime is more than $400 billion. A conservative estimate would be $375 billion in losses, while the maximum could be as much as $575 billion. Even the smallest of these figures is more than the national income of most countries and governments and companies underestimate how much risk they face from cybercrime and how quickly this risk can grow.

‘Privilege exploits’ as a common attack vector

The frequency and severity of breaches are increasing

> “For digital businesses, privileged identity management becomes both incredibly important and challenging. It’s important because one administrator with malicious intent or the theft of administrator credentials can have a disastrous effect on your customers, revenues and long-term reputation.”
>
> *- Forrester Research*

“Critical Questions To Ask Your Privileged Identity Management Solution Provider", Forrester Research, September 9, 2014.



By AIMEE PICCHI / MONEYWATCH / February 13, 2014, 12:21 PM

Target i... started

Comment / 14 Shar

For the millions of vict... answers are emerging ... reassuring.

A Pennsylvania-based h... the victim of the "phishi... systems, reports security... in December about the h...

Play VIDEO

Target credit breach victim's identity stol...

CNN politics

Sources: IRS believes massive data theft orig... in Russia

By Chris Frates, CNN
Updated 8:55 AM ET, Thu May 28, 2015

Massive IR...

Washingt... the tax re... data the...

On Tu... pers... mil...

Cisco routers attacked by hackers in four countries

by Reuters
SEPTEMBER 15, 2015, 10:36 AM EDT

Multiple industries and government agencies hit.

Healthcare IT News

News Blog White Papers Webinars Jobs Videos @HIMSS15 More

EHRs Meaningful Use Privacy & Security HIE ICD-10 Interoperability

Hackers hit health sys... 220K

The New York Times

...h Exposed Medical Data

...on Tuesday it was a ...cal data and financial ...ous breach disclosed

KrebsonS...
In-depth security news and in...

02 DEC 14 Sony Breach May... Healthcare, Salar...

The recent hacker break-in at S... theft of far more than unreleased... also stole more than 25 gigabytes o... including Social Security numbers, medical... to look like the attackers may have destroyed... systems.

...l files being traded on torrent ... by this author include a global ... Microsoft Excel file ... mployee

...UMS SUBSCRIBE JOBS

SECURITY & HACKTIVISM

...ads to demise of backup plan

...troy Amazon-hosted customer data.

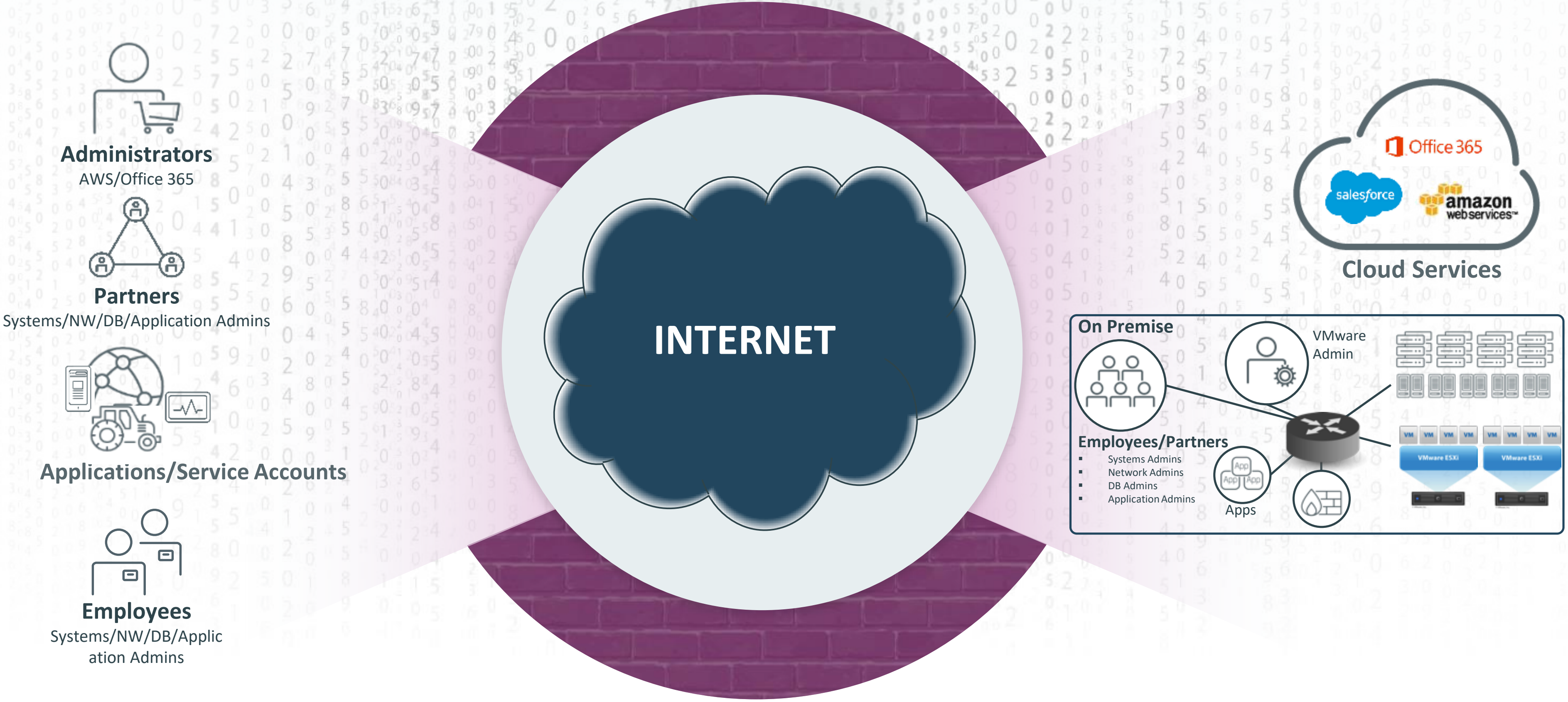
Share Tweet 105

...covery plan has abruptly closed after someone ...rvice account and deleted most of the customer

...ry tale, not just for ... ntrust th...

You can’t protect what you don’t know

The many forms of privileged accounts



Administrators
AWS/Office 365

Partners
Systems/NW/DB/Application Admins

Applications/Service Accounts

Employees
Systems/NW/DB/Application Admins

INTERNET

Cloud Services

On Premise

VMware Admin

Employees/Partners

- Systems Admins
- Network Admins
- DB Admins
- Application Admins

Apps

What can you do to address the threat?

Prevent breaches by protecting administrative credentials, controlling privileged user access, and monitoring and recording privileged user activity across the hybrid enterprise.

Break the Attack Kill Chain with Privileged Access Management (PAM)

Prevent Unauthorized Access

- Strong authentication
- Login restriction
- Automated behavior analytics and threat detection

Limit Privileged Escalation

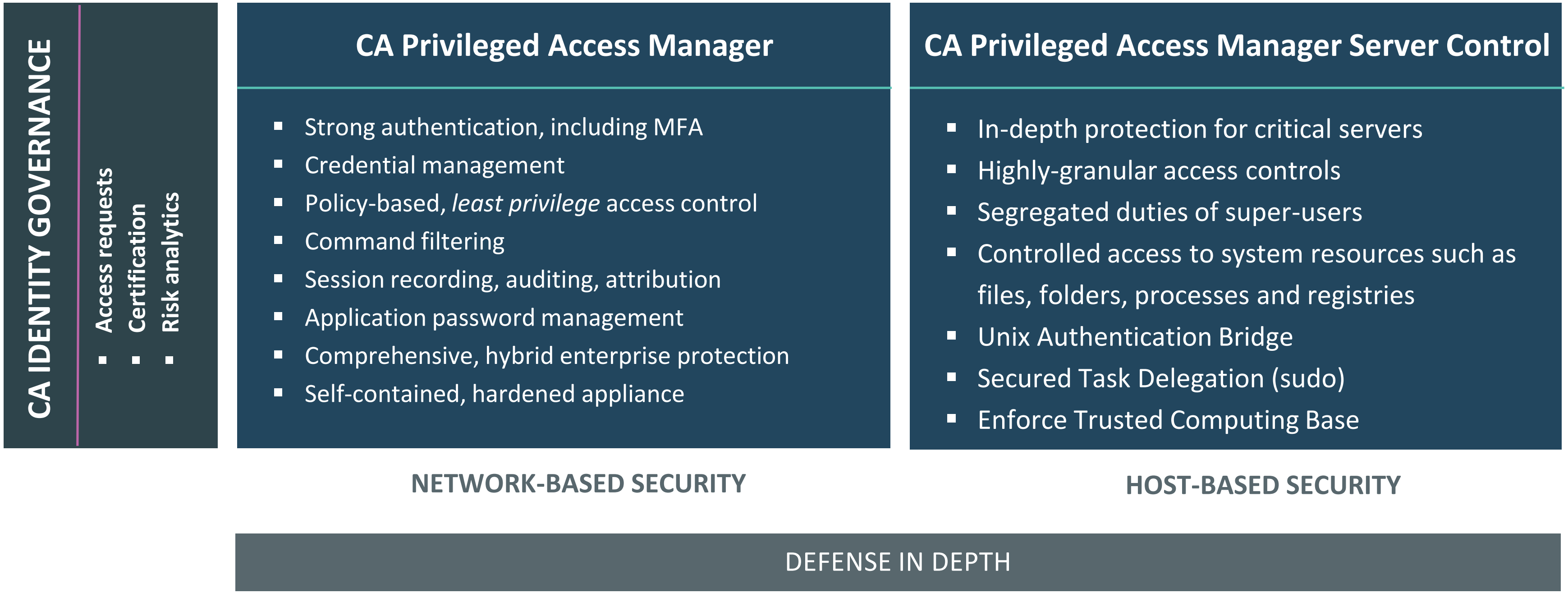
- Command & socket filtering
- Zero trust – deny all, permit by exception
- Proactive policy enforcement

Monitor, record & audit activity

- Session recording & monitoring
- Activity logging & auditing
- SIEM integration

How CA Technologies can help

Delivering comprehensive Privileged Access Management solutions



CA IDENTITY GOVERNANCE

- Access requests
- Certification
- Risk analytics

CA Privileged Access Manager

- Strong authentication, including MFA
- Credential management
- Policy-based, *least privilege* access control
- Command filtering
- Session recording, auditing, attribution
- Application password management
- Comprehensive, hybrid enterprise protection
- Self-contained, hardened appliance

CA Privileged Access Manager Server Control

- In-depth protection for critical servers
- Highly-granular access controls
- Segregated duties of super-users
- Controlled access to system resources such as files, folders, processes and registries
- Unix Authentication Bridge
- Secured Task Delegation (sudo)
- Enforce Trusted Computing Base

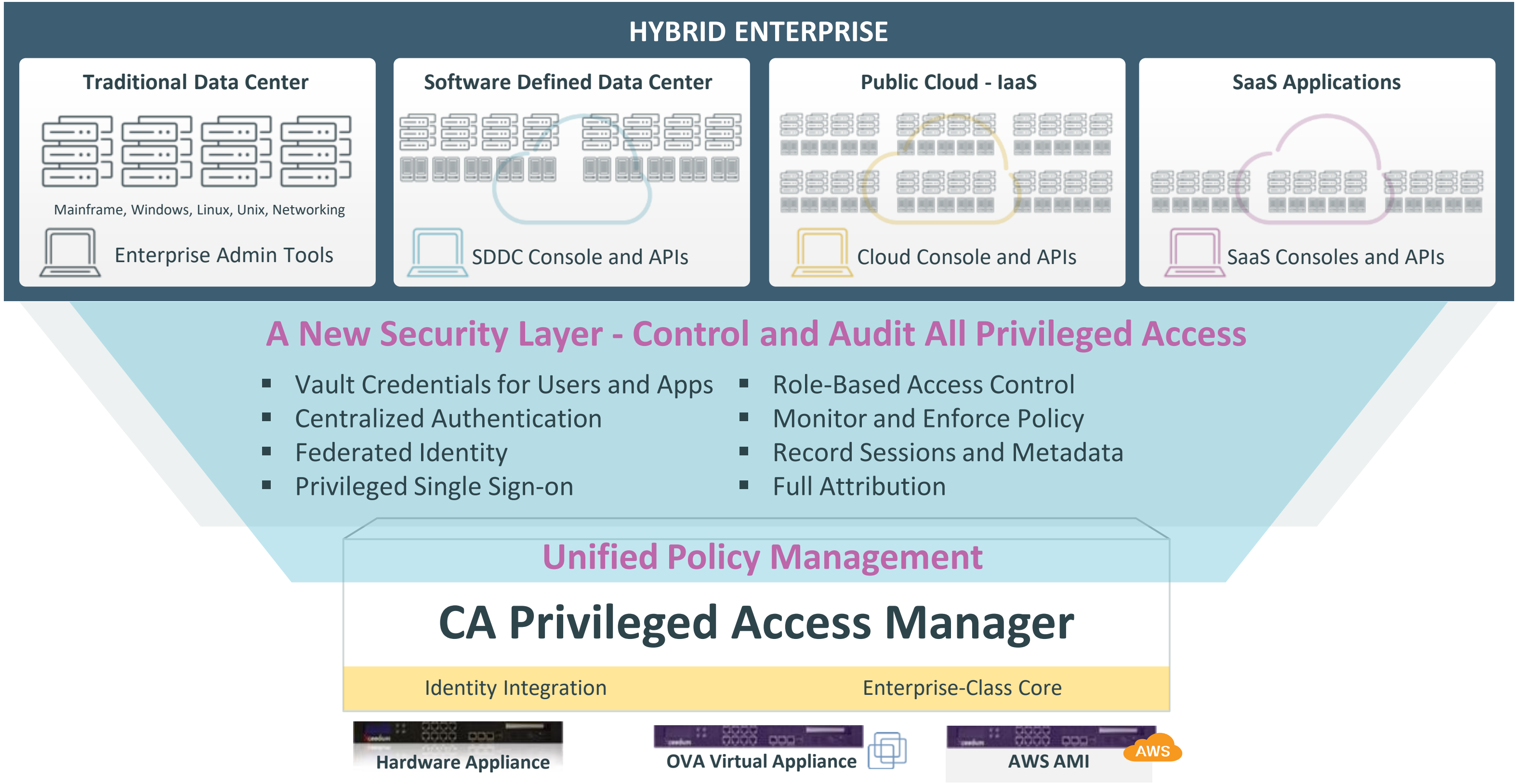
NETWORK-BASED SECURITY

HOST-BASED SECURITY

DEFENSE IN DEPTH

CA Privileged Access Manager

Privileged Account Management for the Hybrid Enterprise



HYBRID ENTERPRISE

Traditional Data Center

Mainframe, Windows, Linux, Unix, Networking

Enterprise Admin Tools

Software Defined Data Center

SDDC Console and APIs

Public Cloud - IaaS

Cloud Console and APIs

SaaS Applications

SaaS Consoles and APIs

A New Security Layer - Control and Audit All Privileged Access

- Vault Credentials for Users and Apps
- Centralized Authentication
- Federated Identity
- Privileged Single Sign-on
- Role-Based Access Control
- Monitor and Enforce Policy
- Record Sessions and Metadata
- Full Attribution

Unified Policy Management

CA Privileged Access Manager

Identity Integration

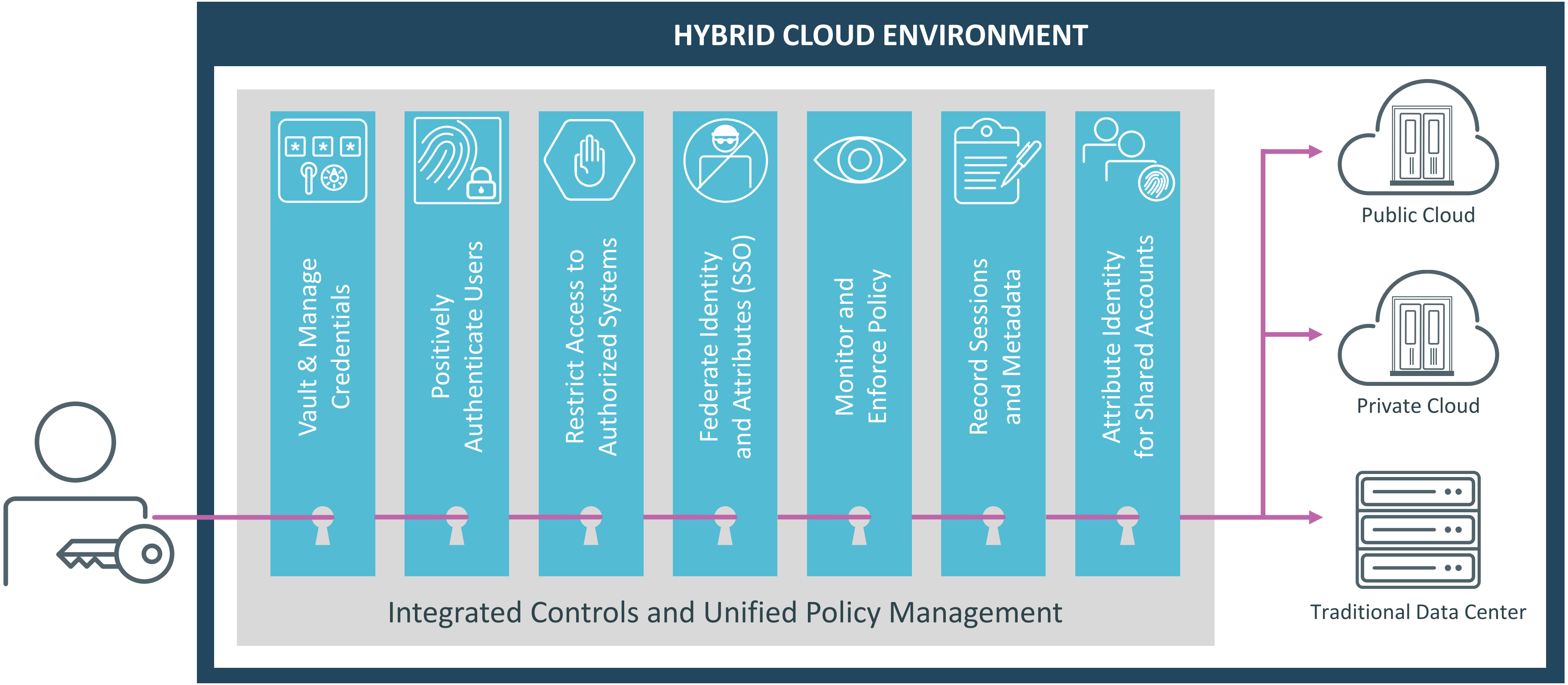
Enterprise-Class Core

Hardware Appliance

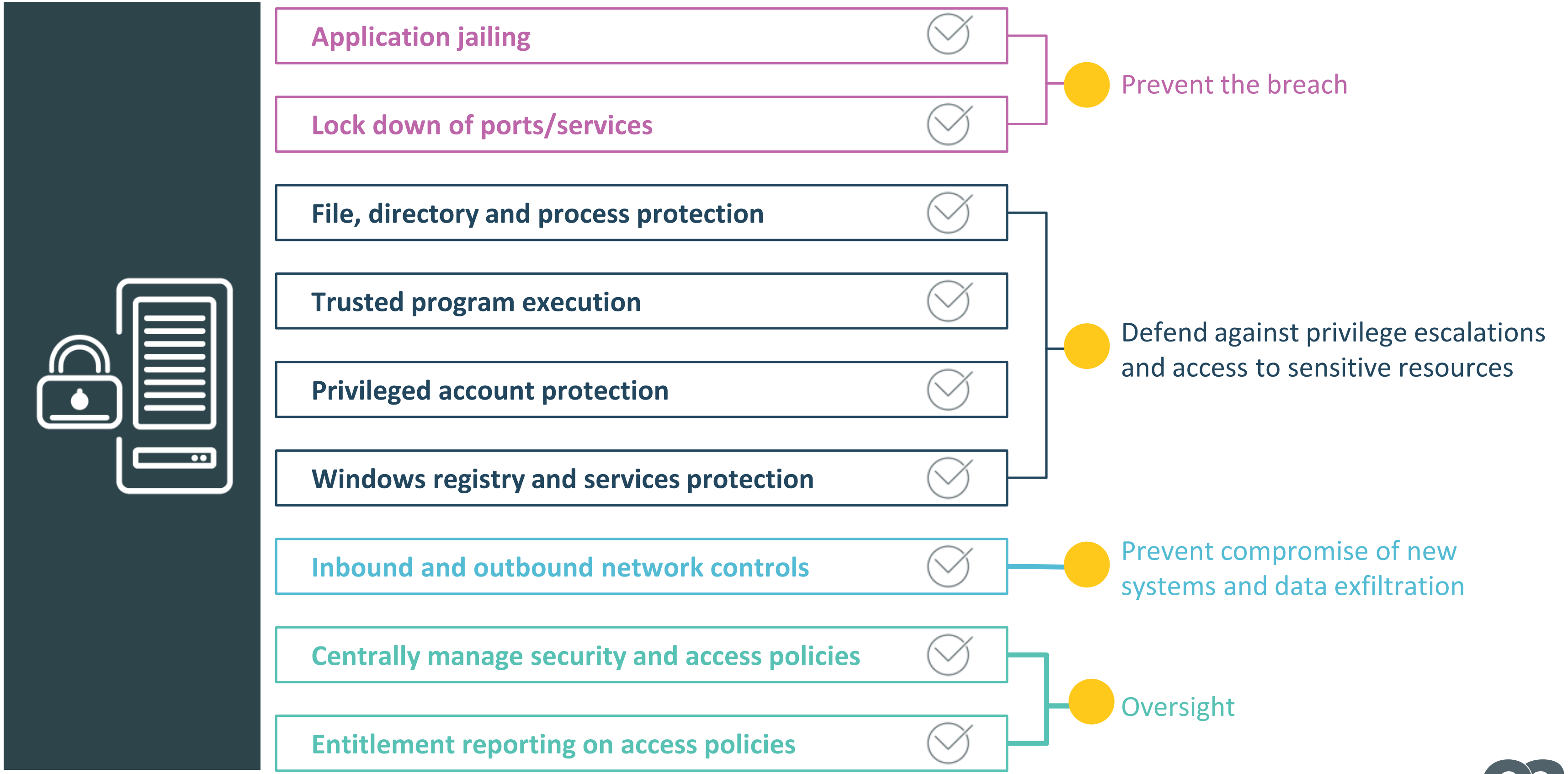
OVA Virtual Appliance

AWS AMI

CA Privileged Access Manager in action


HYBRID CLOUD ENVIRONMENT
Vault & Manage Credentials
Positively Authenticate Users
Restrict Access to Authorized Systems
Federate Identity and Attributes (SSO)
Monitor and Enforce Policy
Record Sessions and Metadata
Attribute Identity for Shared Accounts
Integrated Controls and Unified Policy Management
Public Cloud
Private Cloud
Traditional Data Center

CA Privileged Access Manager Server Control



- Application jailing ✓
- Lock down of ports/services ✓

Prevent the breach

- File, directory and process protection ✓
- Trusted program execution ✓
- Privileged account protection ✓
- Windows registry and services protection ✓

Defend against privilege escalations and access to sensitive resources

- Inbound and outbound network controls ✓

Prevent compromise of new systems and data exfiltration

- Centrally manage security and access policies ✓
- Entitlement reporting on access policies ✓

Oversight

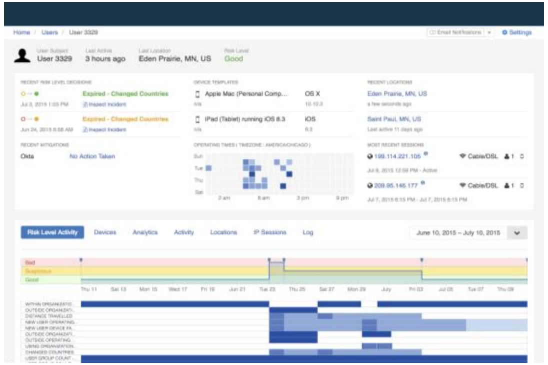
ca technologies

Threat Analytics for PAM

Advanced Behavior Analytics and Automated Mitigation

Advanced Capabilities

- **Automated detection, mitigation and alerting** for critical threats that complements existing PAM, SIEM and SOC workflows and provide continuous intelligent monitoring
- **Advanced behavior analytics** enable enterprise to detect attacks using same approach used by banks to defeat credit card fraud - using historic and real-time activity to assess context and analyze risk
- **Integrated risk mitigations and controls,** including triggering session recording and re-authentication, close the door on insiders and attackers.



Home / Users / User 3329

User Subject: User 3329 | Last Active: 3 hours ago | Last Location: Eden Prairie, MN, US | Risk Level: Good

RECENT RISK LEVEL DECISIONS

Expired - Changed Countries — Jul 3, 2015 1:33 PM — Inspect Incident

Expired - Changed Countries — Jun 24, 2015 8:58 AM — Inspect Incident

DEVICE TEMPLATES

Apple Mac (Personal Comp... — OS X 10.10.3

iPad (Tablet) running iOS 8.3 — iOS 8.3

RECENT LOCATIONS

Eden Prairie, MN, US — a few seconds ago

Saint Paul, MN, US — Last active 11 days ago

RECENT MITIGATIONS

Okta — No Action Taken

OPERATING TIMES (TIMEZONE : AMERICA/CHICAGO)

MOST RECENT SESSIONS

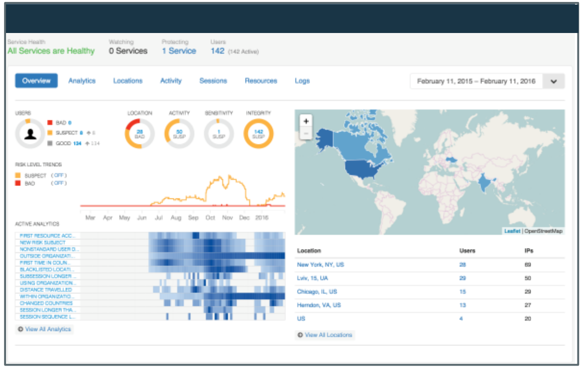
199.114.221.105 — Cable/DSL — 1 — Jul 8, 2015 12:59 PM - Active

209.95.146.177 — Cable/DSL — 1 — Jul 7, 2015 6:15 PM - Jul 7, 2015 6:15 PM

June 10, 2015 – July 10, 2015

Compelling Benefits

- **Reduced risk** - automated analytics provide both threat detection and contextual rich view of user behavior.
- **Meaningful insight** - simplifies risk mitigation, incident response and compliance provided via context rich user interfaces that expose and make it easy to access information regarding user, events and system activities.
- **Quick time-to-value -** Immediately delivers compelling user experience with human-understandable risk and insights
- **Easy deployment -** Deploys as single, virtual machine—no special skills or significant effort required



Service Health: All Services are Healthy | Watching: 0 Services | Protecting: 1 Service | Users: 142 (142 Active)

February 11, 2015 – February 11, 2016

USERS: BAD 0 · SUSPECT 8 · GOOD 134

RISK LEVEL TRENDS: SUSPECT (OFF) · BAD (OFF)

ACTIVE ANALYTICS

FIRST RESOURCE ACC...
NEW RISK SUBJECT
NONSTANDARD USER D...
OUTSIDE ORGANIZATI...
FIRST TIME IN COUN...
BLACKLISTED LOCATI...
SUBSESSION LONGER ...
USING ORGANIZATION...
DISTANCE TRAVELLED
WITHIN ORGANIZATIO...
CHANGED COUNTRIES
SESSION LONGER THA...
SESSION SEQUENCE L...

View All Analytics

Location	Users	IPs
New York, NY, US	28	69
Lviv, 15, UA	29	50
Chicago, IL, US	15	29
Herndon, VA, US	13	27
US	4	20

View All Locations

What others are saying

"CA Technologies is a Market Leader in Identity and Access Management, with a strong footprint in Privileged Management."

Source: KuppingerCole Report Leadership Compass (Privilege Management) 2015

KuppingerCole Report

LEADERSHIP COMPASS

by M. Kuppinger & A. Singh | December 2015

Testimonial

"With CA Privileged Access Manager, we have ***greater visibility*** into the activities of our privileged users. In addition, we have ***significantly reduced our risks*** from insider threats." - Michael Nawrocki, Senior IT Architect, Telesis Corporation

Testimonial

"The **access control component is solid**. It **adds another layer of security** from the basic OS security of Linux and Windows." - Quote from a review of CA Privileged Access Manager via IT Central Station

TECHVALIDATE RESULTS

- **86%** of surveyed IT organizations have significantly improved their confidence in protecting against breaches with CA Privileged Access Manager
- **88%** of surveyed IT organizations were able to reduce security and compliance risks by more than 50% with CA Privileged Access Manager
- **90%** of surveyed IT organizations addressed audit and compliance demands associated with controlling and managing privileged access with CA Privileged Access Manager

Case Study: Global Service Provider

This global service provider is the outsourcer for one of Switzerland's largest financial services firms. The company is part of an $8 billion global organization with 66,000 employees operating in 60 countries – leading their clients on their digital transformation journey, providing innovative next-generation technology solutions and services that leverage deep industry expertise, global scale, technology independence and an extensive partner community.

CHALLENGES

- **Breach prevention** – ensuring the integrity and safety of sensitive corporate data from both external and internal threats
- **Audit and compliance** – satisfying compliance requirements from multiple standards/directives
- **Business continuity and customer satisfaction** – prevent admin errors/fraud that can lead to system outages and SLA violations
- **Protection of outsourcing and cloud services** – protect complex hybrid IT environment from exploits of privileged credentials

SOLUTIONS

Selected CA Privileged Access Manager to:

- Centrally **manage and enforce 'least privilege'** access control policies e.g. restrict offshore admin access only to specific systems/data
- **Monitor and record privileged user activity** e.g. enforce command filtering rules, while monitoring for alerts/policy violations
- Implement controls **to audit, report and monitor** privileged user access to satisfy both internal and external audit and compliance requirements

ENTERPRISE-CLASS SCALABILITY

Implementing CA Privileged Access Manager initially on 3,000 target systems in Switzerland – with the goal of expanding onto other servers globally. With the CA Privileged Access Manager implementation, this organization expects the following results:

- **Reduce the risk of data breach** by restricting privileged access rights to minimum requirements
- **Achieve and maintain compliance** w/multiple standards and directives including:ISO27xxx, SAS70/SSAE16, KonTraG, BDSG, GoBS etc
- **Reduce the risk of system outages** and/or SLA violation by controlling administrator access and monitoring their activity to prevent misuse
- **Improved enterprise-wide security** by enforcing access policies across the entire complex hybrid enterprise consisting of traditional data center, virtualized and cloud environments

Case Study: Telecommunications Titan

This organization is one of the world's leading providers of digital television entertainment services delivering a premium video experience through state-of-the-art technology, unmatched programming, and industry leading customer service to more than 37 million customers in the U.S. and Latin America.

CHALLENGES

- **Compliance readiness** – increasing pressure to comply with internal policies and external standards and regulations; needing a more efficient way of centrally controlling and managing privileged user access to various servers, devices, and applications
- **Targeted attack prevention** – Growing external threats call for better controls around privileged access management – more specifically for privileged password management, least privilege access controls, activity reporting, and cross-platform authentication bridging
- **Insider threat mitigation** – Addressing continued risk of super user account misuse, while ensuring effective performance of system administrative tasks

SOLUTIONS

Leveraging CA Privileged Access Management as a control to address their security and compliance related challenges – particularly by leveraging the following capabilities:

- **Activity auditing and monitoring** – centralized logging and session recording of privileged user activity
- **Fine-grained access control** – SoD & comprehensive access control policy definition & enforcement preventing both insider and external threats
- **Application to application credential management** – elimination of hardcoded passwords within application codes
- **Hybrid enterprise protection** – enforcing strong credentials management across on-premises, virtual & cloud environments

ENTERPRISE-CLASS SCALABILITY

Implementing CA Privileged Access Management solutions initially on 7,500 target systems with the following expected results:

- **Reduce the risk of breaches and attacks** by enforcing powerful privileged access control – helping prevent brand damage, loss of IP and revenue loss/recovery cost from breaches
- **Satisfy compliance demands** by auditing and monitoring administrator activity – helping prevent financial losses stemming from compliance violations and fines
- **Reduce the risk of insider threats** by increasing privileged user accountability
- **Standardize security across the hybrid enterpirse** by enforcing the same high-standard access control policies on various on-premises environments, along with virtualized and cloud environments as well

WHY CA?

CA PRIVILEGED ACCESS MANAGEMENT delivers …

ENTERPRISE-CLASS SCALABILITY

- Single appliance protecting thousands of resources
- Supports a large number of concurrent sessions – at no additional costs

QUICK TIME TO VALUE/PROTECTION

- Installs in hours not weeks or months
- Easy to install, configure, maintain, upgrade and manage

DEFENSE-IN-DEPTH PROTECTION

- Comprehensive PAM solution in both network and host based form factors
- Supports physical, virtual and cloud environments
- Threat Analytics help reduce the threat of breach

Legal

This document is for your informational purposes only. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "as is" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised in advance of the possibility of such damages.

CA does not provide legal advice. Neither this document nor any CA software product referenced herein shall serve as a substitute for your compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, policy, standard, guideline, measure, requirement, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. You should consult with competent legal counsel regarding any Laws referenced herein.

Q&A