Privileged Access Management

Breaking the Kill Chain

August 2018

For Informational Purposes Only

Terms of this Presentation

Copyright © 2018 CA, Inc. All rights reserved. All marks used herein may belong to their respective companies. This document does not contain any warranties and is provided for informational purposes only. Any functionality descriptions may be unique to the customers depicted herein and actual product performance may vary.

The views expressed in this presentation are those of the author(s) and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the U.S. Government.

Copyright © 2018 CA, Inc. All rights reserved.

Agenda

1. KEY FINDINGS OF INSIDER THREATS REPORT
2. NATURE OF INSIDER THREAT
3. THE IMPACT OF INSIDER THREAT
4. THE SOLUTION: PRIVILEGED ACCESS MANAGEMENT
5. 5 WAYS PAM BREAKS THE KILL CHAIN
6. WHY CA TECHNOLOGIES

Copyright © 2018 CA, Inc. All rights reserved.

Key Finding: Most feel vulnerable to insider threats

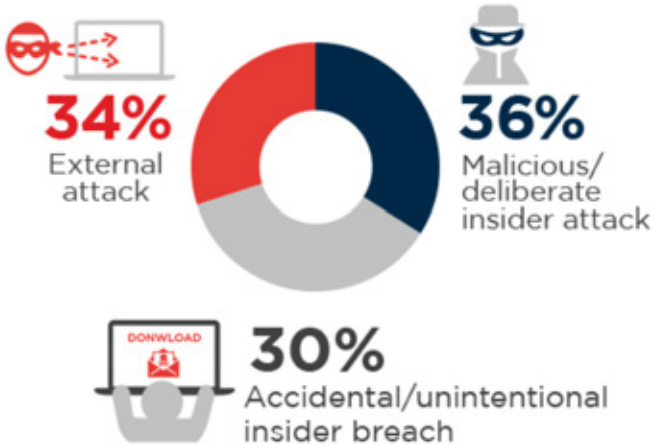
Copyright © 2018 CA, Inc. All rights reserved.

Key Finding: How effective are your controls?

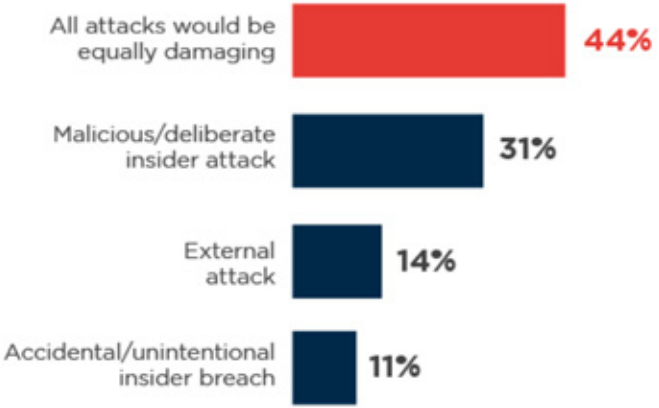
Copyright © 2018 CA, Inc. All rights reserved.

Nature of Threat: Who poses the biggest threat?

Q: What threat do you consider most LIKELY to happen to your organization?



Q: What threat do you consider more DAMAGING to your organization?



44% increase in reported data breaches from 2016 to 2017[1]

Copyright © 2018 CA, Inc. All rights reserved.

1. 2017 Verizon Breach Report

Nature of Threat: Which users are riskiest?

Q: What type(s) of insiders pose the biggest security risk to organizations?*

56%
Regular employees

55%
Privileged IT users/admins

42%
Contractors/service providers/ temporary workers

Privileged business users/ executives

Customers/ clients

None

Not sure/ other

*Multi-response questions do not add up to 100%

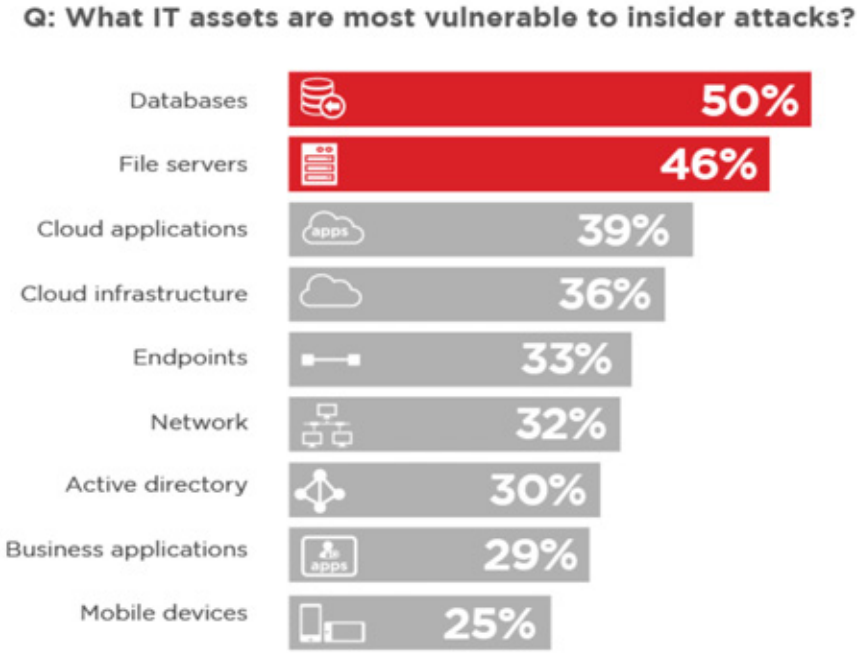
Copyright © 2018 CA, Inc. All rights reserved.

Nature of Threat: What data are they trying to steal?

Copyright © 2018 CA, Inc. All rights reserved.

1. 2017 Verizon Breach Report

Nature of Threat: Which systems are most vulnerable?

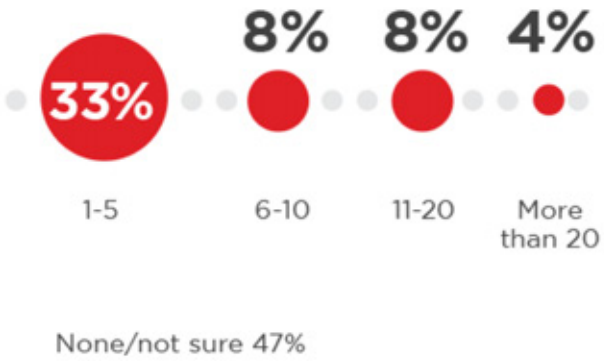


Copyright © 2018 CA, Inc. All rights reserved.

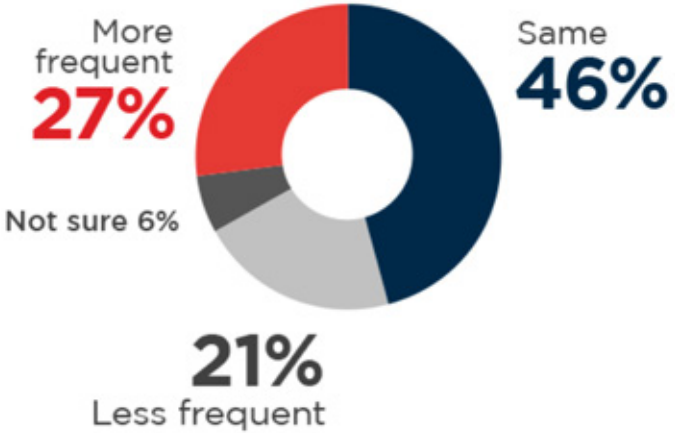
1. 2017 Verizon Breach Report

Impact of Threat: Is the threat real or not?

Q: How many insider attacks did your organization experience in the last 12 months?



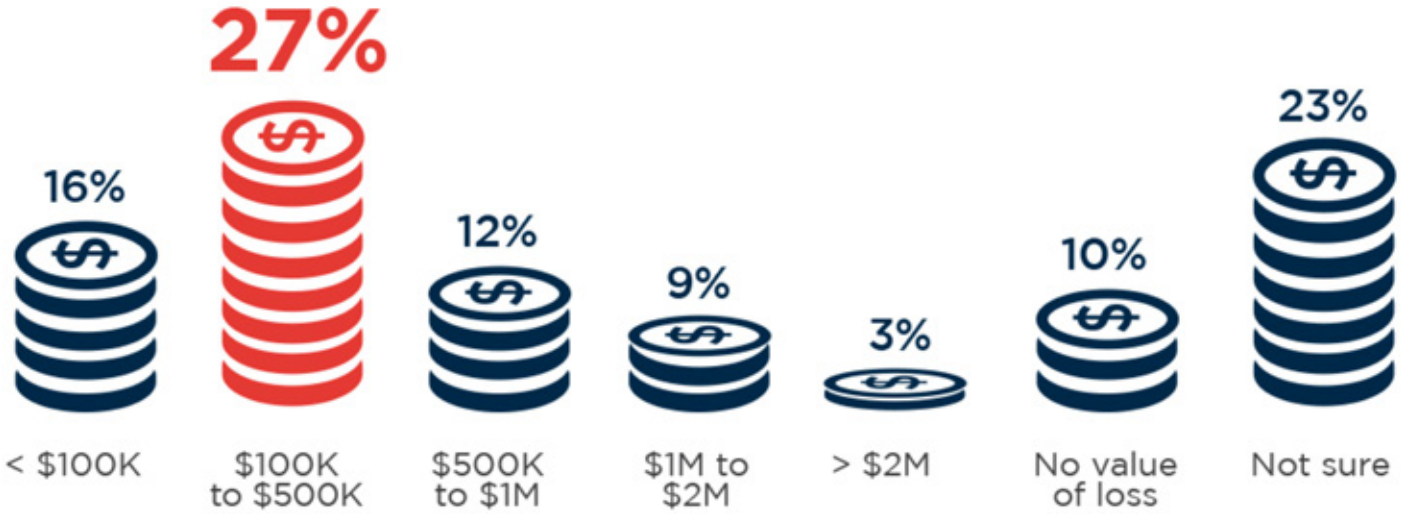
Q: Have insider attacks against your organization become more or less frequent over the last 12 months?



Copyright © 2018 CA, Inc. All rights reserved.

Impact of Threat: What is the cost of the attack?

Q: What would you estimate is the potential cost/loss of an insider attack in US Dollars?



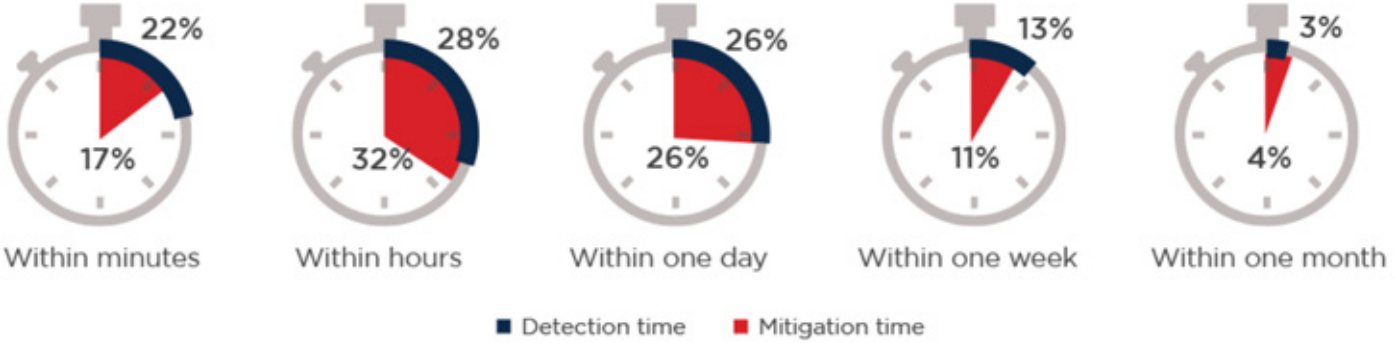
60% of all insider breaches are financially motivated[1]

Copyright © 2018 CA, Inc. All rights reserved.

1. 2017 Verizon Breach Report

Impact of Threat: How long to detect an attack?

Q: How long does it typically take your organization to detect an insider attack?



50% organizations detect an insider attack within hours

Not sure 8%

Q: How long does it typically take your organization to mitigate and stop an insider attack?

49% organizations mitigate and stop an insider attack within hours

Not sure 10%

Copyright © 2018 CA, Inc. All rights reserved.

THE SOLUTION

Privileged Access Management

- Stops **Targeted Attacks**
- Mitigates **Insider Threats**
- Achieves & Sustains **Compliance**
- Improves **Efficiencies**
- Secures the **Hybrid Enterprise**

Copyright © 2018 CA, Inc. All rights reserved.

THE SOLUTION

PAM | Disrupts the attack sequence

Copyright © 2018 CA, Inc. All rights reserved.

THE SOLUTION

5 Ways PAM **Breaks** the Chain

VALUE STATEMENT

Provides foundation for combatting insider threats and targeted breaches
Centrally manages and protects access and usage of privileged accounts

1 Privilege Vault builds the foundation

What challenges does it solve:

- Protects and manages privileged credentials
- Authenticates and links users to privileged activity
- Adopts zero-trust posture – permit by exception

ca technologies

THE SOLUTION

5 Ways PAM **Breaks** the Chain

VALUE STATEMENT

Session recording is out of the box, highly scalable, and delivered with no additional infrastructure requirements

2 Session Recording is Critical

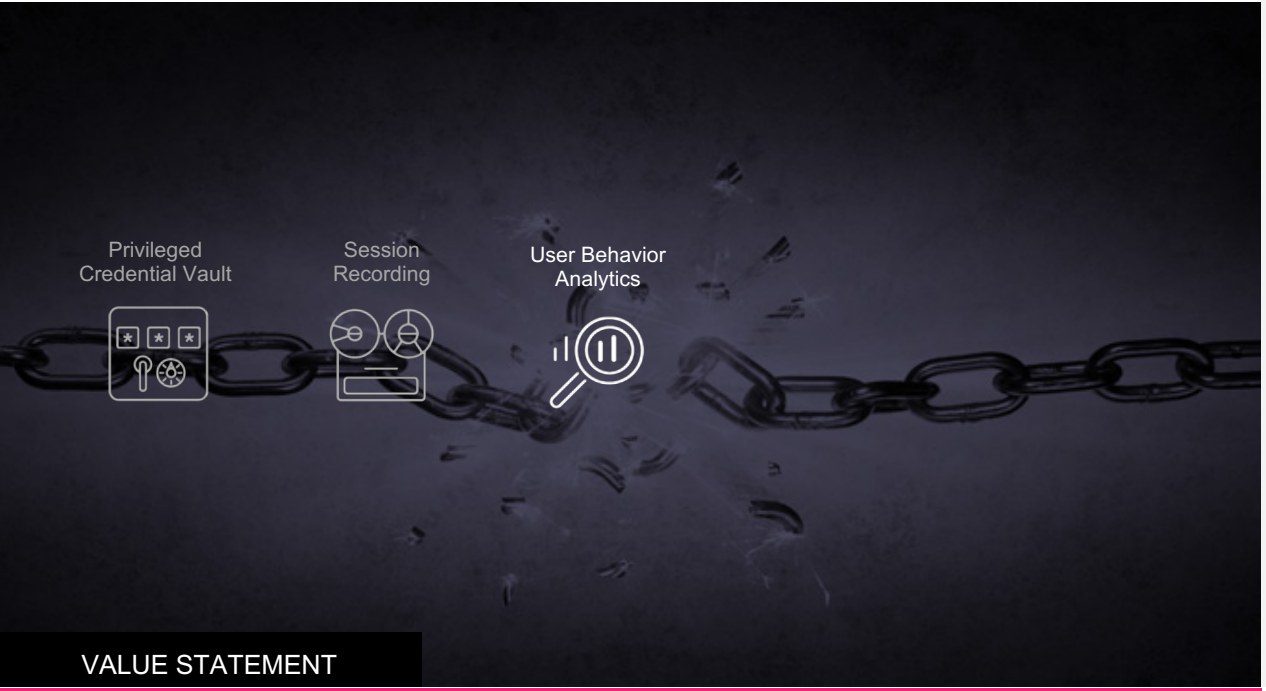
A “must have” capability that provides:

- Video coverage of all privileged user activity
- Individual accountability
- Forensic evidence of accidental or malicious actions

ca technologies

THE SOLUTION

5 Ways PAM **Breaks** the Chain



VALUE STATEMENT

CA Threat Analytics for PAM continuously assesses risk to quickly detect malicious activity so you become

3 User Behavior Analytics **supercharges** static controls

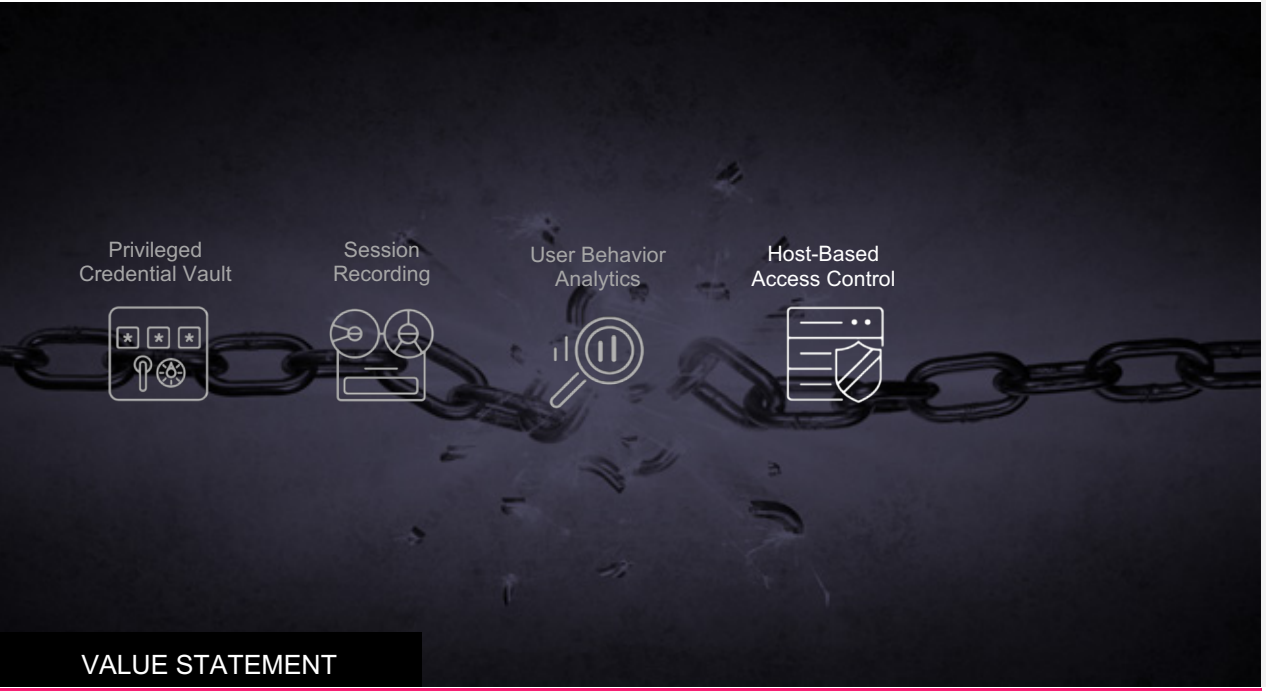
A “must have” *emerging* capability because it:

- Can quickly identify abnormal behavior
- Assess the risk associated with this activity
- Trigger automated migration to the risk

ca technologies

THE SOLUTION

5 Ways PAM **Breaks** the Chain



VALUE STATEMENT

CA PAM Server Control provides an extra layer of security for your most mission critical servers

4 Host-Based Access Control **complements** Privilege Vault

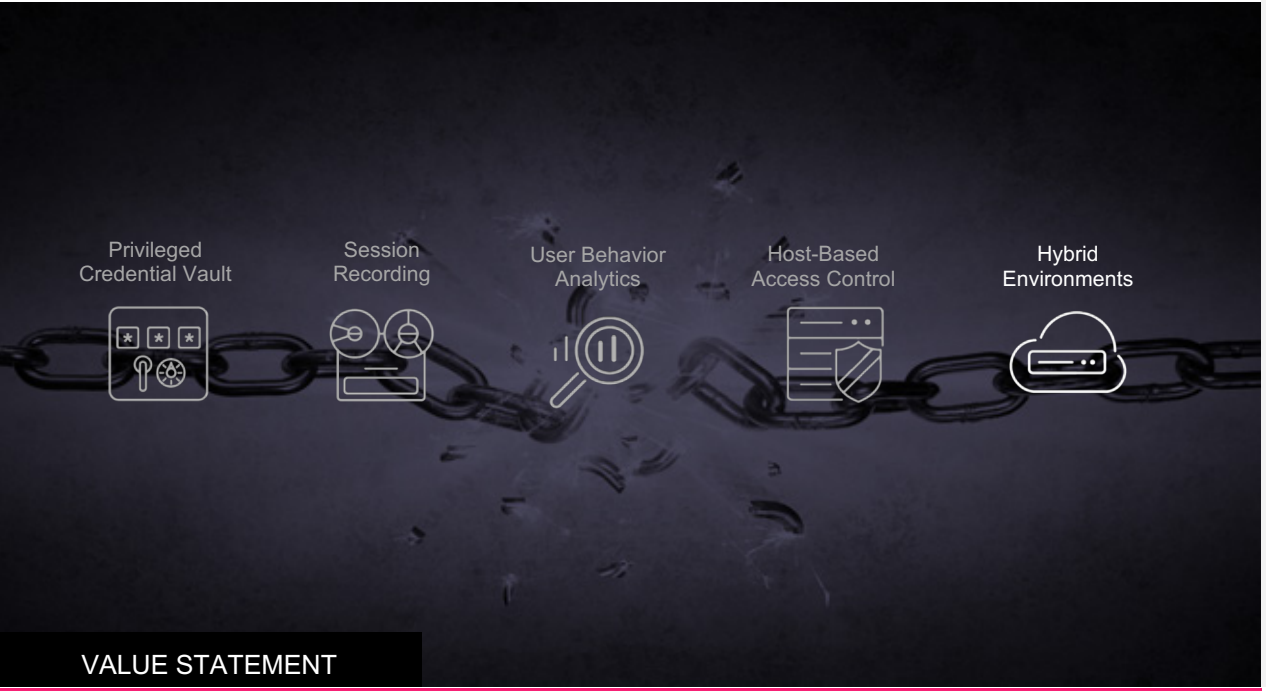
A “value add” security capability that provides:

- Fine-grained access control for critical servers
- Command and socket filtering
- Monitoring and alerts when changes made
- Secure task delegation

ca technologies

THE SOLUTION

5 Ways PAM **Breaks** the Chain



VALUE STATEMENT

No limitations solutions goes wherever your apps go… either physical, virtual or cloud.

5

The Modern Software Factory is Complex

A “value add” security capability that provides:

- Cloud-based
- Mainframe
- On-premise
- Virtual

ca technologies

WHY CA Privileged Access Management

Comprehensive privileged access security

1 Quick **Time to Value** Protection

Installs in hours not weeks or months

Easy to install, configure, maintain, upgrade and manage

Enhanced features in base software license costs

Less infrastructure reduces overall total cost of ownership

2 Enterprise-Class **Scalability**

Single appliance protecting thousands of resources

Session recording runs in appliance, no additional hardware required

Supports a large number of concurrent sessions – at no additional costs

3 Defense-In-Depth **Protection**

Comprehensive PAM solution in network and host based form factors

Supports physical, virtual and cloud environments

Threat Analytics help reduce the threat of breach

ca technologies

Copyright © 2018 CA, Inc. All rights reserved.

Thank You

To learn more about Insider Threat, visit us at:

https://www.ca.com/us/products/insider-threat.html

To learn more about CA PAM, visit us at:

ca.com/pam

Copyright © 2018 CA, Inc. All rights reserved.

Robert Marti
Product Marketing Director, PAM
Robert.Marti@ca.com

@casecurity
Slideshare/CAinc
Linkedin.com/company/ca-technologies