Protecting Data and Your Reputation on the Mainframe

Chip Mason
Lead, Product Management– Mainframe Security

April 25, 2019

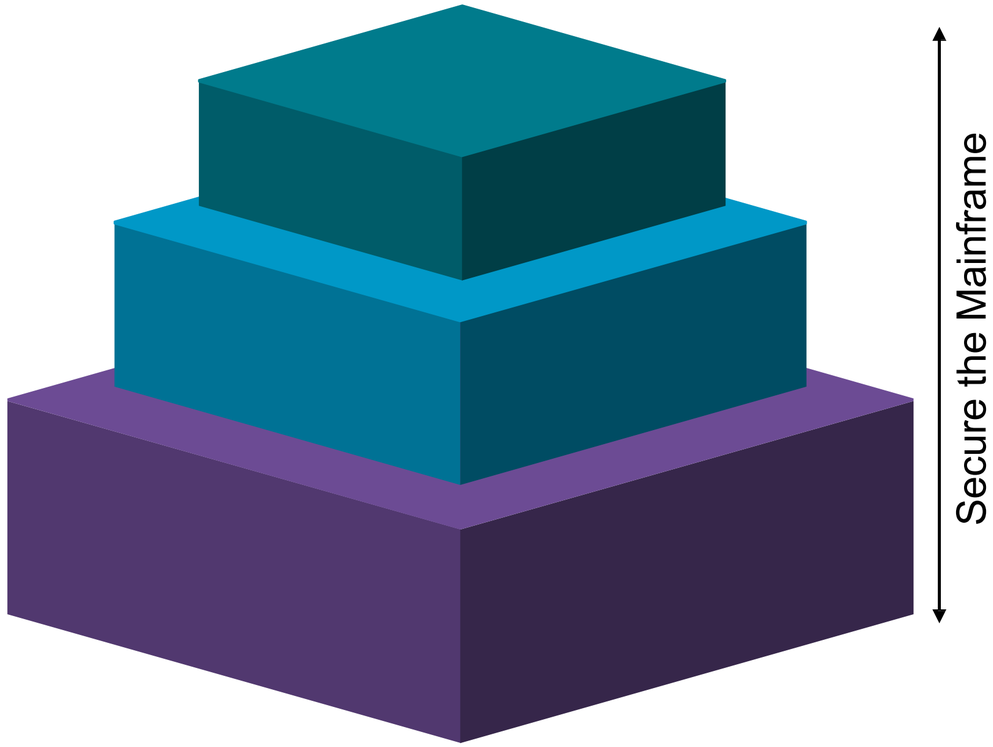
BROADCOM®

Your Mainframe is at Risk

People
Insider threats range from malicious users to well-intentioned employees making a mistake.

Data
70% of today's corporate data – including sensitive and regulated data like PII – reside on the mainframe.

Systems
The mainframe is increasingly connected into the digital economy – applications, mobile devices, Big Data.



"Big iron is still very secure…unfortunately we have this thing called people that surround the mainframe." – Patrick Gray, Ex FBI Security Agent

The Data Security Challenge

High Cost

$11.5B
Ransomware damage costs in 2019[1]

Discovery Time

147
Days infiltrated before detection[3]

Data Breaches

53,000
Incidents this year[2]

2,216
Confirmed data breaches

Continuous Risk

49%
of those attacked were successfully attacked again within one year

Internal Threats

10,637
Incidents from privilege misuse

Skills Gap

285,000
Cyber security roles went unfilled in the US last year

BROADCOM

The Regulatory Ecosystem

GDPR

- Prove that data is being protected
- Appoint a Data Protection Officer
- Fines of 4% of annual turnover

FISMA

- Framework for protecting Federal Data
- NIST 800-53, -37
- DHS CDM Phase 2, Phase 4

PCI DSS

- Protect stored cardholder data
- Encrypt transmissions
- Maintain InfoSec policy

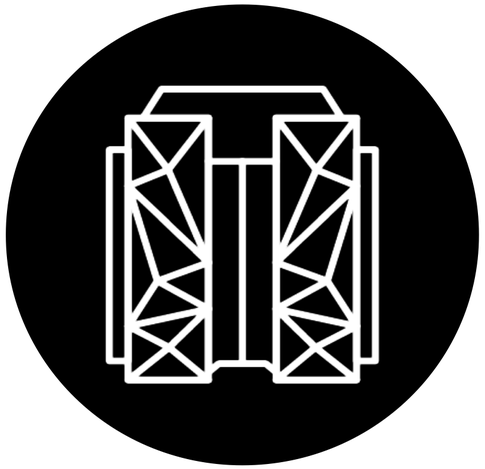
EU-U.S. Privacy Shield

- U.S. Department of Commerce and European Commission
- Individual choice & control
- Security

Know which regulations apply to your business

BROADCOM

How Data-Centric Mainframe Security Helps



- **BOTTOM UP SECURITY**
- **CONTROL THE DATA**
- **LIMIT INTERNAL THREAT VECTORS**
- **CONTINUOUS COMPLIANCE**
- **UNDERSTAND UNDERLYING RISK**

"CA mainframe security solutions provide us with a high level of confidence that access to sensitive data is secured and properly managed."

IT Specialist, Fortune 500 Banking Company

HOW TO LEVERAGE A DATA-CENTRIC APPROACH

Data	Understand	Monitor	Limit Access
Start with the data.	Understand data at risk	Access to critical data and systems.	Limit to only those with business need

BROADCOM

Mainframe Security Lifecycle

Effective security and compliance requires full lifecycle support, oversight, and automation

Real–time notifications of potential security breaches for continuous compliance

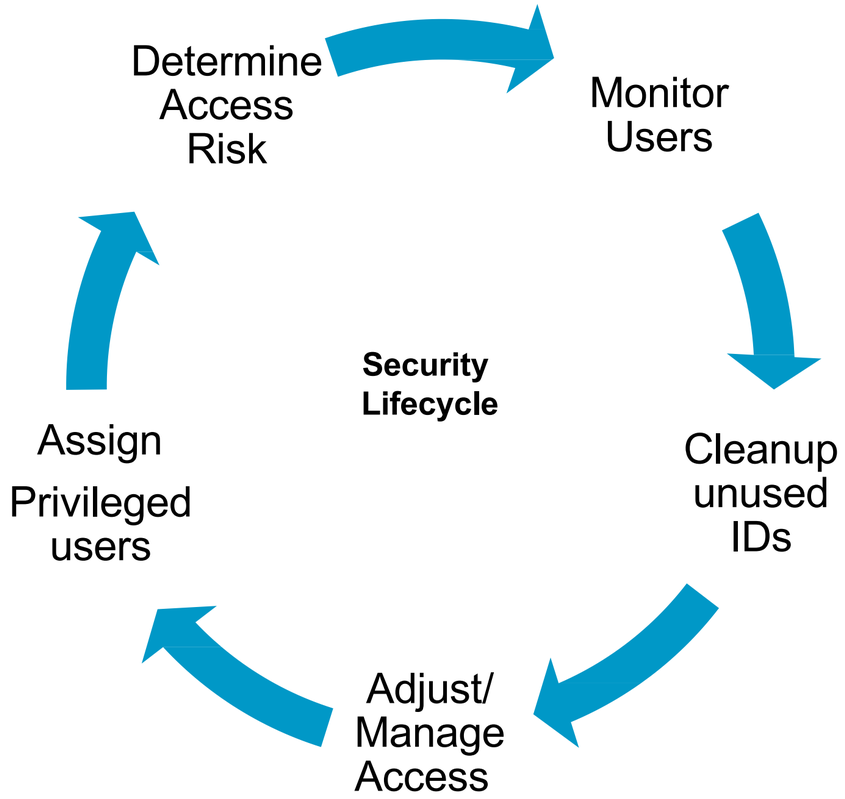
Ongoing scanning and classification of data at rest and in motion

Continuously monitor all privileged user activity

Ensure ongoing scalable and streamlined mainframe security

Easily automate continuous and unattended security file cleanup

Role discovery / RBAC model
Automated entitlement certification for all end-points



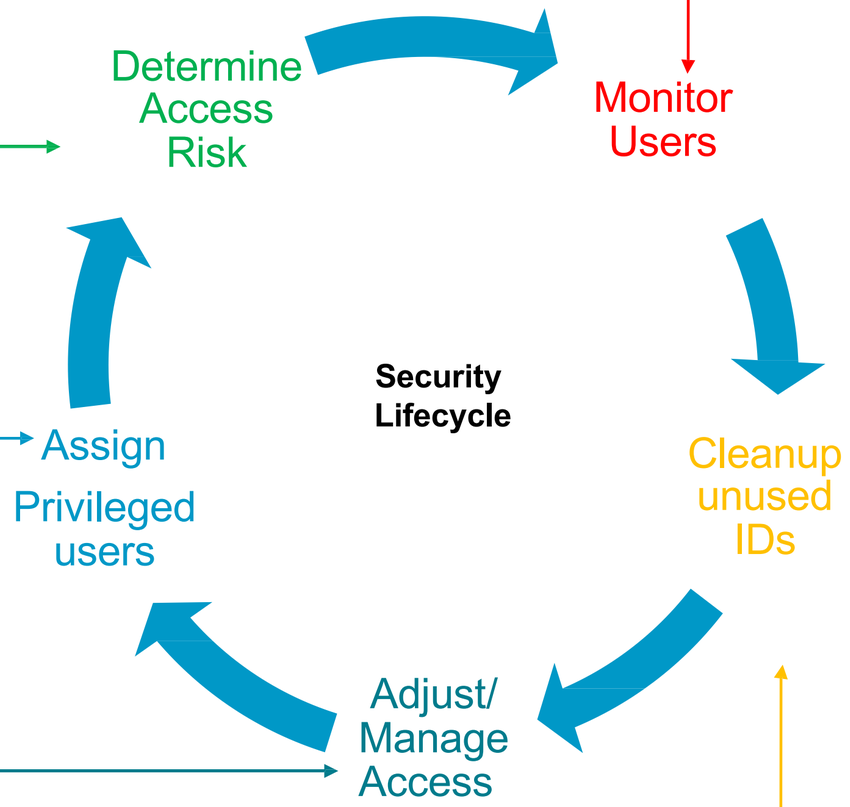
BROADCOM

Succeed with the Right Technology Stack

Effective security and compliance requires full lifecycle support, oversight, and automation

New!

Real–time notifications of potential security breaches for continuous compliance	**CA Compliance Event Manager**
Ongoing scanning and classification of data at rest and in motion	**CA Data Content Discovery**
Continuously monitor all privileged user activity	**CA Trusted Access Manager for Z**
Ensure ongoing scalable and streamlined mainframe security	**CA ACF2 & Top Secret**
Easily automate continuous and unattended security file cleanup	**CA Cleanup**
Role discovery / RBAC model Automated entitlement certification for all end-points	**CA Identity Governance**



BROADCOM

Use Cases

US Government IT Initiatives

Cybersecurity

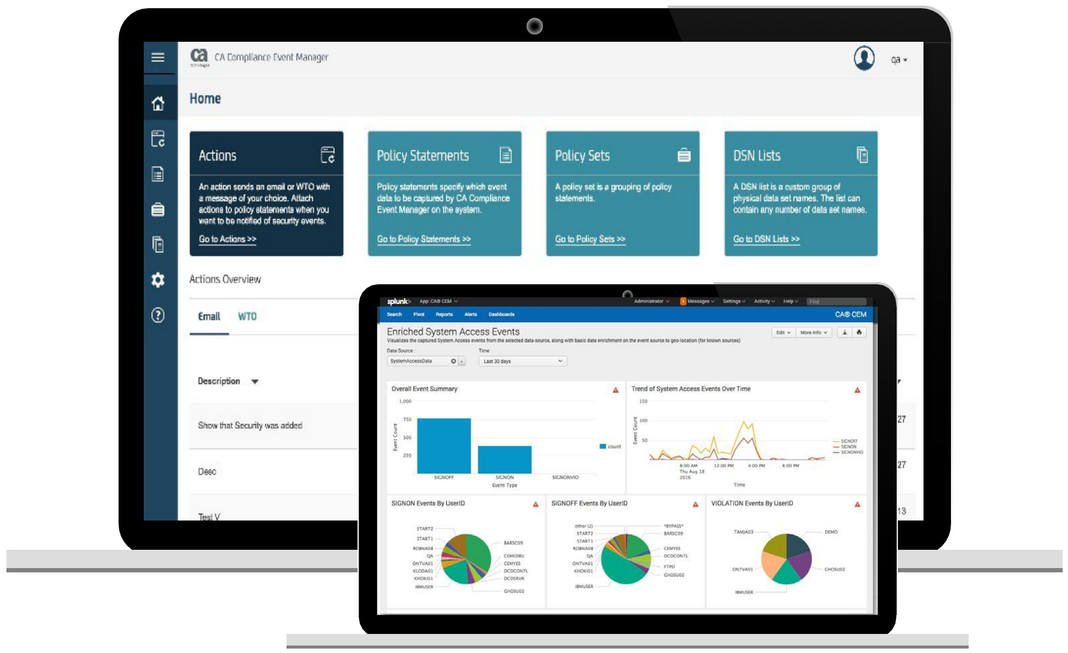
1. **Monitor users for suspect activity and possible insider threat**
2. **Understand the underlying Cyber Risk of data**
3. **Least Access: ensure that only those with a validated need have access**

Identity, Credential and Access Management

4. **Reduce risk by managing Privileged Access Rights**
5. **Leverage Multi-factor authentication for mainframe applications and management.**

BROADCOM

Monitor users for suspect activity and possible insider threat



CA Compliance Event Manager

Real-time notifications of violations to critical security systems and resources, so stakeholders can react quickly.
Real-time alerting

Critical System Files can be easily edited to reduce alert ‘noise’ and hide activity
File Integrity Monitoring

Mainframe is often not included in SOC due to flood of events. Filter and forward to SIEM for holistic view of the security infrastructure.
SIEM Forwarding

Advanced audit and compliance information for deeper insights into critical security issues.
Auditing and forensics

CA Compliance Event Manager

Key Features Include:

Real-time alerting.
Immediate notification of potential security threats, allowing stakeholders to react quickly.

SIEM event forwarding.
Filter critical mainframe security events and forward to SIEM and other platforms.

File Integrity Monitoring
Alerts to changes in critical system files.

Advanced auditing and forensics.
Deeper insight into security and compliance issues for an improved risk posture.

Regulatory compliance.
Detailed yet simple reporting to easily communicate security posture.

100 percent on platform.
Critical data never leaves the z/OS platform.

Understand the underlying Cyber Risk of data

Easily find sensitive or regulated data across multiple data sets.

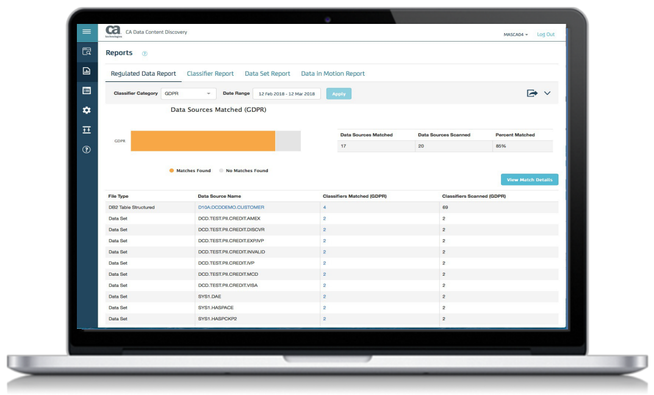
Classify Risk related to regulatory or business concerns.

Review compliance results and label sensitive data. Provide comprehensive compliance reports to auditing.

Set up and initiate data scans to find sensitive date at rest, and in motion.

Adjust Access to improve security posture.

Identify who has access to what data and who accessed data.



CA Data Content Discovery

CA Data Content Discovery

Key Features Include:

Web-based.
Access results through an easy-to-use web interface.

ZIIP-enabled 100 percent on platform.
Critical data never leaves the z/OS platform.

Access analysis.
Quickly visualize who has access to sensitive data.

Over 180 classifiers.
Classify data based on risk level.

Immediate notification.
Receive email alerts for scan notifications.

On demand.
Scans run when it is best for your business.

Data dictionary.
Use out-of-the-box and custom data repositories.

Optimal performance.
Exploit IBM mainframe specialty processors.

Machine learning.
Improve accuracy with machine learning for Db2.

Least Access: only those with a validated need have access

50% **of mainframe security databases contain orphaned, obsolete or redundant identities and entitlements.**

Reduce Time and Cost of Compliance and Mitigate Risk

Analyze

- ✓ Quickly gain insight into active and inactive user IDs, profiles and permissions
- ✓ Identify risks in privileged access management

Consolidate

- ✓ Automatically remove incorrect or obsolete entitlements and access groups
- ✓ Restrict privileged access rights to align with the principle of least access

Maintain

- ✓ Continuously monitor system activity
- ✓ Automate and streamline compliance processes and establish controls

CA Cleanup

BROADCOM

CA Cleanup

Key Features Include:

24/7 monitoring.
Continuously monitoring your security system activity to record security definitions.

Enhanced security recertification.
Monitor security activity and identify used and unused user or application access.

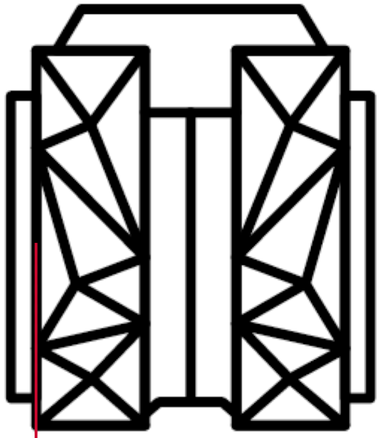
System and admin overhead reduction.
Remove unused access rights and IDs from the security system.

Report generator.
Batch utility program to produce reports for specific purposes.

Command generation.
Create commands to restore removed IDs if and when needed.

Reduce risk by managing Privileged Access Rights

Insiders are the Biggest Threat to Your Organization!



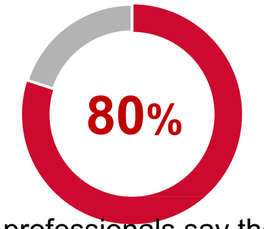
Challenges to Privileged Access Management

Volume of data and resources → Credential sharing → Limited auditability

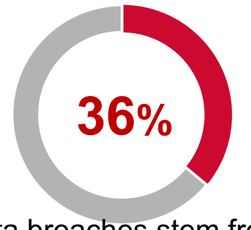
Audit all activities performed by privileged users.

Control access to a privileged state with Escalation and Automation.

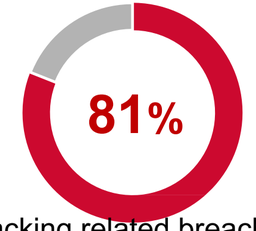
Protect against insider threats and deliver trust.



IT professionals say their company doesn't implement least privilege control[1]



Data breaches stem from inadvertent misuse of data by employees[2]



Hacking related breaches involving the misuse of stolen or weak credentials[3]

CA Trusted Access Manager for Z

BROADCOM

CA Trusted Access Manager for Z

Key Features Include:

Reduce credential sharing.
Promote and demote existing user identities to manage, monitor and control access.

Deliver trust and efficiency.
Helps ensure all access requests have a business need through service desk integrations.

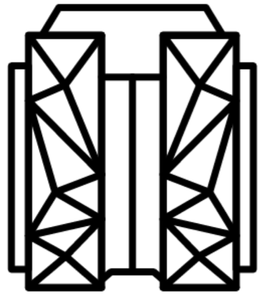
Align with workflows.
Works directly with CA ACF2 and CA Top Secret using the same interface, so you can start using it right away.

Advanced auditing and forensics.
Integrates with CA Compliance Event Manager for in-depth auditing of all user activity.

100 percent on platform.
Industry-first mainframe only solution for privileged access management.

Leverage Mainframe Multi-factor authentication

CA Broadcom- Leaders in managing Identity and Access on Mainframe – CAACF2, CA TopSecret



User Provisioning

Manage user information on multiple systems and applications.

User Access

Control access to critical resources by implementing reliable security measures. **Passphrase**

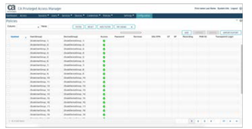
Breach Prevention

Protect against unauthorized access to sensitive data with **Advanced Authentication Mainframe**.

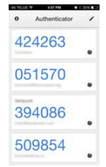
New Multi-factor Support

- RSA Secure ID

- PIV/CAC using CA PAM



- RADIUS Protocol Support



Support available for ACF2, TopSecret and RACF

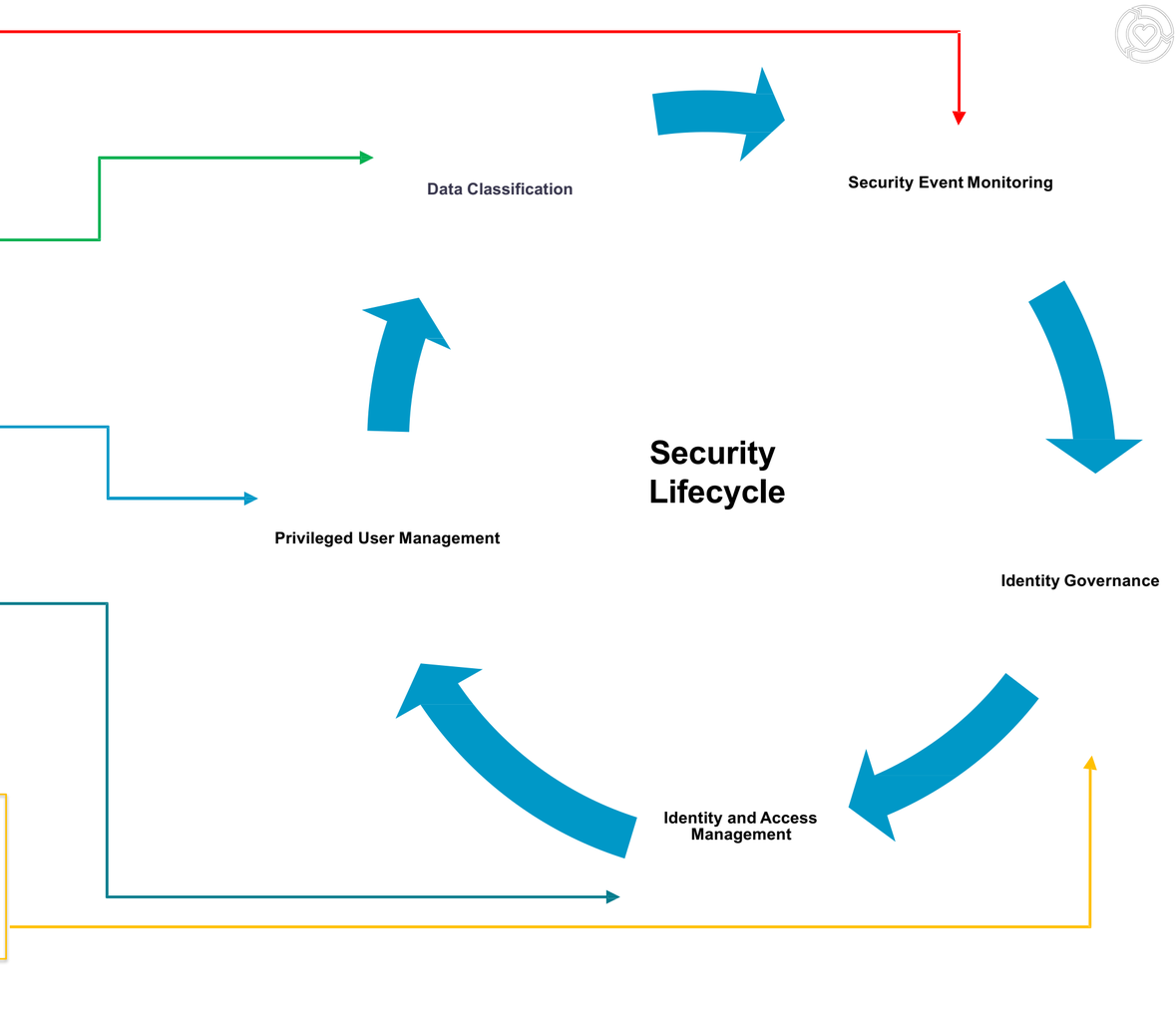
BROADCOM

Bring Mainframe Security to Today's Standards

Effective security and compliance requires reporting, oversight, and automation

New!

Real–time notifications of potential security breaches for continuous compliance	**CA Compliance Event Manager**
Ongoing scanning and classification of data at rest and in motion	**CA Data Content Discovery**
Continuously monitor all privileged user activity	**CA Trusted Access Manager for Z**
Ensure ongoing scalable and streamlined mainframe security	**CA ACF2 & Top Secret**
Easily automate continuous and unattended security file cleanup	**CA Cleanup**
Role discovery / RBAC model Automated entitlement certification for all end-points	**CA Identity Governance**



BROADCOM

Evaluate Your Audit Readiness

DATA ACCESS	• Do you have systems in place to limit access on a need to know basis, ie. timebox the duration of privileged access? • Do you have a strategy for designing “least access” controls? • Can you manage your test data?
DATA IDENTIFICATION	• Do you have complete visibility and control over your data? • Are you able to define risk-based data protection rules? • Do you have rules for sensitive data management?
REPORTING	• Can you audit all privileged access requests and activity performed? • Can you identify data breaches in real-time using comprehensive forensics?