Compliance and Cybersecurity: Mainstreaming the Mainframe

John Crossno, PMC-III, CSPO,
Principal Product Manager

September 27, 2018

Key Takeaways

- GDPR impact to businesses
- Market problems addressed by Application Audit
  - Application user behavior to combat growing cybersecurity risks
  - Increasing compliance mandates
- Application Audit's unique value
  - Granularity of data captured
    - Fits compliance and security needs
- Types of Insider Threat Actors
  - Malicious, inadvertent, negligent

Key Takeaways

- Consequences for breached companies:
  - Forfeiture of revenue
  - Degraded brand reputation
  - Remediation expenditures
  - Diminished market share
  - Business disruption
  - Collateral security risks
  - Compromised intellectual property
  - Legal and regulatory repercussions (GDPR, HIPAA, PCI, NY, California, NDB, Corp Policies, etc.)

What is GDPR?

- I Am Not A Lawyer
- General Data Protection Regulation
- New European Union Law
  - Came into effect May 25th, 2018
  - Affects how personal data is collected and processed
    - Personally Identifiable Information (PII)
  - Impacts any company doing business in the EU
- GDPR replaces the EU Data Protection Directive
  - Only applied to the processing of PII on EU located equipment

Does GDPR apply to my business?

- Do you have a business location in the EU?
- Do you allow European residents to transact business with you?
- Do you collect PII from European residents?
  - Do you store it?

Did you say YES to any of the questions?

- How do you collect it?
- Six principles of use apply

Do You Have Consent?

Six Principles of Use

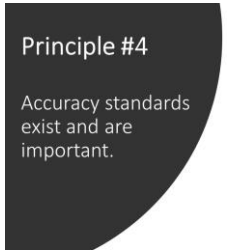
- Lawfulness, fairness and transparency
  - Data must be processed transparently (consent given)
- Purpose Limitation
  - Collected for specific, explicit and legitimate purposes
  - Collected and used for a specific, explicit and legitimate purpose, and **ONLY** that purpose
    - Not further processed in a manner incompatible
  - When its specific purpose of use has expired, then it must be deleted
  - Archiving may not be a valid purpose

Principle 1 - Lawfulness, Fairness & Transparency

GDPR Core Principle 2 - Purpose Limitations

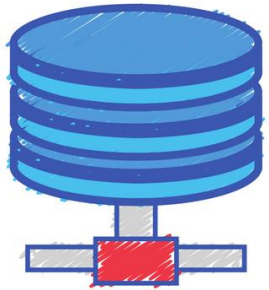
Six Principles of Use

- Data minimization
  - Adequate, relevant and limited to what is necessary in relation to the purpose for which it was collected
- Accuracy
  - Kept accurate, up to date
    - Every reasonable step must be taken to ensure accuracy
  - The purpose for collecting must be maintained, else it needs to be deleted or rectified without delay



Six Principles of Use

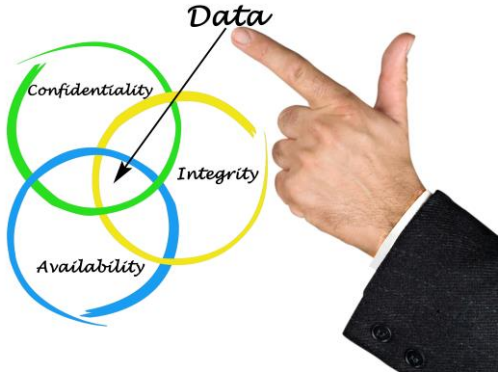
- Storage limitation
  - Kept in a form which permits identification of data subject for no longer than necessary for the purpose it was collected
  - May be stored longer insofar as it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (in accordance with Article 81(1)
    - Subject to implementation of the appropriate technical and organizational measure required by the regulation to safeguard the rights and freedoms of the data subject.



GDPR Core Principle 5 - Storage Limitations

Six Principles of Use

- Integrity and Confidentiality
  - Processed in a manner that ensures appropriate security of the personal data;
    - Including protection against unauthorized or unlawful processing
    - And against accidental loss, destruction, using appropriate technical or organizational measures



- Accountability – Not technically a principle
  - The controller shall be responsible for, and be able to demonstrate compliance

Right to be Forgotten

- Forget about me!
  - The ultimate owner of the PII is the individual
    - Companies are just stewards of that data
  - The individual may ask:
    - What do you know about me?
    - Delete everything you know about me
      - What about backups?
  - Wait a minute!!!!
    - The user may ask, but is compliance required?
      - Always?

Portability

- The data is mine!
  - The ultimate owner of the PII is the individual
  - The individual may want to take his data to another business or provider
    - You are required to provide the individual with their data
    - What about data formats?
      - Highly industry dependent

Right to be Notified

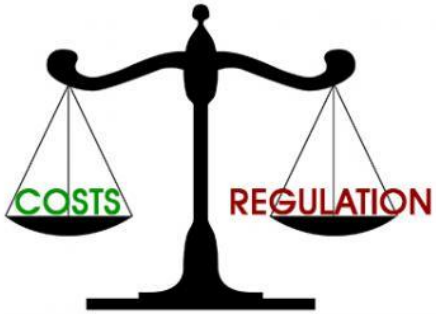
- Breach discovered, now what?
  - Within 72 hours of Identifying the breach
    - Notification of affected individuals
    - Notification of the regulatory bodies

What does non-Compliance Cost?

Up to €20M (±$24M)

4% of Global Revenue

Whichever is greater!



Market Problem

Growing Cybersecurity Risks

- Breaches are increasing:
  - 5% increase between 2014 and 2015
  - 2016: 4B records stolen; >2x 2014 + 2015 combined[1]
  - 2017: 6.7% increase
- Takes too long to find breaches:
  - Global average time to detection = 146 days[2] (469 days for EMEA)

Increasing Compliance Mandates

- Risk non-compliance with regulations (e.g. GDPR) and industry mandates
  - Mechanisms to control, monitor and report access
  - Automated detection of breaches
  - Notifying those affected if breach occurs

[1] IBM X-Force® Research: 2016 & 2017 Data Breach Review
[2] FireEye Releases First Mandiant M-Trends EMEA Report

Cybersecurity Cost

of attacks are by **insiders**[1]

Average cost
of breach is

$3.8M per case[1]

When uncovered by **active detection**
(ex: monitoring), median loss and duration were **lower**[2]

[1] IBM X-Force® Research: 2017 Cyber Security Intelligence Index
[2] Association of Certified Fraud Examiners, 2016 Report on Occupational Fraud and Abuse

The Problem

- Most sensitive data and business-critical systems sit on mainframe
- Mainframe is **inherently highly secure and the most securable platform, but …**

– **Security teams lack visibility into application user behavior**

  - Users with access
  - Users with unauthorized access

– **Reliant on insiders or outsourcers that may be ones committing crime**

Note: All systems have this problem!

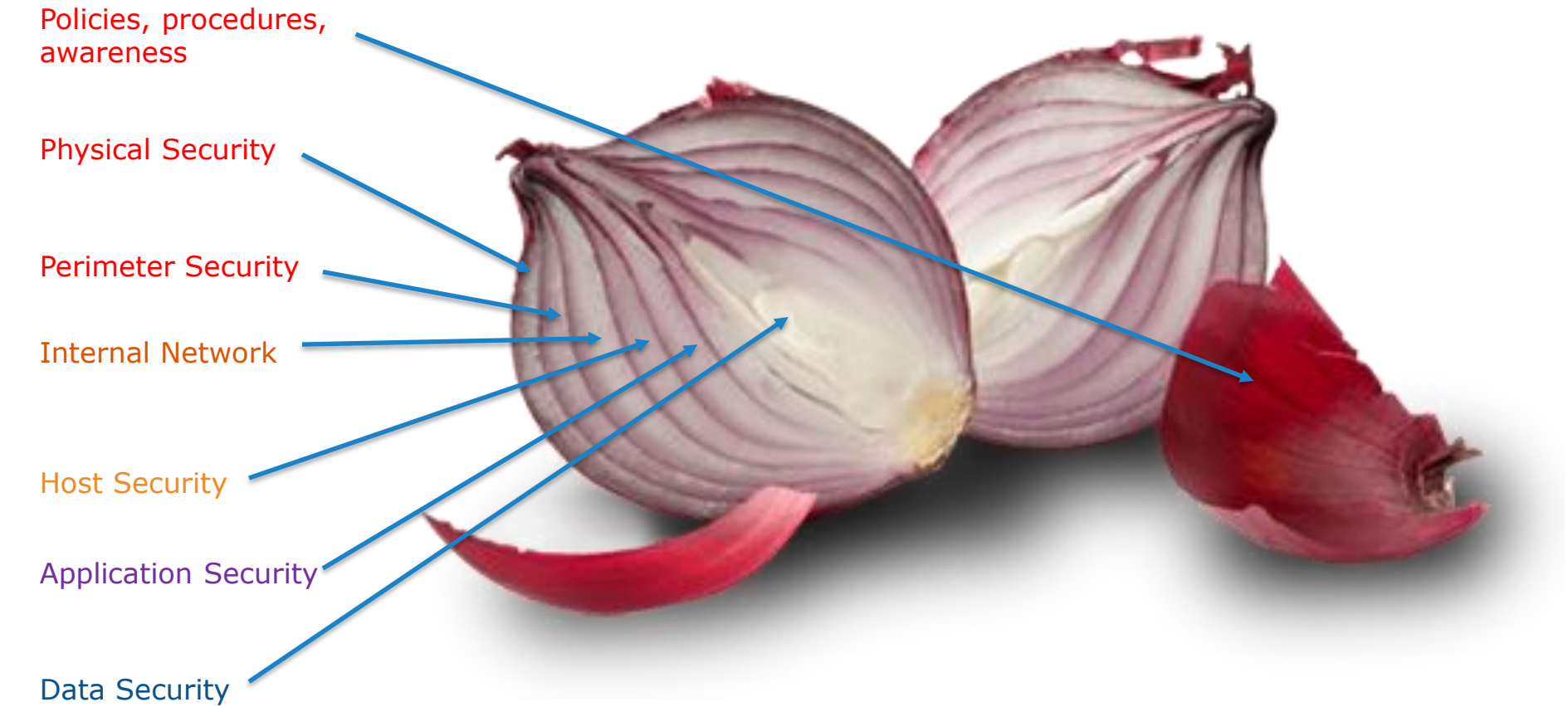
Additional Statistics

- SMF data
- Scans of disparate logs
- SIEM tools
- RACF, CA ACF2, CA Top Secret

Additional Statistics

- 88 percent of end users say their job requires them to access and use proprietary information - *Varonis 2016 Study of US & European Organizations*
  - 62 percent say they have access to company data they probably shouldn't see
- 75% of incidents go unreported – *Carnegie Mellon US Cert*
- $500,000 is the cost that 75% of companies estimate to remediate an insider breach – *2016 Insider Threat Spotlight report*
- 2/3 of insider incidents are due to employee negligence – *2016 Ponemon Institute Survey*
- 56% of employees believe it's OK to take information with them when they leave a job – *Symantec*
- Trade Secrets Global Annual Impact Loss > $2.2T – *PwC 2016 Survey*
- 91% of hacking attacks begin with a phishing email - *Wired Magazine*

Peeling Back The Layers Of Security



Insider Threat

Insider

Any individual who has valid credentials to access internal resources

Insider Threat

Individual who uses authorized access to negatively impact system integrity or confidentiality of intellectual property or data

Who may pose an insider threat?

Types of Insider Threat Actors

Malicious

Negligent

Inadvertent

Characteristics of Potential "At Risk" Insider

Malicious or Negligent

- Self-entitlement
- Debilitating introversion
- Intolerant of criticism
- Lack of empathy
- Passive aggressive
- Ethical flexibility
- Greed or financial distress
- Susceptibility to blackmail
- Extreme compulsiveness

Characteristics of Potential “At Risk” Insider

Inadvertent

- Unwitting
- Careless
- Unawareness
- Inattention
- Needs training

Examples of "Insider" Breaches

U.K. Bank

Privileged user accesses bank app to transfer funds into dummy accounts also set up through standard banking apps

European Credit Card Processor

Contracted SysProg accesses apps to monitor and report/sell geography info for particular credit card usage

U.S. Healthcare Provider

Stolen credentials used to breach mainframe sensitive data

U.S. Government Agency

Hackers steal credentials later used to access mainframe data

Equifax

Last but not least

And on and on …

What Do Companies Stand to Lose?

- Forfeiture of revenue
- Remediation expenditures
- Diminished market share
- Business disruption
- Collateral security risks
- Compromised intellectual property
- Legal and Regulatory repercussions (GDPR, HIPAA, PCI, NDB, Corp Policies, etc.)
- Degraded brand reputation
  - "It takes 20 years to build a reputation, and five minutes to ruin it."
    - Warren Buffet

Be Offensive!

"The best defense is a good offense." — Vince Lombardi

- Today's threats are ever evolving, But one constant is the human element as a primary threat vector.
- Get ahead of a potential incident by identifying human threat indicators
- Can't just monitor network/database activity and block when something doesn't look right.
- Don't ignore analysis – Connect the dots – User behavior analytics

Data must be analyzed, or why bother collecting it?

How Does This Relate to Data Privacy?

The “Insider Threat” is after the Sensitive Data!

- Data has to be secured and protected
- $$ Money is the primary driver $$

Compliance

- GDPR
- HIPAA
- Corporate policies
- Others

How Security Helps with Compliance

Mechanisms to control and monitor access

- Control = access authorizations
- Monitor = Knowing who accesses what
  - Level of granularity plays a critical role

Automated detection of breaches

- What is a “Breach”?

Data for notifying those affected if breach occurs

- What was seen?
- When was it seen?
- How often was it seen?
- What was done with it?

Employee Privacy and Monitoring

- The downside of monitoring users

- How do employees feel about being monitored?
  - Is “Big Brother” really watching?

- The value of monitoring users
  - Improved breach detection
  - User Behavior Analytics
  - Prevention of “negligent” behavior
  - Protection of sensitive data
  - **Protection for the employee**
- **Education is needed!**

The Importance of Test Data Privacy

Is production data the best for dev/test/QA?

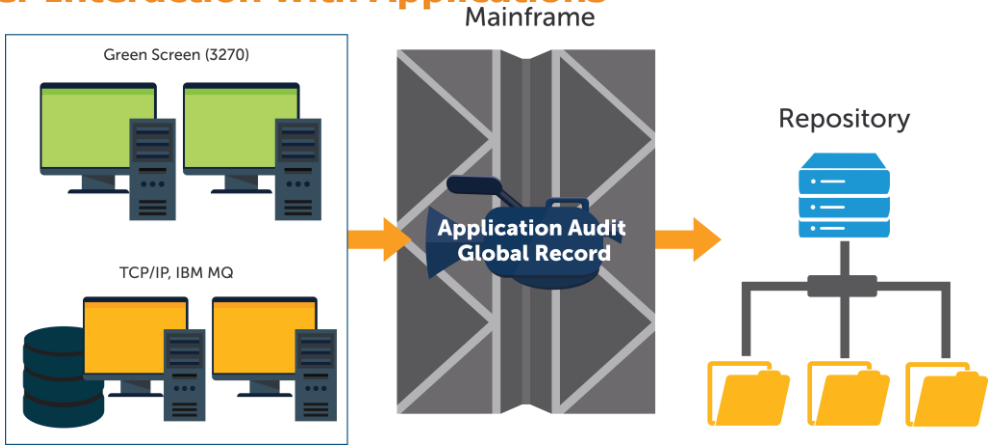
- Does it provide for better testing?
- How do you protect it?
- How do you know when it's been "breached"?
- How do you comply with regulatory mandates?
- How does it complicate matters?

What changes if production data is privatized?

- No need for the same protection as production
- Are concerns about it being breached the same?
- Are regulatory mandates still in play?
- Limited exposure!

Compuware Application Audit

User Interaction with Applications

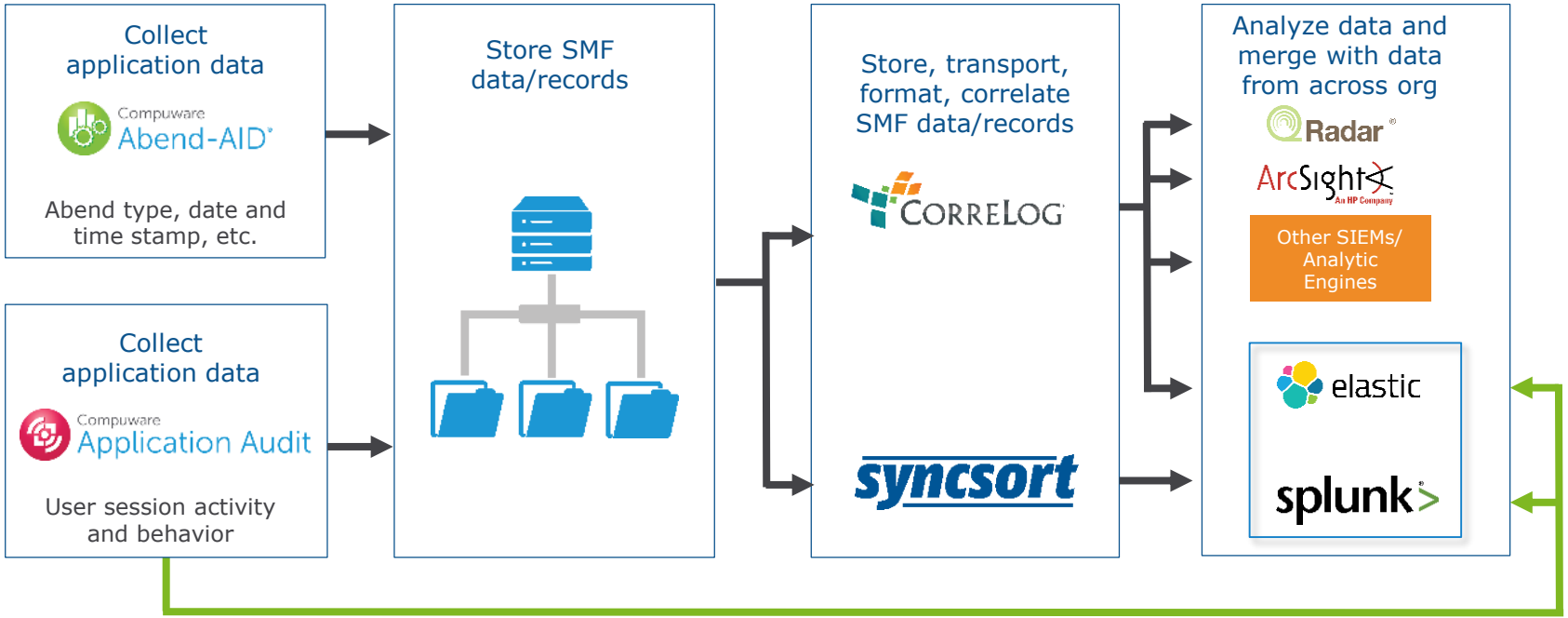


- Detect, investigate, respond to:
  - Inappropriate activity by internal users
  - Hacked or illegally purchased user accounts
- Credible forensics to support legal proceedings
- Fulfill data compliance mandates
- Improved analytics with SIEM integrations
- Familiar web UI enables separation of duties: administration vs. installation

No modification of mainframe apps required

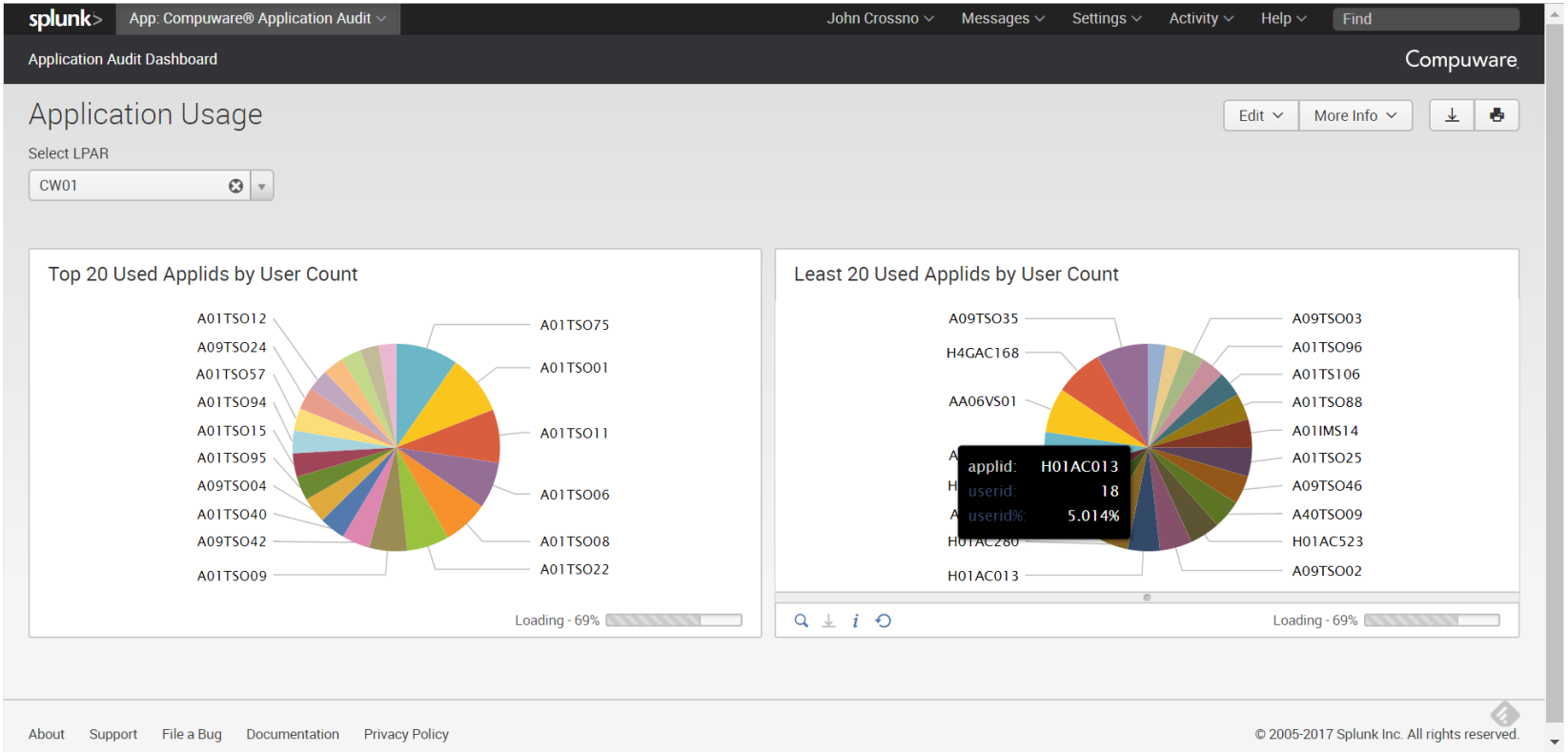
SIEMs and Compuware

Provide Abend and User Application Behaviors for Analytics

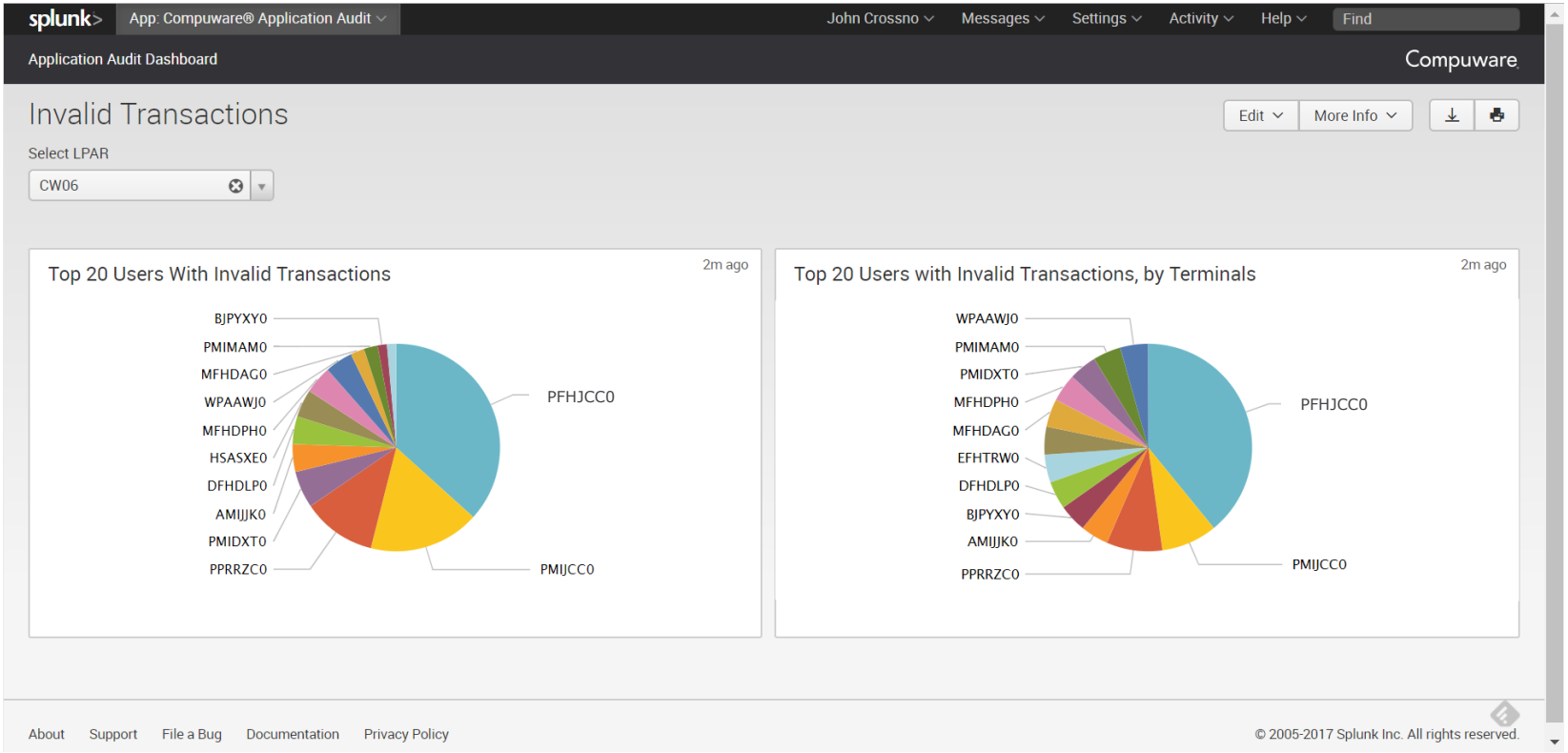


Application Audit Splunk Dashboard

Application Audit Splunk Dashboard



Application Audit Splunk Dashboard



Limiting the Exposure to Sensitive Data

Growing Cybersecurity Risks

- Gain insight to address the increasing breaches, by insider threat actors
- Reduce the time it takes to detect breaches

Increasing Compliance Mandates

- Helps address the risks of non-compliance with regulations (e.g. GDPR) and industry mandates
  - Mechanisms to control, monitor and report access
  - Automated detection of breaches
  - Notifying those affected if breach occurs

"Never, never, never give up" – Winston Churchill

Focus on Insider Threat and User Behavior Analytics

The Mainframe Software Partner
For The Next 50 Years