PCI Security Standards Council

Evidence-Based Scoping in the Zettabyte Era

Stephen Cavey | Co-founder and Chief Evangelist at Ground Labs

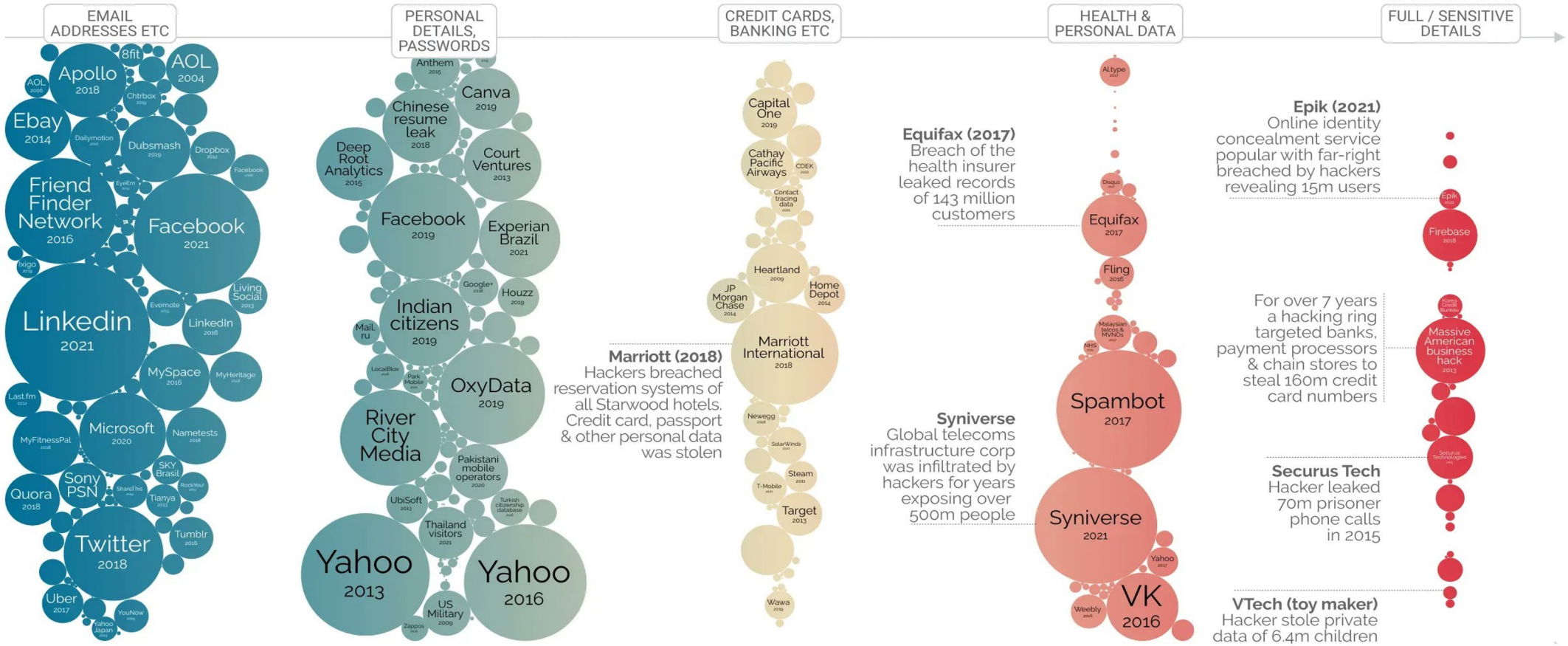
Evidence-Based Scoping in the Zettabyte Era

In this session, you'll discover:

- How poor data management leads to payment fraud
- The basics of data awareness for effective data management
- How to implement an evidence-based approach to data awareness for sustainable scoping and data security
- How this approach supports PCI DSS v4.0 compliance beyond scoping

PCI Security Standards Council

Notable Data Breaches 2004-2022 by data sensitivity



David McCandless **Information is Beautiful**
interactive version: geni.us/IIB-DBFB

total: 413 breaches // **sources** multiple press reports
updated 17th Jun 2022 // **data** geni.us/databreaches

PCI Security Standards Council


Data
Data
Data
Data
Data
Data
Data
Data
Data
Data
Data
Data
Data
PCI
Security
Standards Council

Legacy Data Risk in Digital Transformation

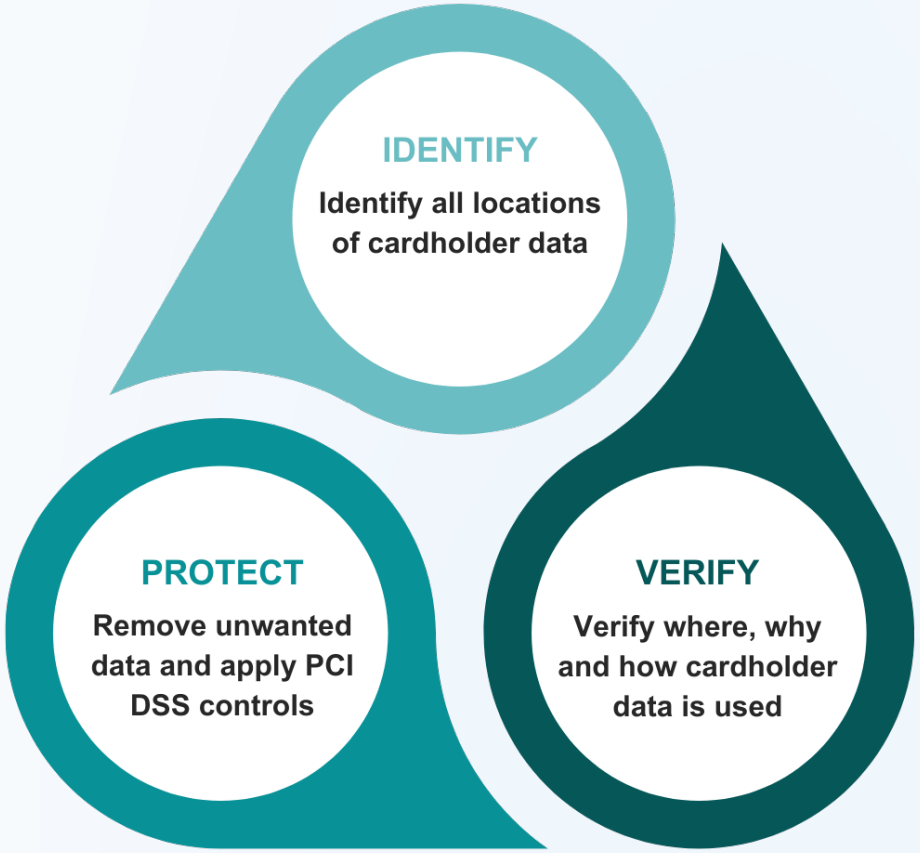
- Data collection practices that drive vast data stores
- Limited oversight resulting in poor visibility of high-risk data
- Accelerated digital transformation increasing fragmentation
- Increasingly complex supply chains leading to wider data distribution

PCI Security Standards Council

Data, Where? Everywhere

PCI Security Standards Council

Building Data Awareness



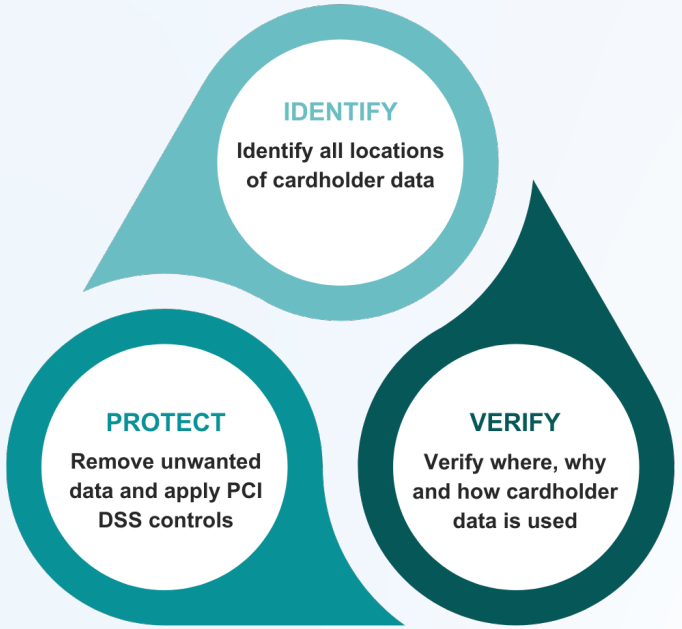
PCI Security Standards Council

Three Steps For Sustainable Scoping

- Scoping for PCI DSS is the “process of identifying all system components, people, and processes to be included in a PCI DSS assessment”

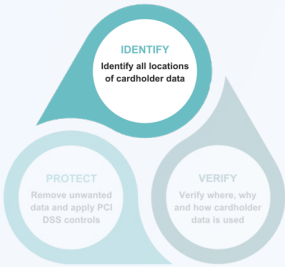
  (PCI DSS v4.0, Appendix G PCI DSS Glossary of Terms, Abbreviations, and Acronyms)

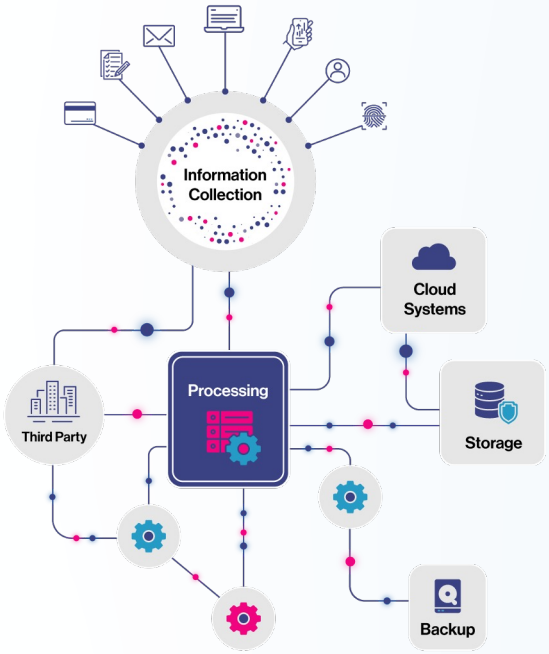
- This can be broken into three steps:
  - **Identify** all locations of payment account data
  - **Verify** those locations to confirm they are all part of the CDE
  - **Remediate** (protect) any rogue data found outside the CDE
- As a periodic or continuous process, this supports compliance with the new scoping controls in PCI DSS v4.0



PCI Security Standards Council

Data Discovery: The Ugly, the Bad and the Good



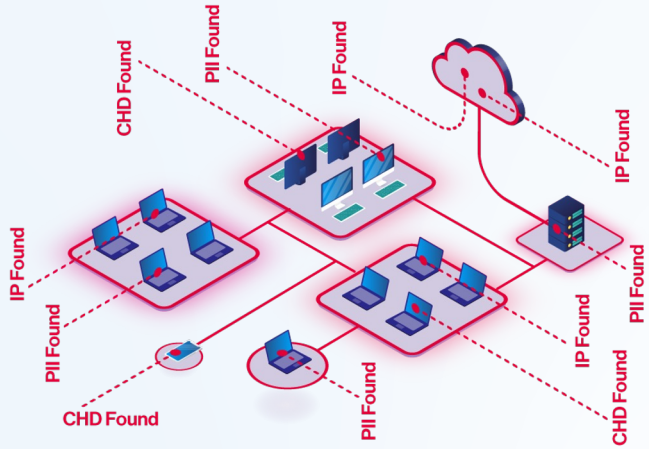


Data flow diagrams tell us where we expect to find data based on process and system design

Data flow diagrams are based on assumptions and intended design. This can lead to a false assumption that organizations have a well-managed data environment

/(reg)ex/

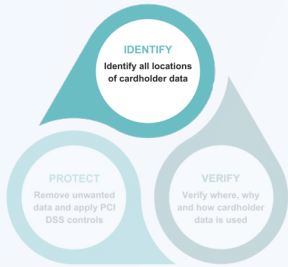
Regular expression script-based searches can't be used across all systems and platforms and result in a high number of false positives



Evidence-based data discovery is context-aware and identifies data in unexpected places across all systems and platforms with minimal false findings

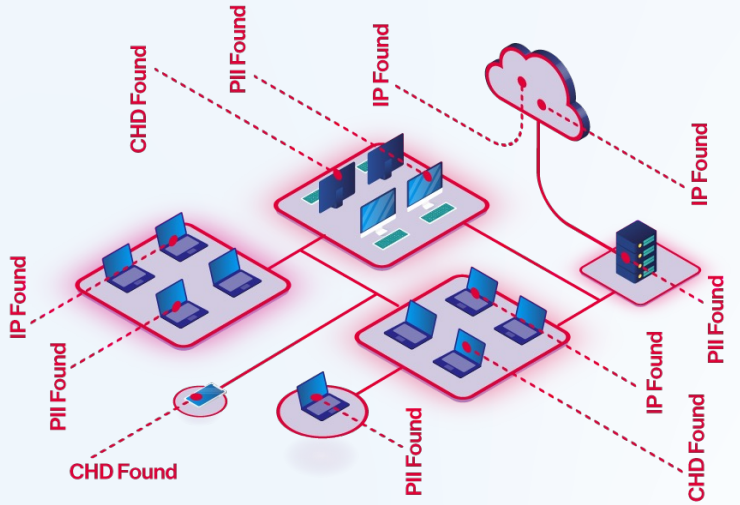
PCI Security Standards Council

Identifying Data With Evidence



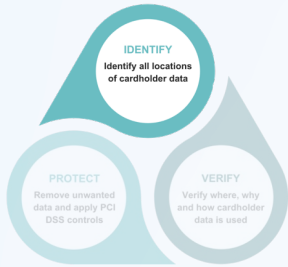
Eliminate assumptions

- Don’t accept **assumptions** about the data landscape of your business
- Instead use an **evidence-based** approach to validate the data you have and understand where it resides



PCI Security Standards Council

Consider All Data Storage Areas



Cloud and SaaS

Collaboration and Email

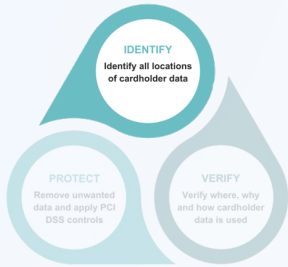
Databases and Big Data

Servers and NAS

POS and Endpoints

PCI Security Standards Council

Consider All Data Sources

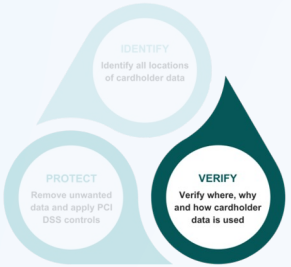


A thorough data discovery process should support:

- A wide range of data types
- Email, audio and image sources
- Structured and unstructured data
- Binary Large Objects (BLOBs)
- User data files - server and endpoint
- Multi-layered files
- Shadow files
- Collaboration tools
- Deleted files
- Data in memory

PCI Security Standards Council

Verifying Data With Purpose



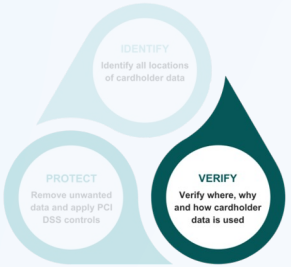
Evaluate and verify

Gather input from teams across the business to understand:

- The data they need to operate
- The purpose of the data
- What data is no longer required

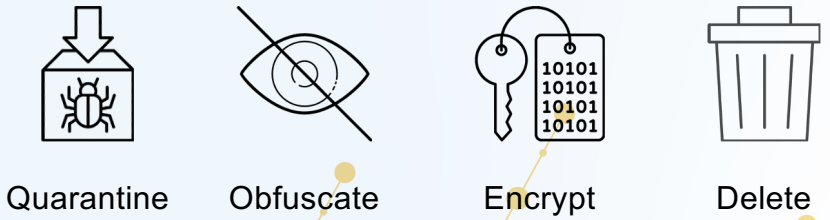
PCI Security Standards Council

Make Remediation a Shared Responsibility



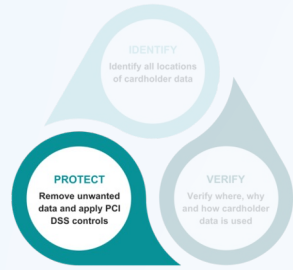
After initial discovery share findings with system and/or data owners and:

- Verify all cardholder data are inside the cardholder data environment
- Highlight any data residing outside the cardholder data environment
- Agree an appropriate treatment plan



PCI Security Standards Council

Protecting Data With PCI DSS v4.0

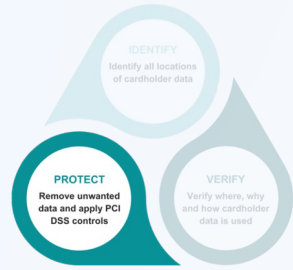


Apply PCI DSS v4.0

- Cleanse unnecessary data stores
- Remediate cardholder data outside the defined CDE
- Manage and maintain scope beyond assessment for sustainable compliance

PCI Security Standards Council

Data Discovery Supports 27 Controls in PCI DSS v4.0



Requirement 1: Install and maintain network security controls
Data discovery validates the network boundaries of scope and demonstrates data flows are up to date.

Requirement 3: Protect stored account data
Discovery scans identify account data, including SAD, wherever it is stored. Periodic scans can confirm that data has been deleted when it has passed its retention period.

Requirement 6: Develop and maintain secure systems and software
Discovery scans verify that account data is not present in non-production environments

Requirement 12: Support information security with organizational policies and programs
As part of periodic scope revalidation, data discovery verifies in-scope systems and data repositories. Advanced discovery solutions offer remediation-in-place for data found in unexpected locations.

PCI Security Standards Council


IDENTIFY
VERIFY
PROTECT
IDENTIFY
Identify all locations of cardholder data
PROTECT
Remove unwanted data and apply PCI DSS controls
VERIFY
Verify where, why and how cardholder data is used
PCI Security Standards Council

Evidence-Based Scoping in the Zettabyte Era

- Historic data collection, rapid digital transformation and growing data volumes has led to excessive storage of data and a multitude of unintended repositories
- Eliminate assumptions about data with an evidence-based approach to **identify** all data
- Evaluate and **verify** data, to understand the information that is valuable and serves a legitimate purpose
- **Protect** data based on its sensitivity and dispose of data no longer required
- Establish a continuous data awareness process (Identify—Verify—Protect) for PCI DSS scoping and effective data management.
- Sustainable compliance starts with data awareness

PCI Security Standards Council

PCI Security Standards Council

GROUND LABS

Thank You For Listening

Visit us at **www.groundlabs.com**

Download from
https://go.groundlabs.com/gl-pcidss4