The only deployment ready solution that secures and controls access to digital assets

Secure.Data Overview

This presentation runs automatically. To move backward, forward, or stop the presentation, use these buttons.

protegrity
securing digital assets

Risk

"There is much more illegal and unauthorized activity going on in cyberspace that corporations admit to their clients, stockholders and business partners or report to law enforcement. Incidents are widespread, costly and commonplace."

Source: Patrice Rapalus, Computer Security Institute Director

Risk

"Now, more than ever, government and private sector need to work together to share information and be more cognitive of information security so that our nation's critical infrastructures are protected from cyber-terrorists."

Source: Bruce J. Gebhardt, FBI Executive Assistant Director

Risk

90% of respondents detected computer security breaches within the last twelve months.

Source: 2002 CSI/FBI Computer Crime and Security Survey

Risk

80% acknowledged financial losses due to computer breaches.

Source: 2002 CSI/FBI Computer Crime and Security Survey

Risk

44% were willing and/or able to quantify their financial losses, averaging over $2.4 million dollars

Source: 2002 CSI/FBI Computer Crime and Security Survey

Risk

The most serious financial losses occurred through theft of proprietary information.

Source: 2002 CSI/FBI Computer Crime and Security Survey

Risk

These losses averaged over $4.1 million dollars.

Source: 2002 CSI/FBI Computer Crime and Security Survey

Risk

How do you protect your most valuable proprietary data?

Agenda

- Overview of Protegrity
- Marketplace
- Solution
- Differentiators
- Customer Base
- Summary

Protegrity: Market

- Pressures on Corporations come from several areas
  - Regulations
    - US GLBA, US HIPAA, US FDA 21 CFR Part 11
    - EU Privacy Data Protection Acts/Safe Harbor, Canada's PIPEDA
    - Australia, Hong Kong, Japan Privacy Acts etc.
    - Argentina Privacy Acts etc.
    - Visa U.S.A. CISP
  - Audit
    - Internal Audit for company privacy standards
    - External Audit for Compliance
  - Unauthorized malicious access
    - External Hackers, Industrial espionage
    - Internal malicious access

Protegrity: Market

- Corporate data has a small percentage that is “Critical Threat” data
  - On average about 10% of data in a database is confidential

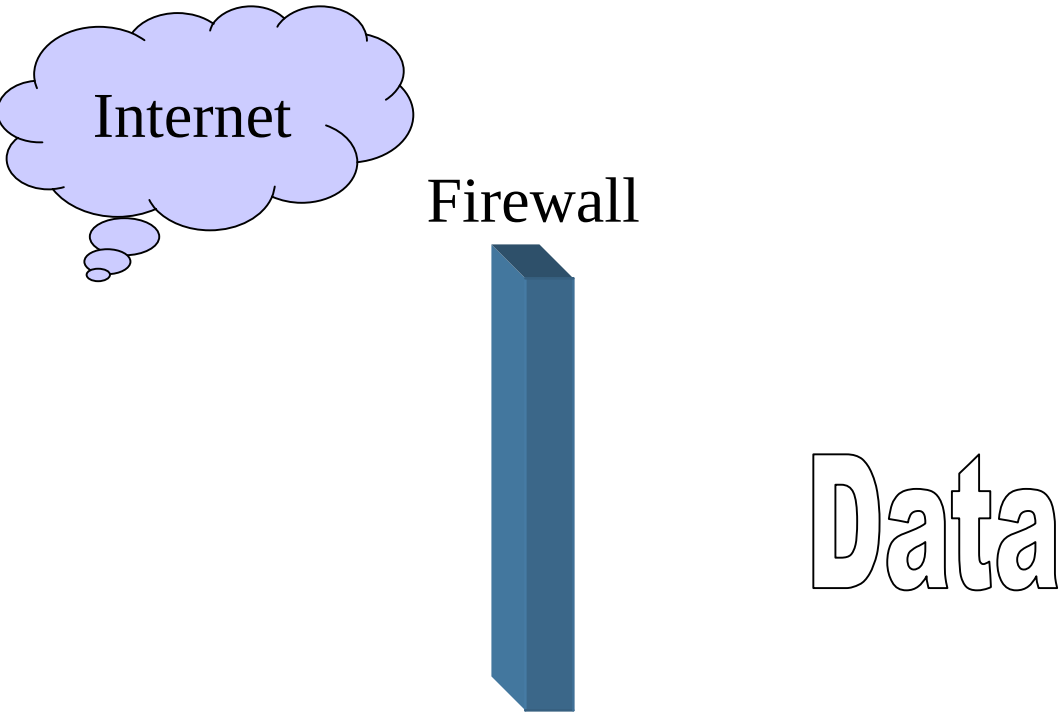
- Breaches of this information occurs from two basic sources
  - External threats account for 40% of disclosures
  - Internal threats account for 60% of disclosures

- The Regulations, Unauthorized access and Audit all demand the same Basic and fundamental conditions be met:
  - Absolute control of access to “Critical Threat” Data
  - Absolute audit of all access to “Critical Threat” Data

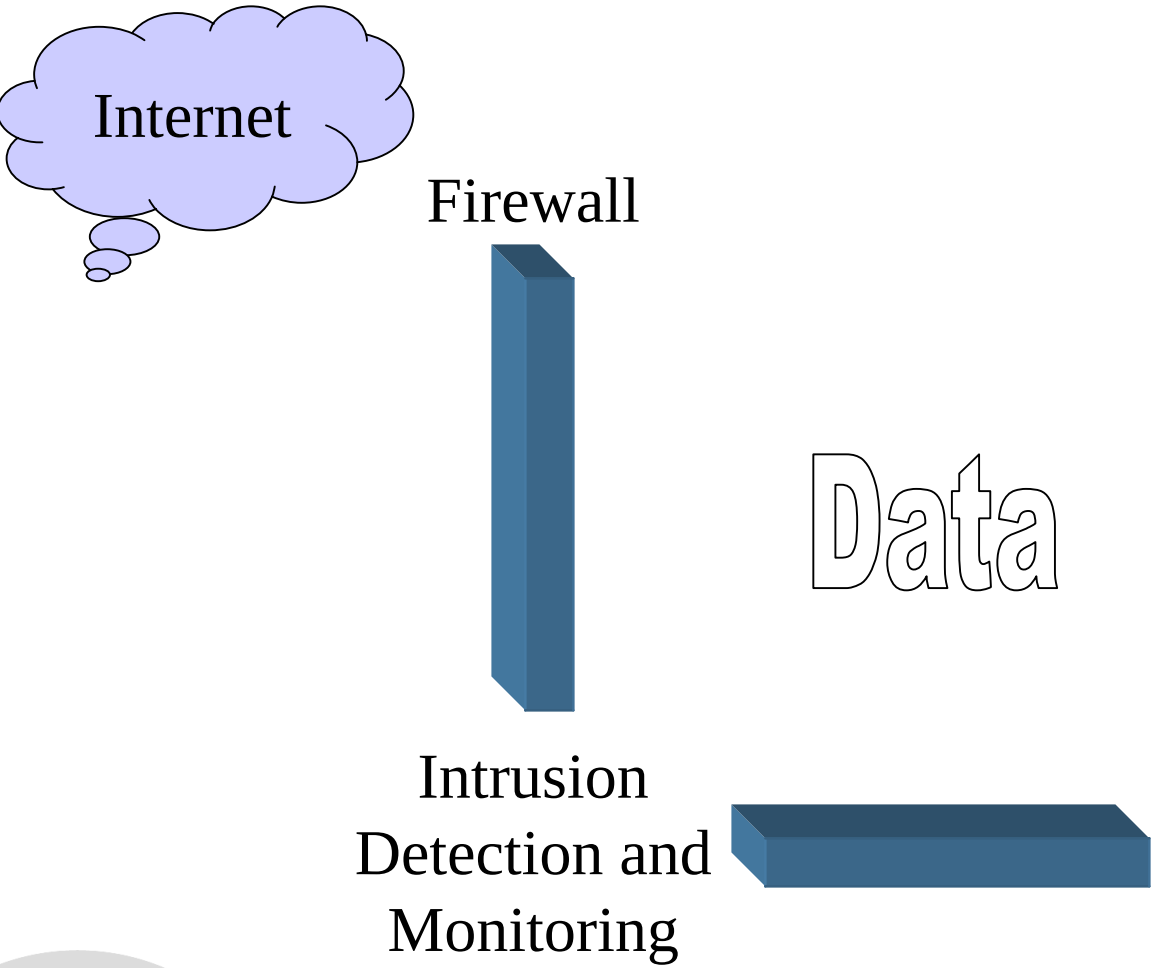
Protegrity: Market

- Companies build walls of protection around this “Critical Threat” Data
  - Four categories of security are commonly deployed

Protegrity: Market

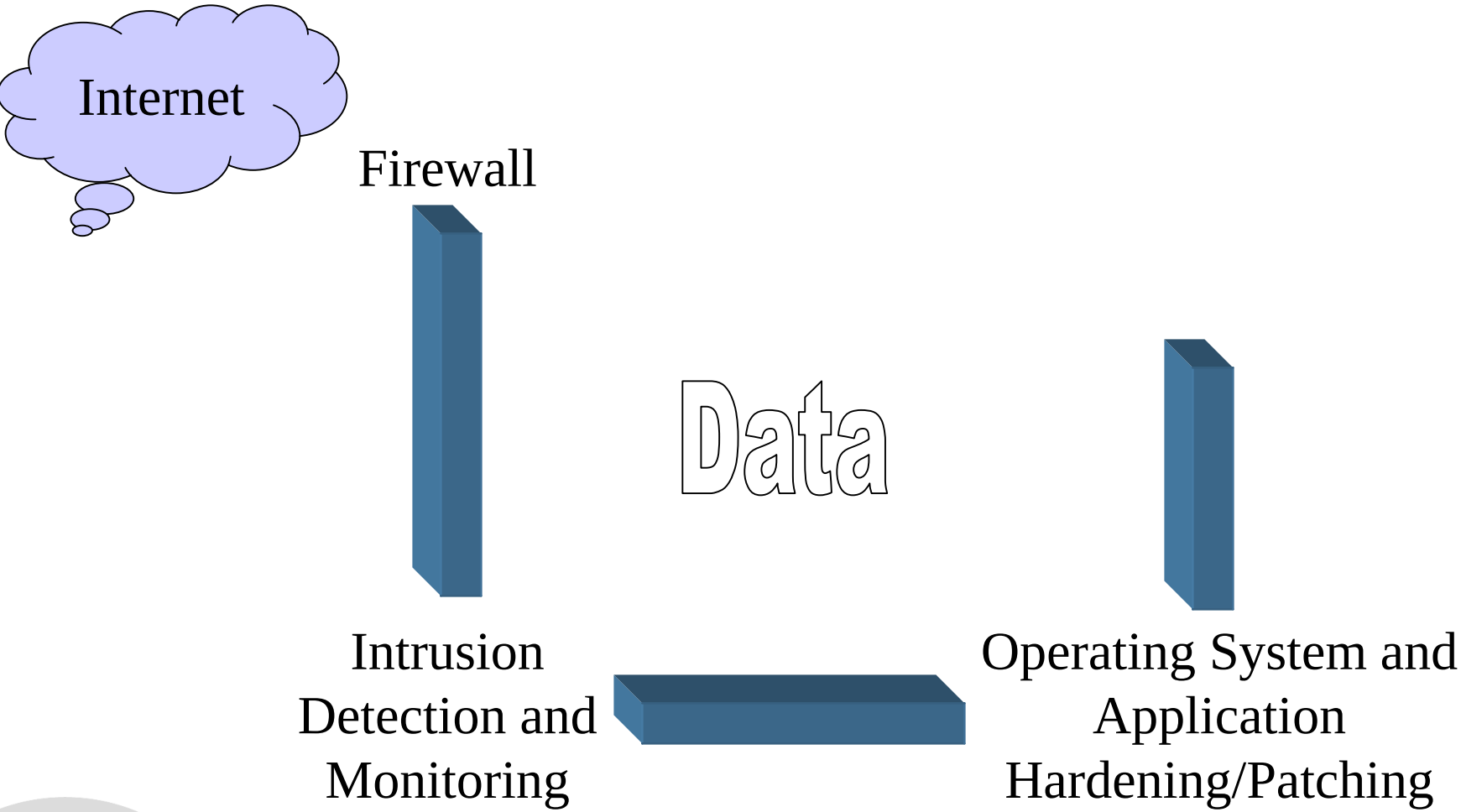


Protegrity: Market



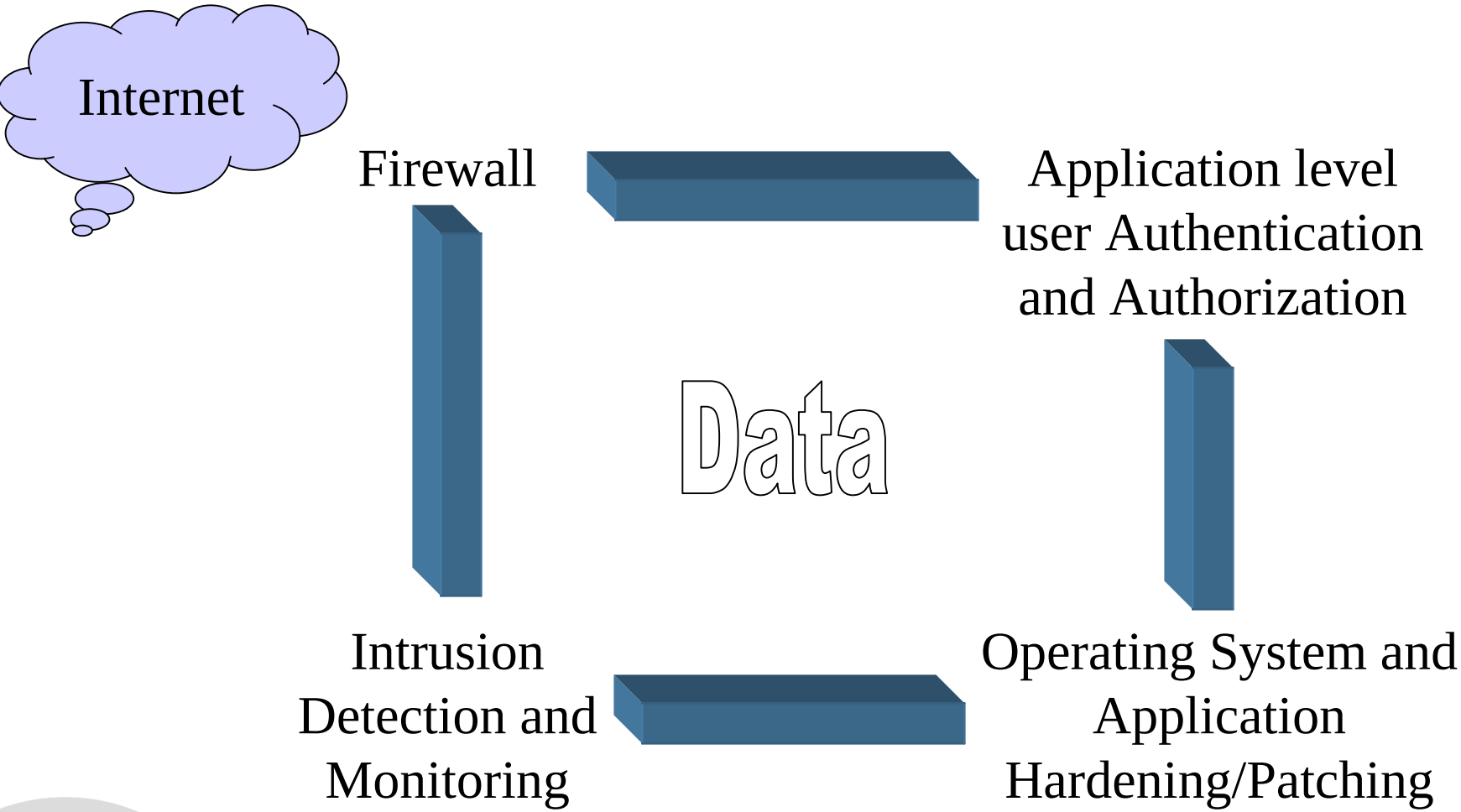
protegrity
securing digital assets

Protegrity: Market



protegrity
securing digital assets

Protegrity: Market



protegrity
securing digital assets

Protegrity: Market

- The Goal
  - Absolutely control access to “Critical Threat” Data
  - Absolutely audit all access to “Critical Threat” Data

- Who still has unrestricted and un-auditable access to “Critical Threat” Data?
  - Application Programmers
  - Database Administrators
  - Super User Accounts, Root/Admin
  - Back up Tapes
  - Physical Access
  - Open Query Tools, Access, Crystal Reports, Excel
  - Hackers who penetrate your firewall

Protegrity: Solution

- Protegrity's Secure.Data Solution
  - Absolute control of access to "Critical Threat" Data
  - Absolute audit of all access to "Critical Threat" Data
  - Unique, proven and patented solution

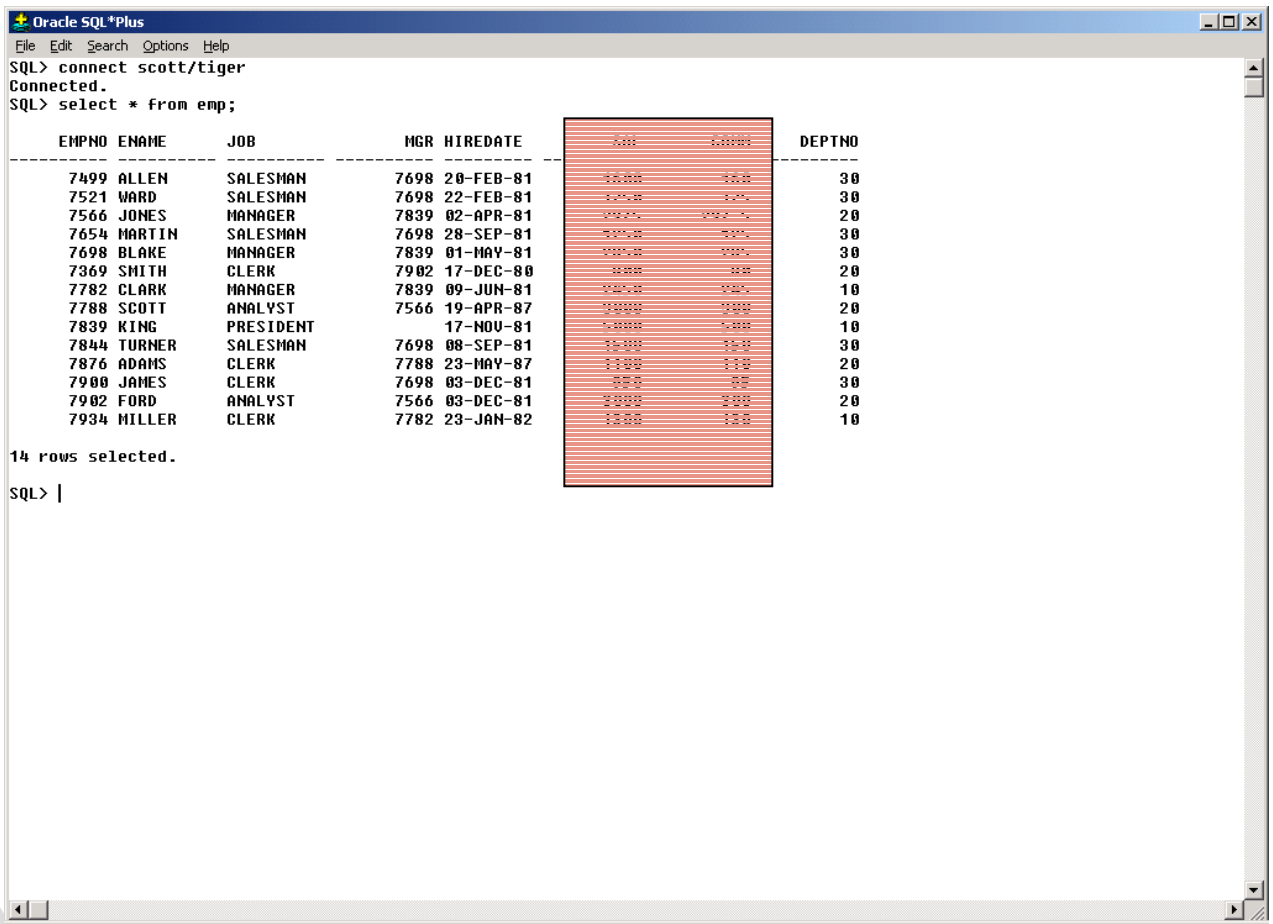
Protegrity: Solution

Four Critical Elements to Securing your “Critical Threat” Data

- Make the “Critical Threat” Data default to no access
  - This is done through selective strong encryption
- Provide access only to explicitly authorized entities
  - This is accomplished by a Role Based Access Control Engine
- Securely audit all access to “Critical Threat” Data
- Create a Segregation of Duties
  - This is done by having Access control and Administration as clearly separate duties

Protegrity: Solution

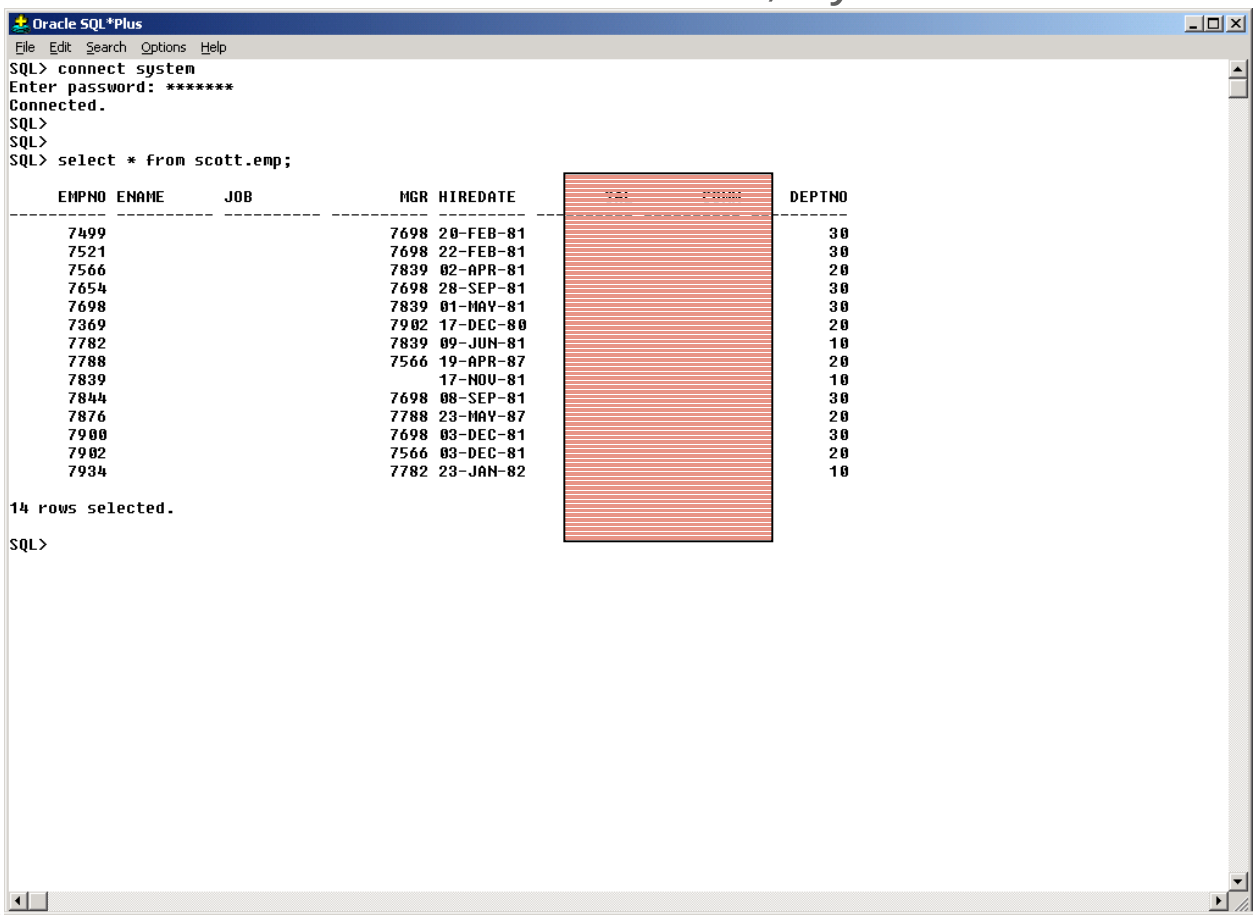
- Uncontrolled access without Secure.Data, Table owner Scott



protegrity
securing digital assets

Protegrity: Solution

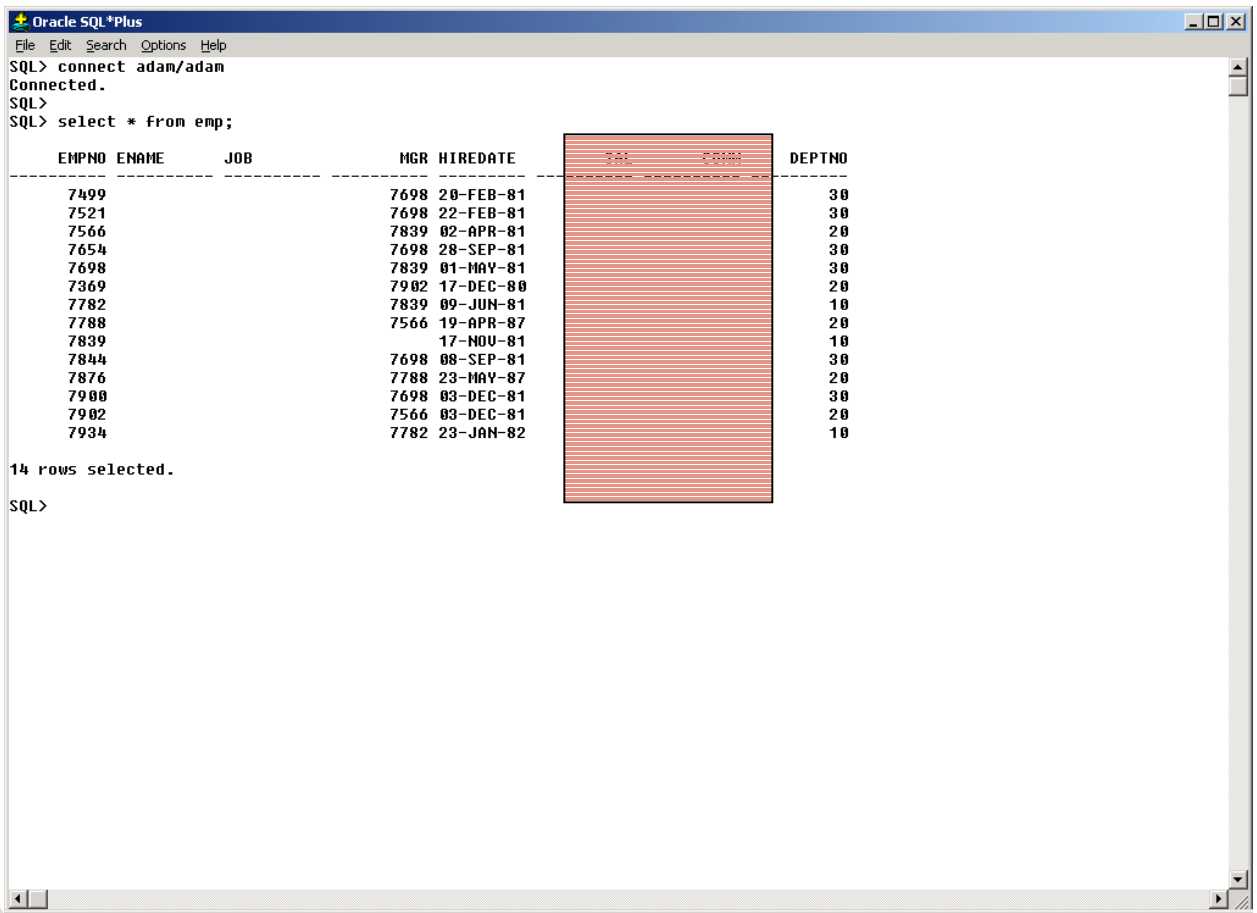
- Controlled access with Secure.Data, System



protegrity
securing digital assets

Protegrity: Solution

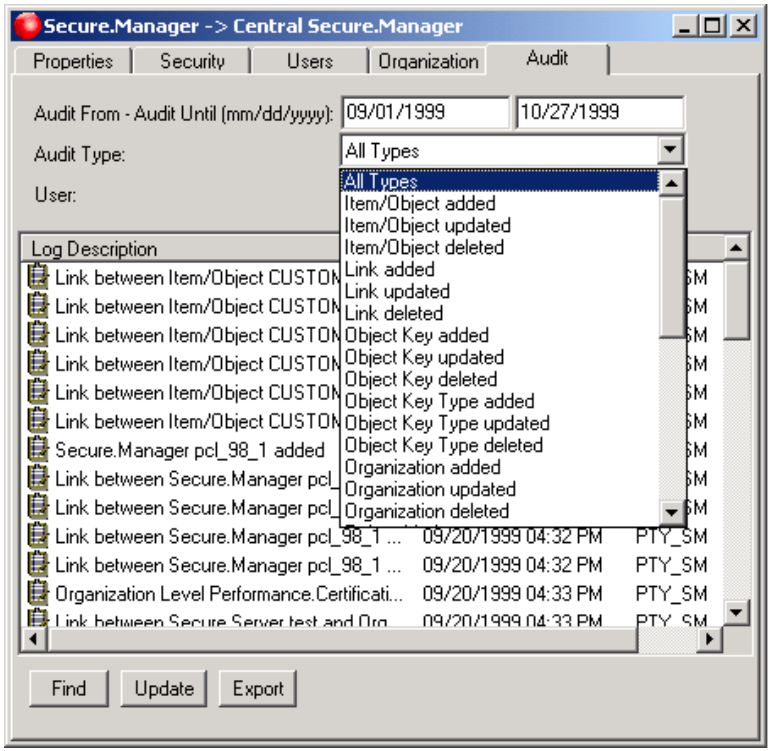
- Controlled access with Secure.Data, Unauthorized User

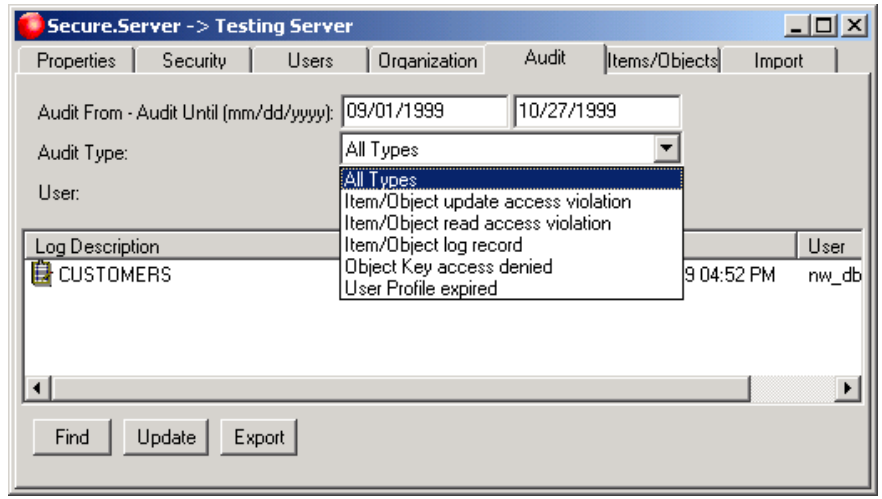


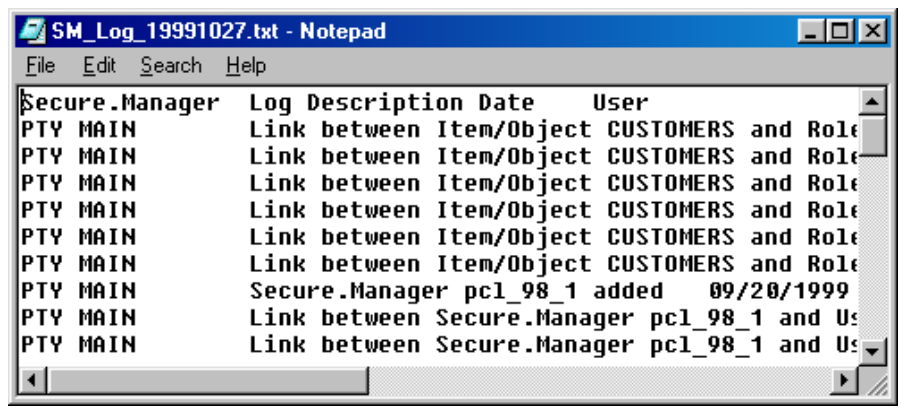
protegrity
securing digital assets

Protegrity: Solution

- Secure Audit of Access to “Critical Threat” Data and policy changes







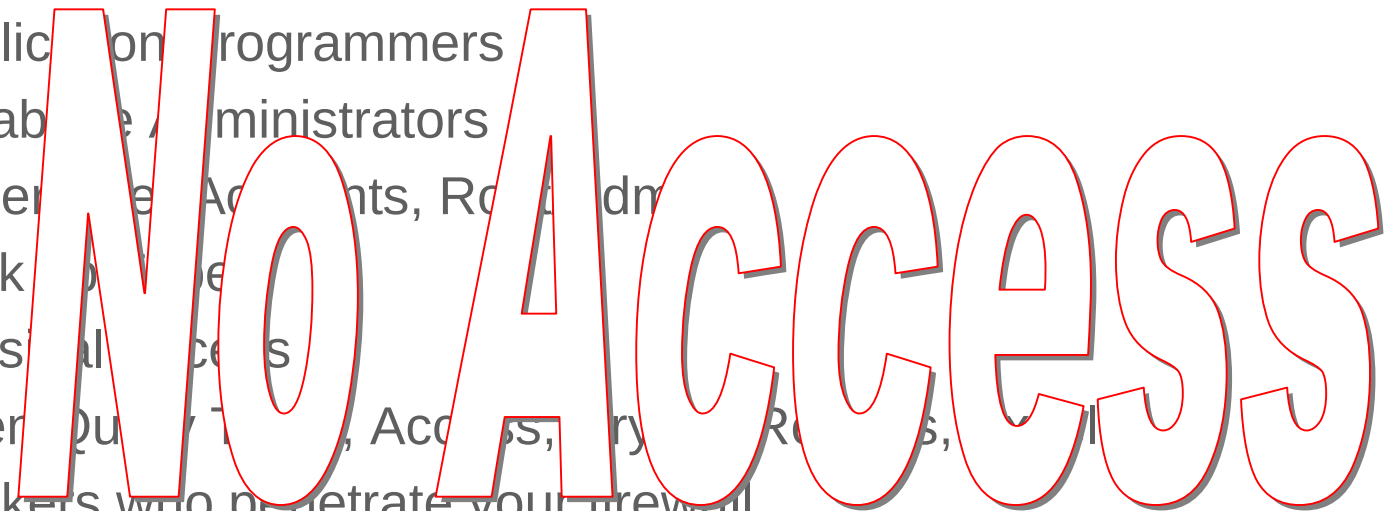
protegrity
securing digital assets

Protegrity: Solution

- With Secure.Data installed, who still has unrestricted and un-auditable access to “Critical Threat” Data?
  - Application Programmers?
  - Database Administrators?
  - Super User Accounts, Root/Admin?
  - Back up Tapes?
  - Physical Access?
  - Open Query Tools, Access, Crystal Reports, Excel?
  - Hackers who penetrate your firewall?

Protegrity: Solution

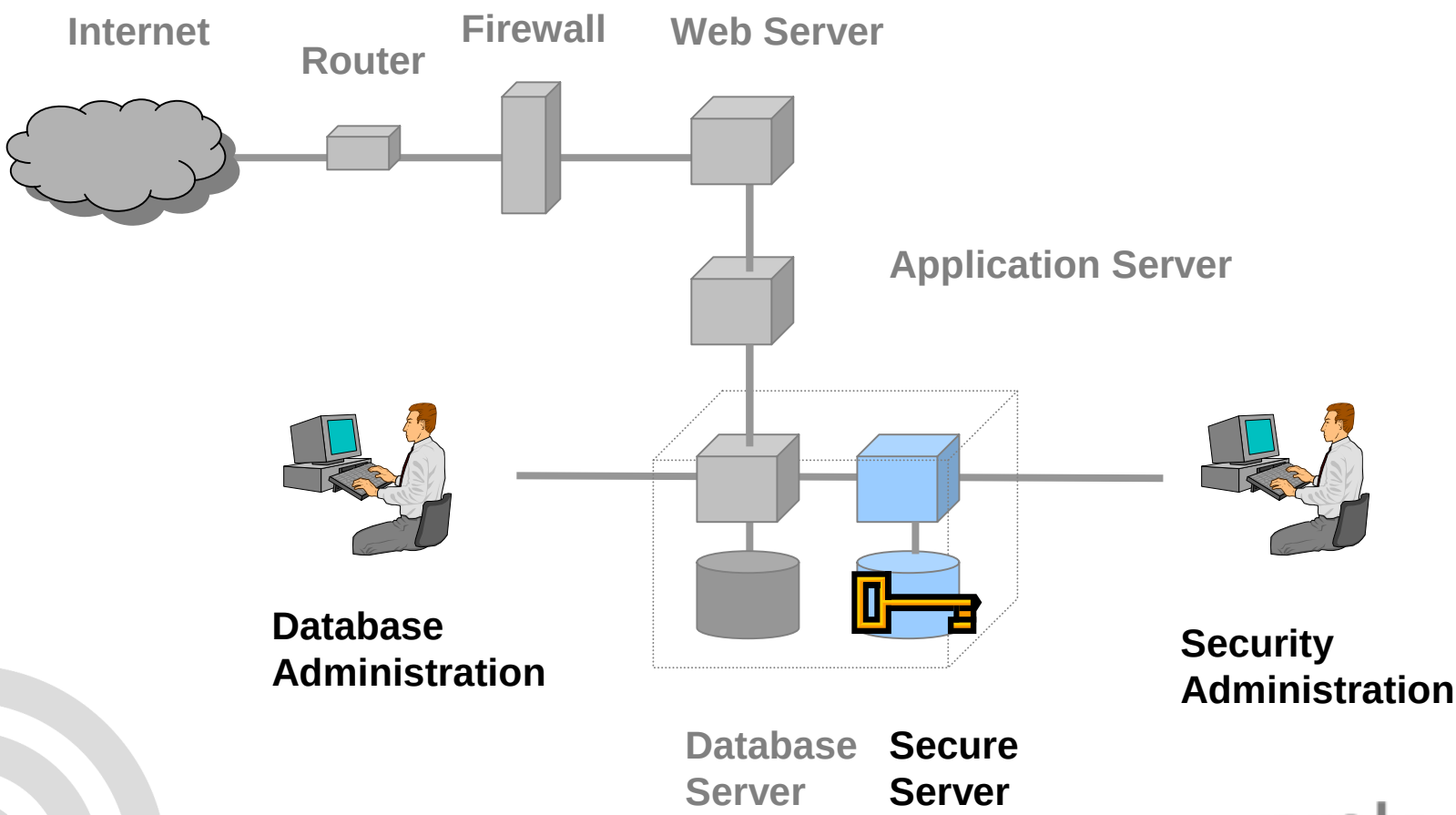
- With Secure.Data installed, who *still* has unrestricted and un-auditable access to “Critical Threat” Data?
  - Application Programmers
  - Database Administrators
  - Super[illegible] Accounts, Root/Admin
  - Back[illegible]
  - Physical Access
  - Open Query Tools, Access, Query Results, Applications
  - Hackers who penetrate your firewall



protegrity
securing digital assets

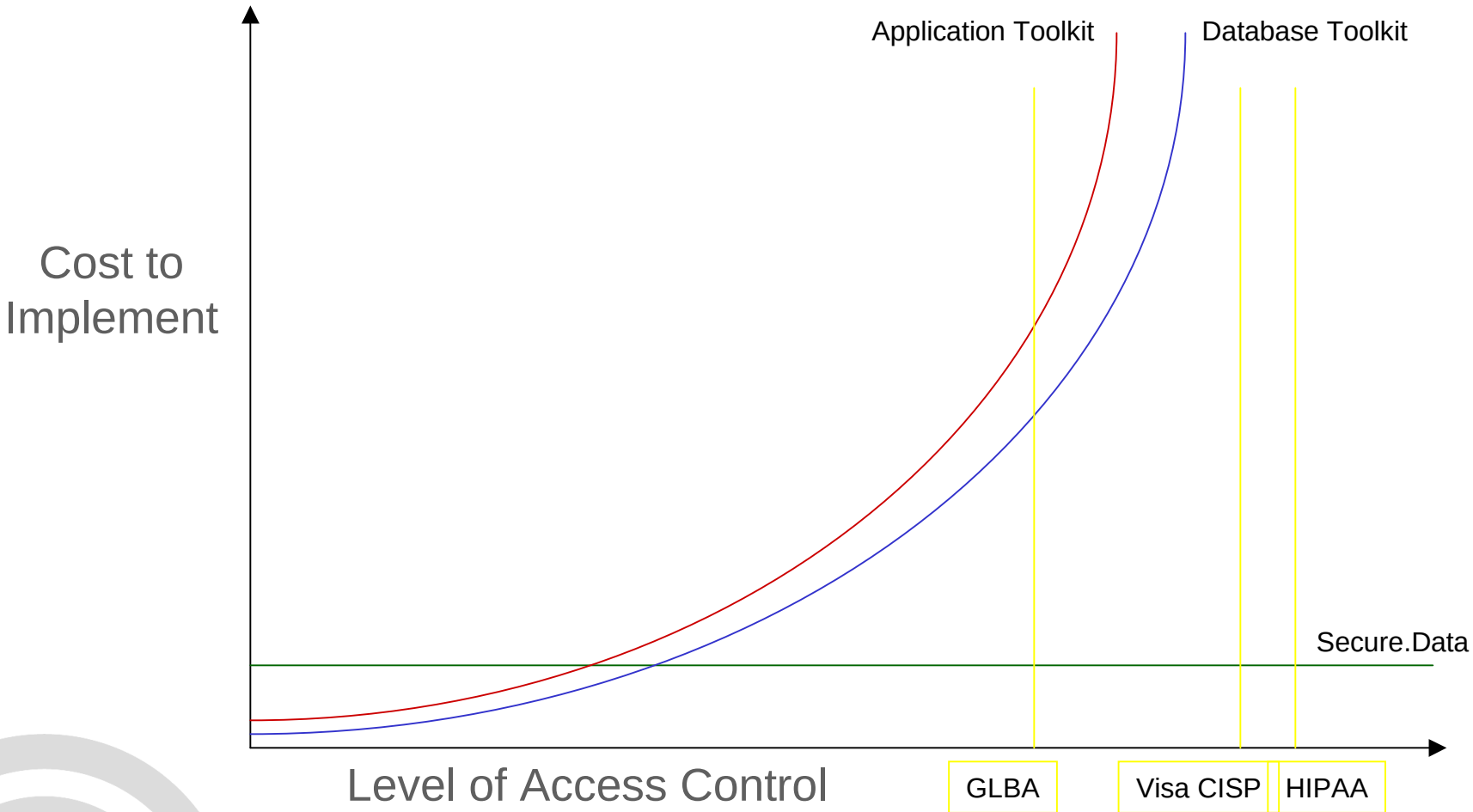
Protegrity: Solution Architecture

- Secure.Data Architecture



protegrity
securing digital assets

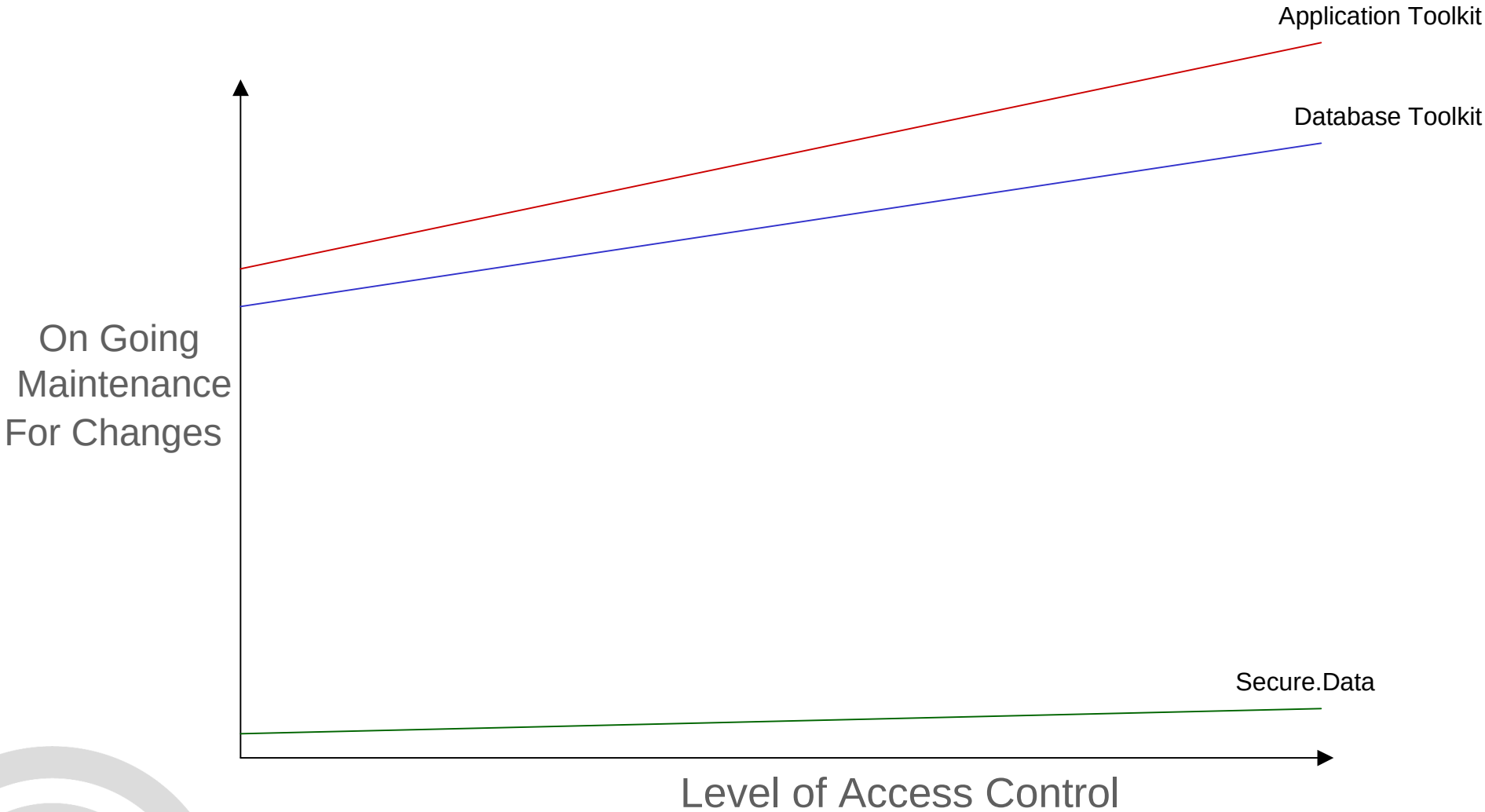
Protegrity: Competitive Advantage



Secure.Data vs. Competitors

protegrity
securing digital assets

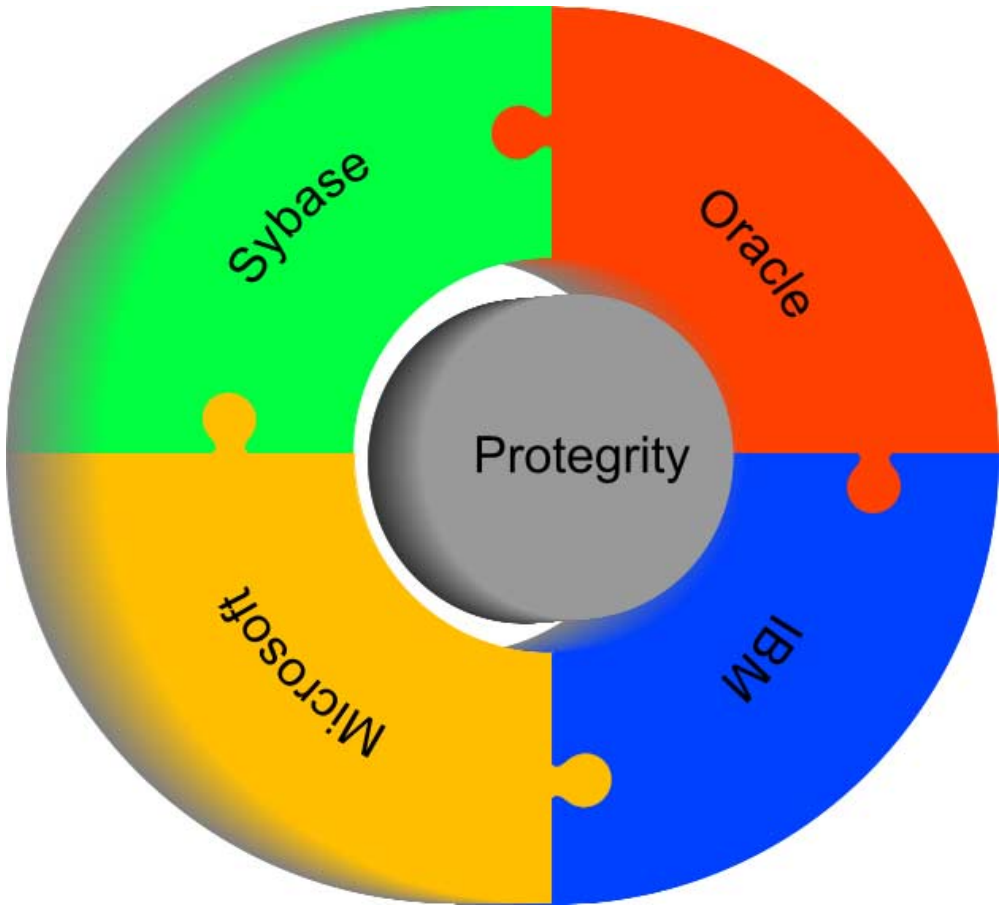
Protegrity: Competitive Advantage



Secure.Data vs. Competitors

protegrity
securing digital assets

Privacy Infrastructure for All Database Platforms



We Protect it!

protegrity
securing digital assets

Tangible Benefits of Secure.Data

- Prevent losses and liabilities to the company and executive management
- Enable new business initiatives
- Facilitate out-of-the-box compliance with new privacy and security requirements

Protegrity: Customer Base

- Who is using this new approach to protect their “Critical Threat” Data?

E-Commerce

Commercial Finance

Pharmaceutical

Consumer Finance

Healthcare

Investment Banking

Consumer Products

protegrity
securing digital assets

Summary:

- Elegant solution that solves a difficult and real problem

- Proven technology, protecting “Critical Threat” data in:
  - Investment Banks
  - Consumer Financial Companies
  - Pharmaceutical Companies
  - Commercial Financial Institutions
  - Healthcare Companies
  - Consumer Product Companies

The only deployment ready solution that secures and controls access to digital assets

www.protegrity.com

protegrity
securing digital assets