



The Security Division of EMC

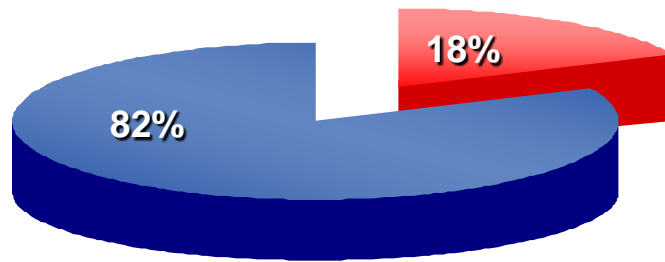
Information Risk Management *Security Solutions for Business Acceleration*

Matt Gaudio, CISSP

RSA, The Security Division of EMC

Is Your Information an Asset or a Liability?

“Despite massive investment in security technology and services...



... fewer than one in five companies feel that all their data is adequately protected.”

Today's Security Challenges

Information Security is perceived
as a **business inhibitor**,
not a ***business accelerator***



Business Initiatives

IT Security

ineffective

not protecting what's important
resource-constrained

costly

too many security products
too many security procedures

inhibiting compliance

too many controls
manual, complicated, labor-intensive

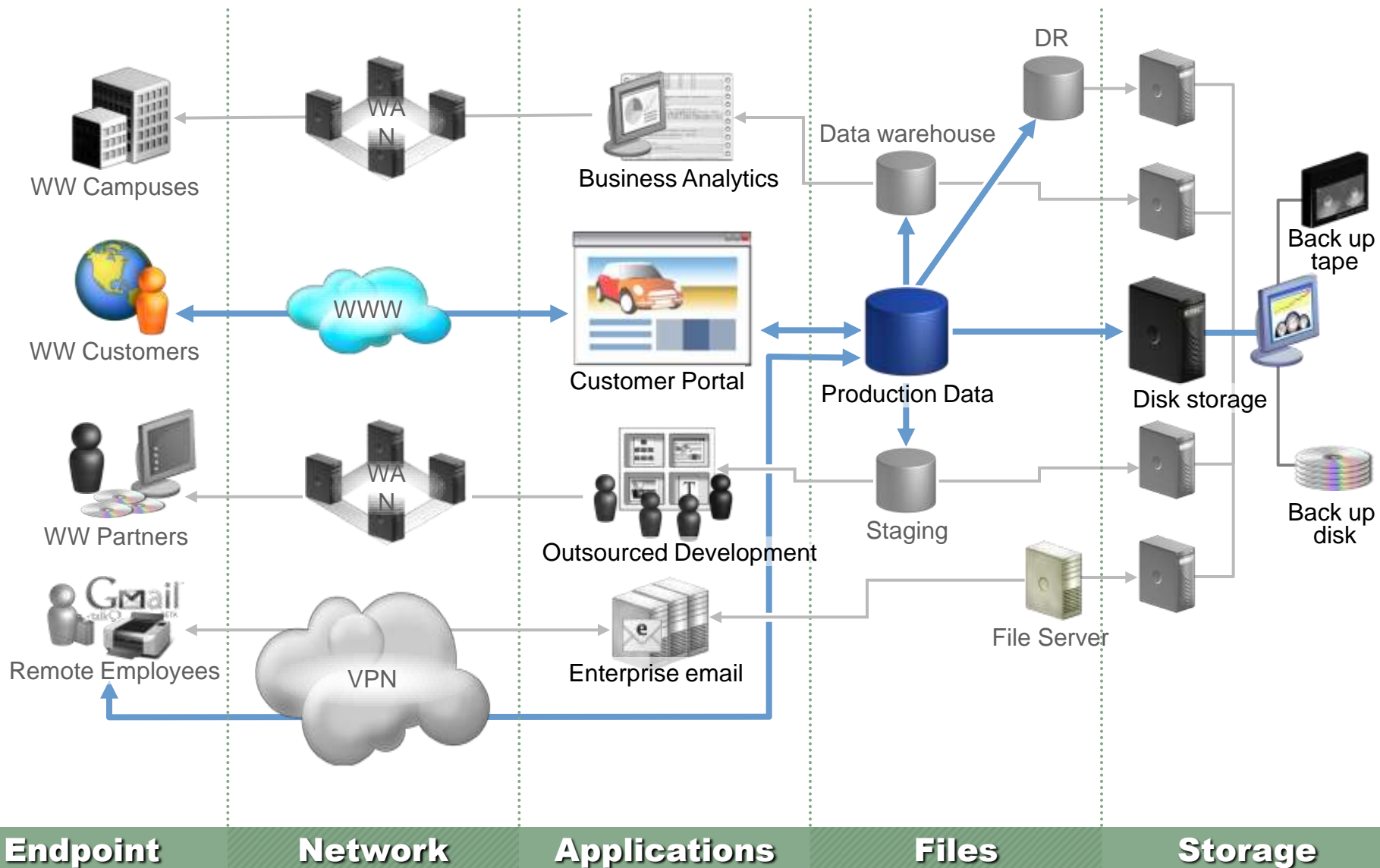
increasing complexity

information growth
infrastructure complexity
regulatory landscape
distributed organizations

Need a holistic approach that makes security
more effective and aligns it with the business

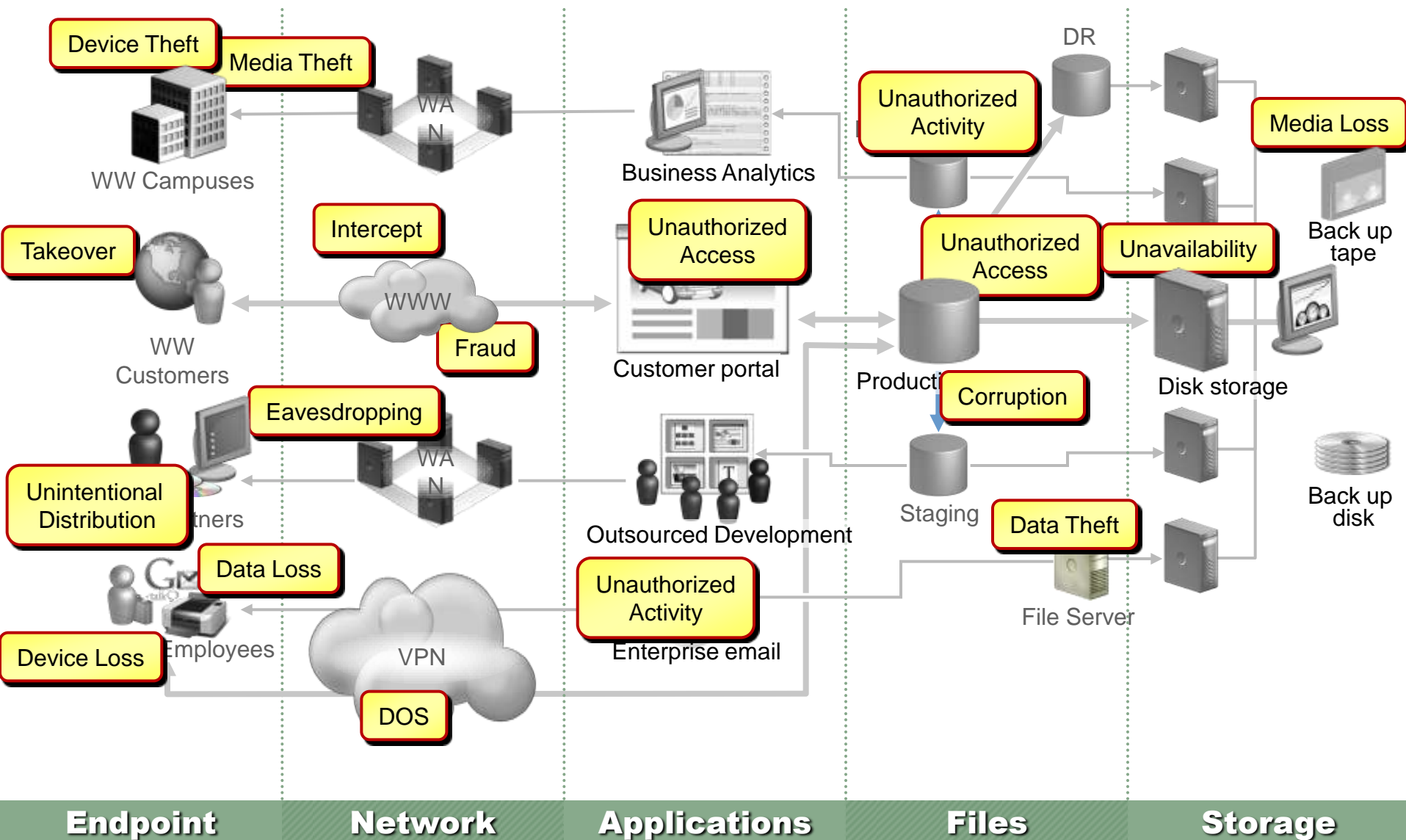
Why is Information Security So Difficult?

...because sensitive information is always moving and transforming



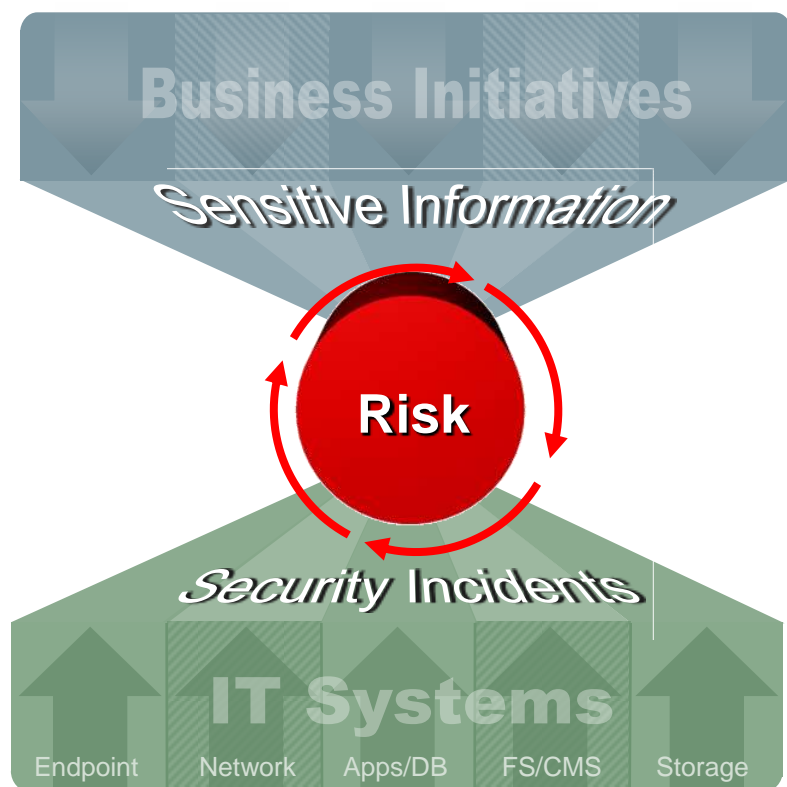
Why is Information Security So Difficult?

...and every movement & transformation has unique risks



Information Risk Management

a strategy for protecting your most critical assets



Information-centric

Clarifies business context and reveals potential vulnerabilities

Risk-based

Establishes a clear priority for making security investments

Repeatable

Based on foundation of broadly applicable best practices and standard frameworks

Reveals where to invest, why to invest, and how security investments map to critical business objectives



The Security Division of EMC

Understanding Risk

“**Risk** is the combination of the probability of an event and its consequences.” (ISO definition)

Risk Components

Assets (Information, infrastructure, etc.)

Threats (Sources, Objectives & Methods)

Vulnerabilities (People, Process & Technology)

Managing Risk

**RSA & EMC
Can Help**

Avoid – Eliminate the source of the risk

Control – Implement controls to reduce risk

Accept – Be aware but take no action

Ignore – Refuse to acknowledge risk

Transfer – Assign risk to other agency

Risk Aligns Security Investments to the Business

Revenue Growth

Cost Reduction

Customer Retention

Business Continuity

Compliance

Sensitive Information

What information is important to the business?

Risk

What risks are we willing to accept, what risks do we need to protect against to enable the business?

Security Incidents

What bad things can happen?

Endpoint

Network

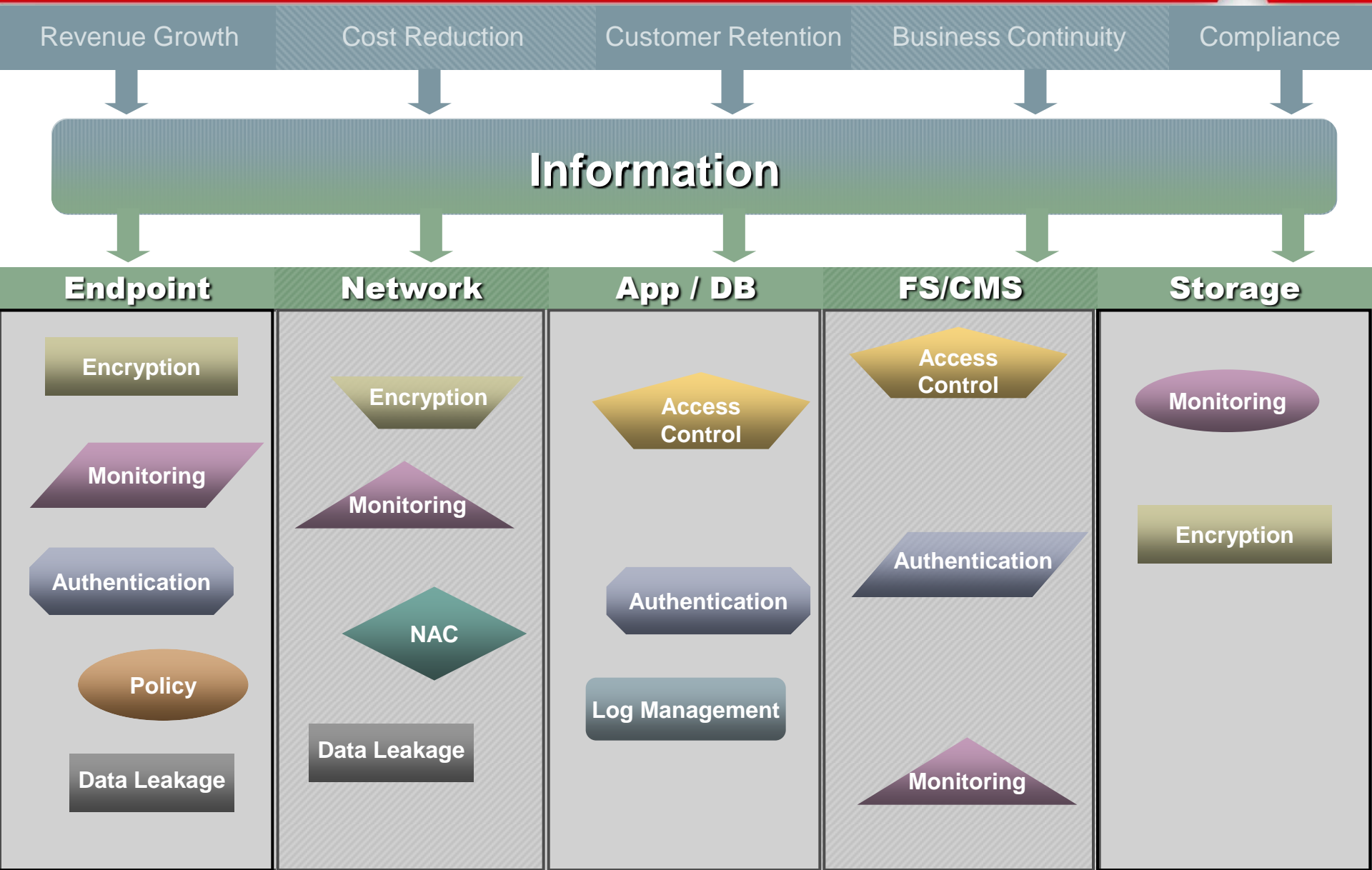
App / DB

FS/CMS

Storage

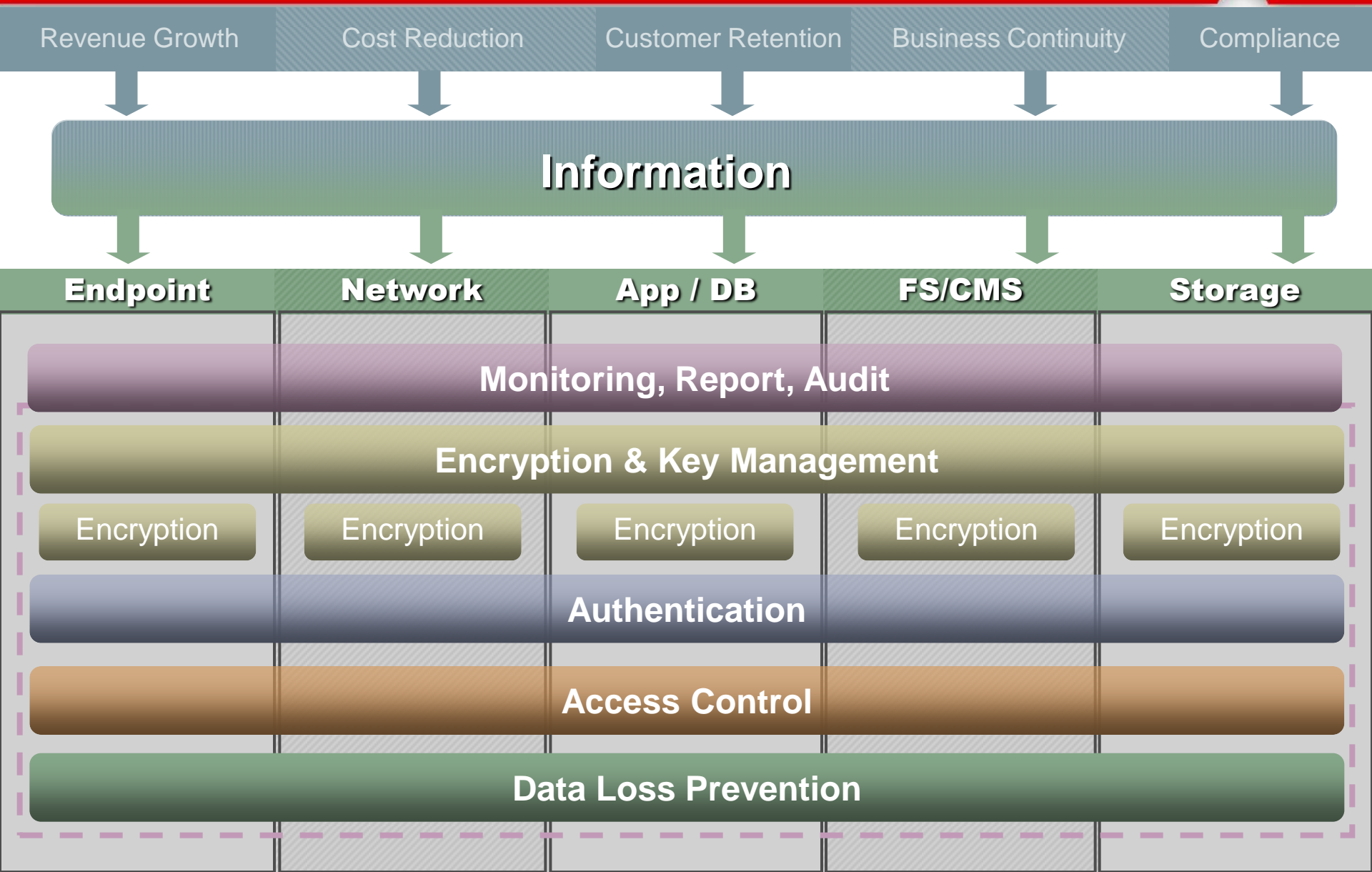
The Silo Approach to Risk Management

Non-integrated Narrowly Targeted Controls



A Framework-Based Approach to Risk Management

Solutions That Address a Wide Range of Constantly Changing Risks



Information Risk Management Framework

The Payoff

“IT organizations that have taken a risk-oriented, framework-based approach have been able to reduce their number of controls by 30% to 70%*”

Cost effective investments - Prioritization of controls according to risk

Streamlined compliance - Fewer, more repeatable controls

Clear business alignment - Shared assessment of risk

RSA can help to enable this type of approach



Information Risk Management

The Process



Discover and Classify

Discover all sources of sensitive information across the infrastructure

Define Policy

Describe how sensitive information be protected

Data, People, Infrastructure

Enforce Controls

Establish a control framework and implement appropriate controls to enforce the policy

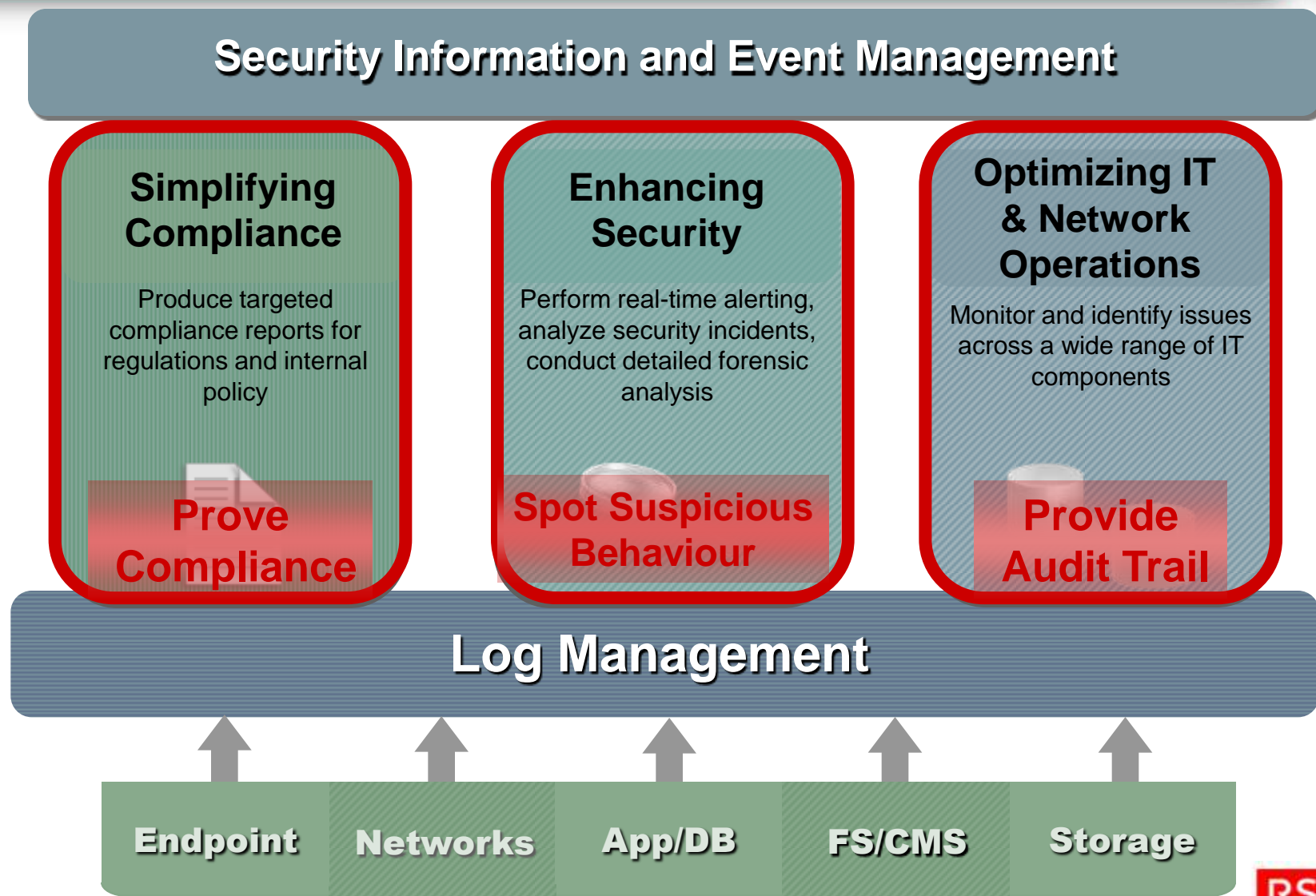
Data Controls

Access Controls

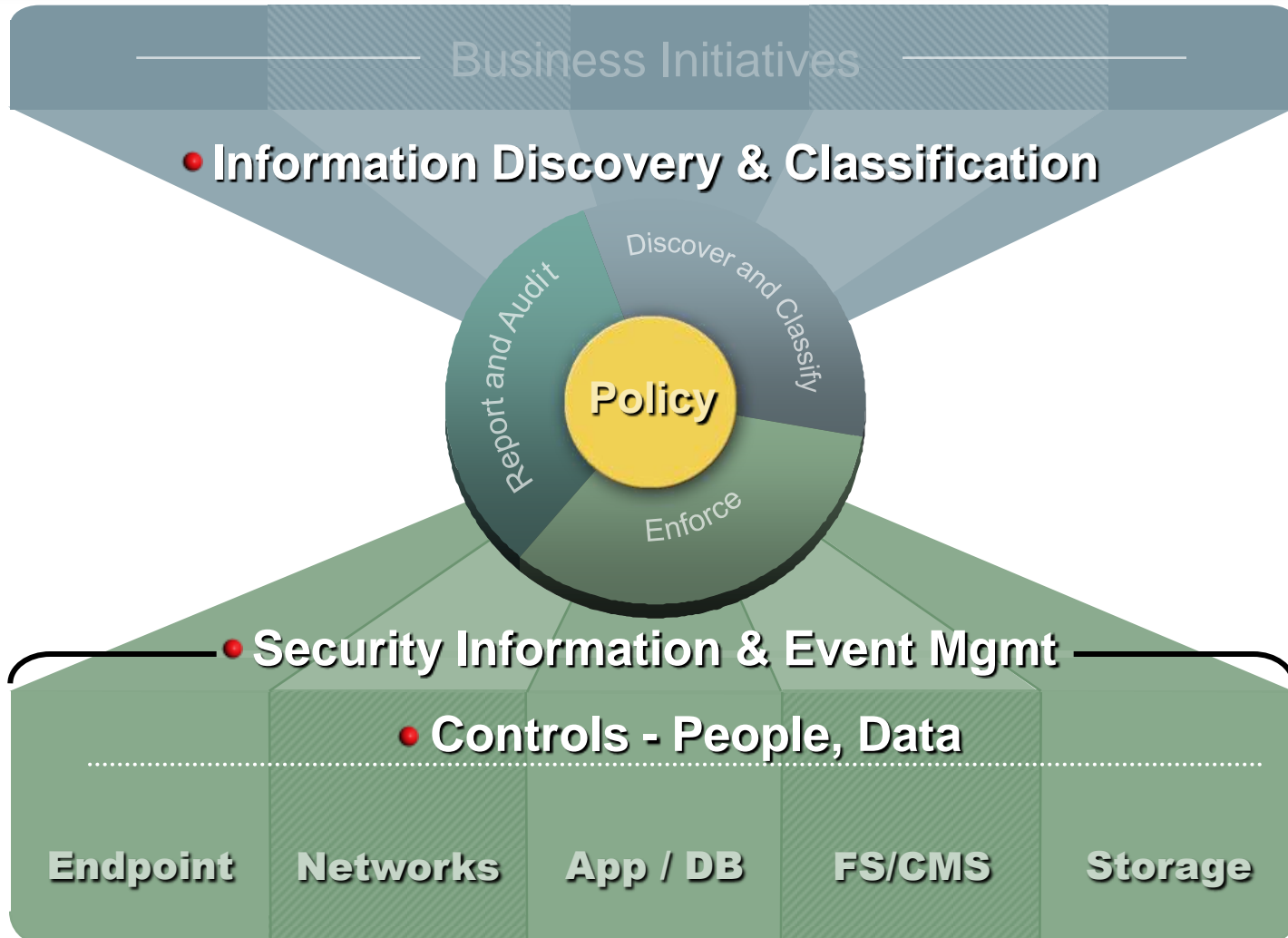
Report and Audit

Audit the environment to ensure and document compliance with policy

Security Information and Event Management



Information Risk Management





The Security Division of EMC

Thank you!