Protecting What Matters Most

Chris Hauser

Senior Security Engineer

IMPERVA®

Security Amuck

- Brief intro and background
- What's at stake? 3 attacks
- Threat Actors and motivations
- Anatomy of an attack
- Q & A

THE FOLLOWING PRESENTATION IS MY OWN OPINION AND NOT THAT OF IMPERVA (*excuse non-pc slides)

SONY
PICTURES

Cyber attacks
are bad and getting

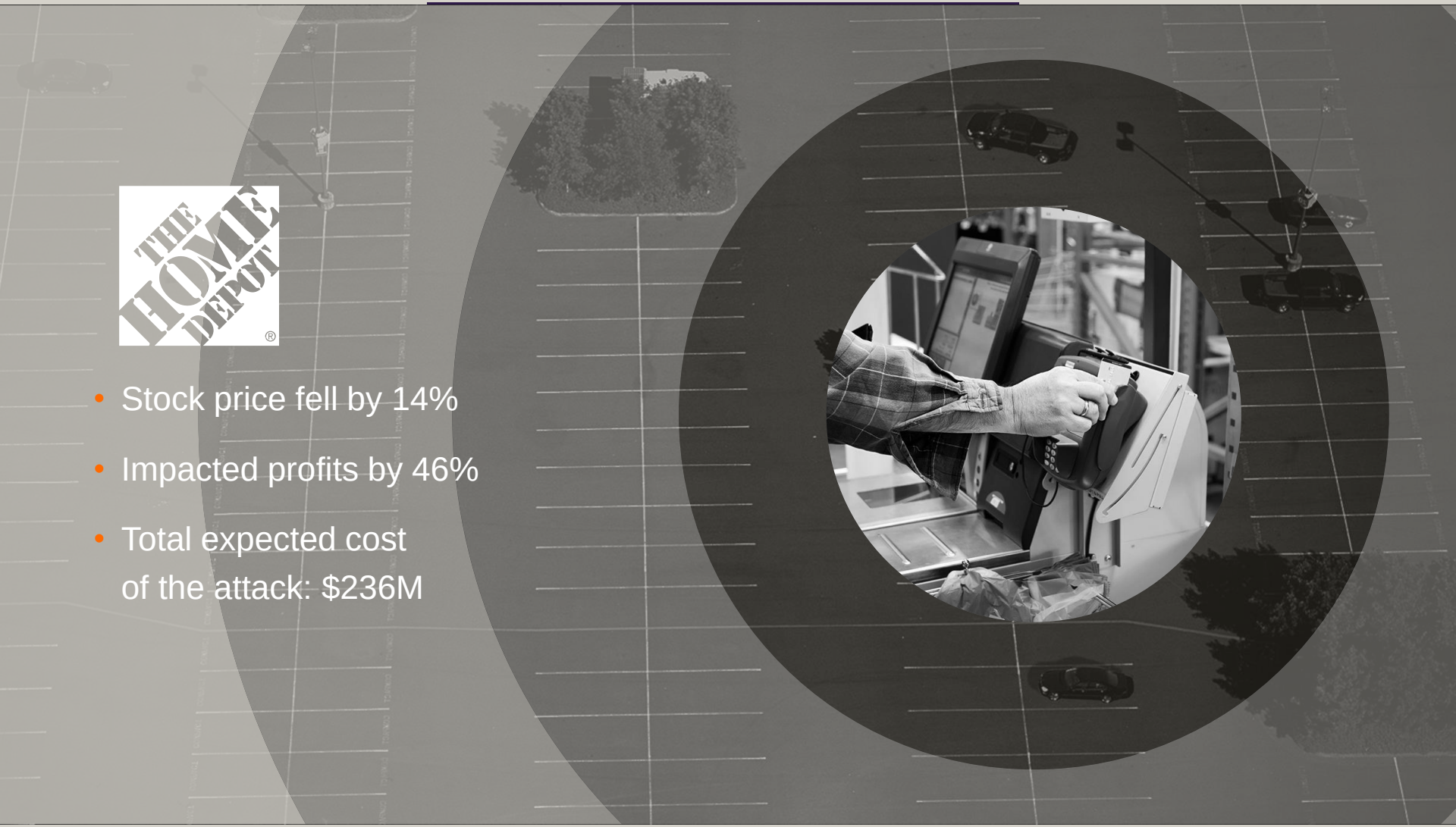
WORSE

SONY PICTURES

- Leaked films and scripts
- Employee lawsuit
- Media field day

Significant economic

FALLOUT



- Stock price fell by 14%
- Impacted profits by 46%
- Total expected cost of the attack: $236M

IMPERVA®

- 80 million records exposed
- Massive Costs for Remediation

Threat Actors

Economic Espionage

Stealing Intellectual Property (IP) and raw data, and spying

- Motivated by: policy, politics, and nationalism
- Preferred Methods: Targeted attacks

Organized Crime

Stealing IP and data

- Motivated by: profit
- Preferred Methods: Targeted attacks, Fraud

Hacktivists

Exposing IP and data, and compromising the infrastructure

- Motivated by: political causes, ideology, personal agendas
- Preferred Methods: Targeted attacks, Denial of Service attacks

Nuisance Threats

Easy Money Scams

- Motivated by: profit, personal agendas
- Preferred Methods: SPAM, Botnets, Defacement, Destructive malware

All Threat Actors Are Not Equal

	Nuisance Threats	Economic Espionage	Organized Crime	Hacktivists
				
Objective	**Launch Points & Nuisance**	**Economic Advantage**	**Financial Gain**	**Defamation, Press & Policy**
Example	Botnets & Spam	Advanced Persistent Threat	Russian Business Network	Anonymous & Lulzsec
Targeted	✗	✓	✓	✓
Persistent	✗	✓	✓	✗

Attacks which are targeted and persistent pose the greatest challenge and the greatest risk.

IMPERVA®

Threat Tactics, Technics and Procedures

- Gain Entry
  - Watering hole
  - Malicious email attachment
  - Spear phishing
- Upload toolkit
- Increase footprint
- Look for access to data
- Exfiltration of data
- Repeat as necessary
- Profit!

IMPERVA®

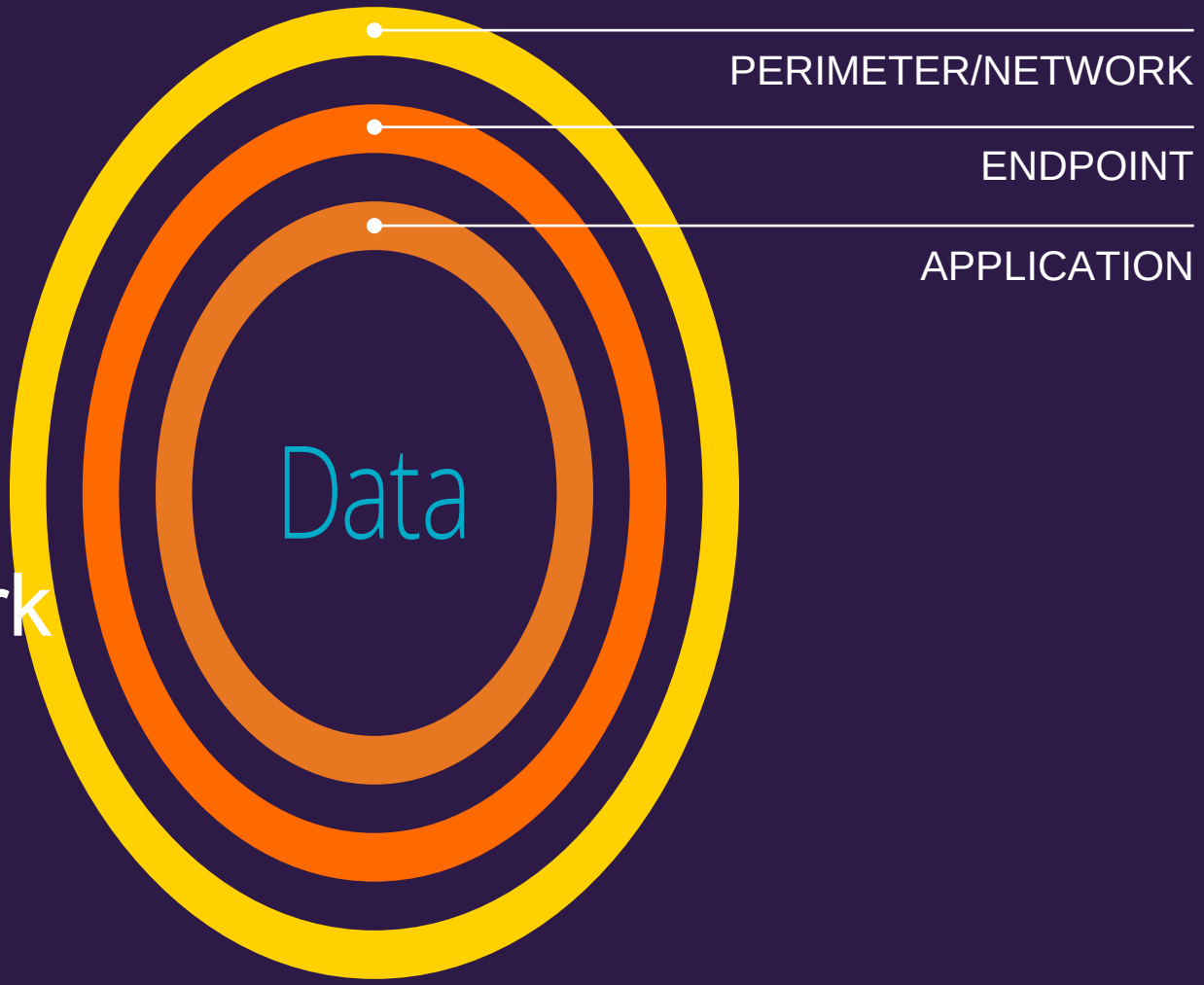
There are two kinds of big companies in the United States. There are those who've been hacked… and those who don't know they've been hacked.

FBI DIRECTOR JAMES COMEY

October 2014

IMPERVA®

Traditional security doesn’t work



IMPERVA®

Traditional security doesn't work

PERIMETER/NETWORK

Insiders bypass the perimeter and compromise your data

Malware leverages unsuspecting users

Applications and data moving to the cloud

IMPERVA®

Traditional security doesn't work

PERIMETER/NETWORK

Insiders bypass the perimeter and compromise your data

Malware leverages unsuspecting users

Applications and data moving to the cloud

IMPERVA®

Traditional security doesn't work

PERIMETER/NETWORK

Insiders bypass the perimeter and compromise your data

Malware leverages unsuspecting users

Applications and data moving to the cloud

IMPERVA®

Traditional security doesn't work

PERIMETER/NETWORK

Insiders bypass the perimeter and compromise your data

Malware leverages unsuspecting users

Applications and data moving to the cloud

IMPERVA®

Traditional security doesn't work

PERIMETER/NETWORK

ENDPOINT

Conspiring with users to steal data

Duping users into opening up vulnerabilities

BYOD

IMPERVA®

Traditional security doesn't work

PERIMETER/NETWORK

ENDPOINT

Conspiring with users to steal data

Duping users into opening up vulnerabilities

BYOD

IMPERVA®

Traditional security doesn't work

PERIMETER/NETWORK

ENDPOINT

Conspiring with users to steal data

Duping users into opening up vulnerabilities

BYOD

IMPERVA®

Traditional security doesn't work

PERIMETER/NETWORK

ENDPOINT

Conspiring with users to steal data

Duping users into opening up vulnerabilities

BYOD

IMPERVA®

Traditional security doesn't work

PERIMETER/NETWORK

ENDPOINT

APPLICATION

Hackers breach applications effectively

IMPERVA®

Traditional security doesn't work

PERIMETER/NETWORK

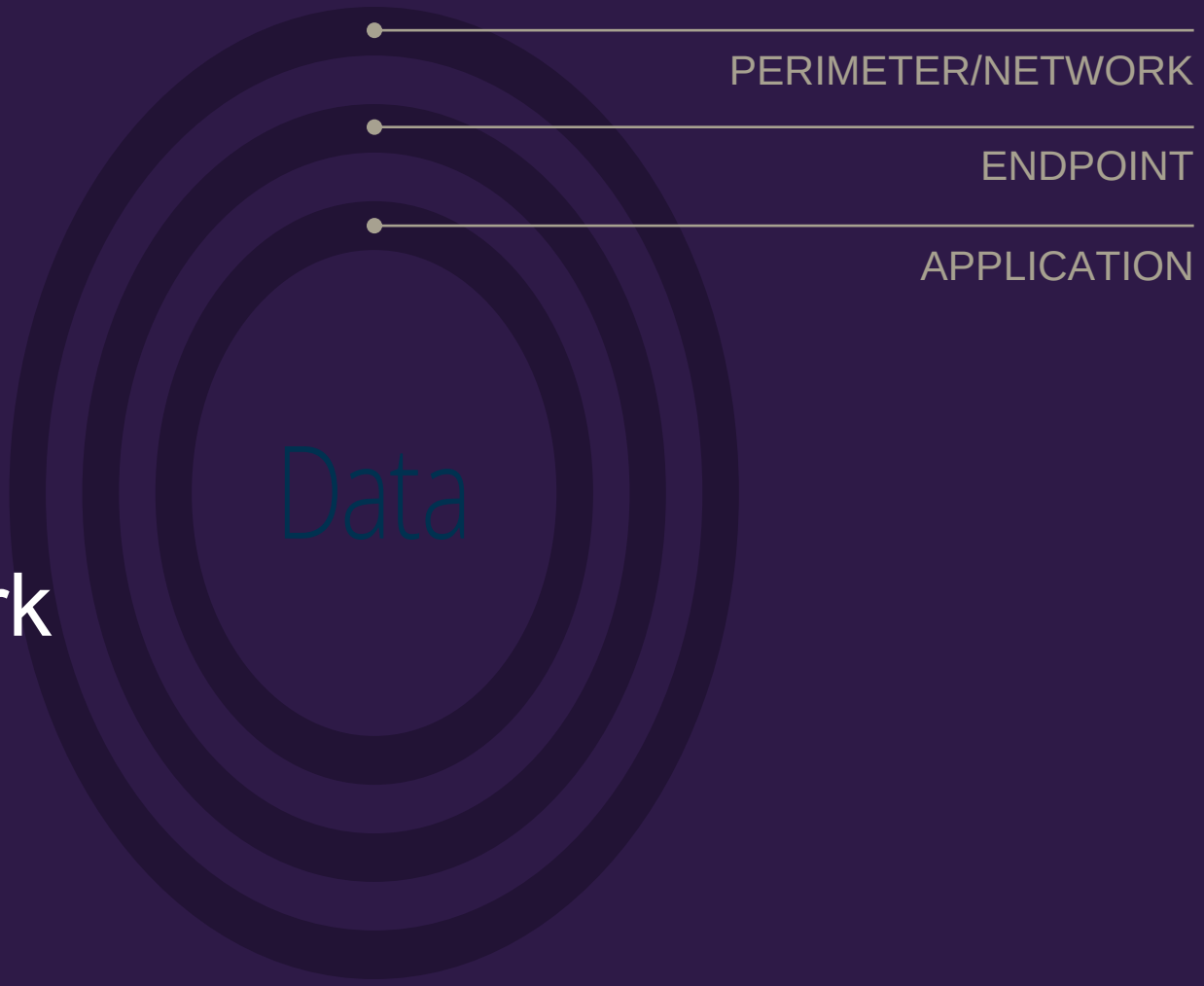
ENDPOINT

APPLICATION

Hackers breach applications effectively

IMPERVA®

Traditional security doesn’t work

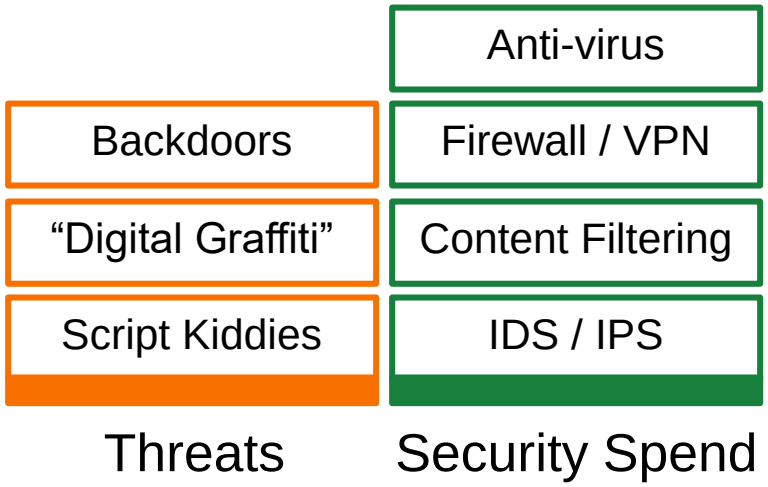


IMPERVA®

The Spending Disconnect

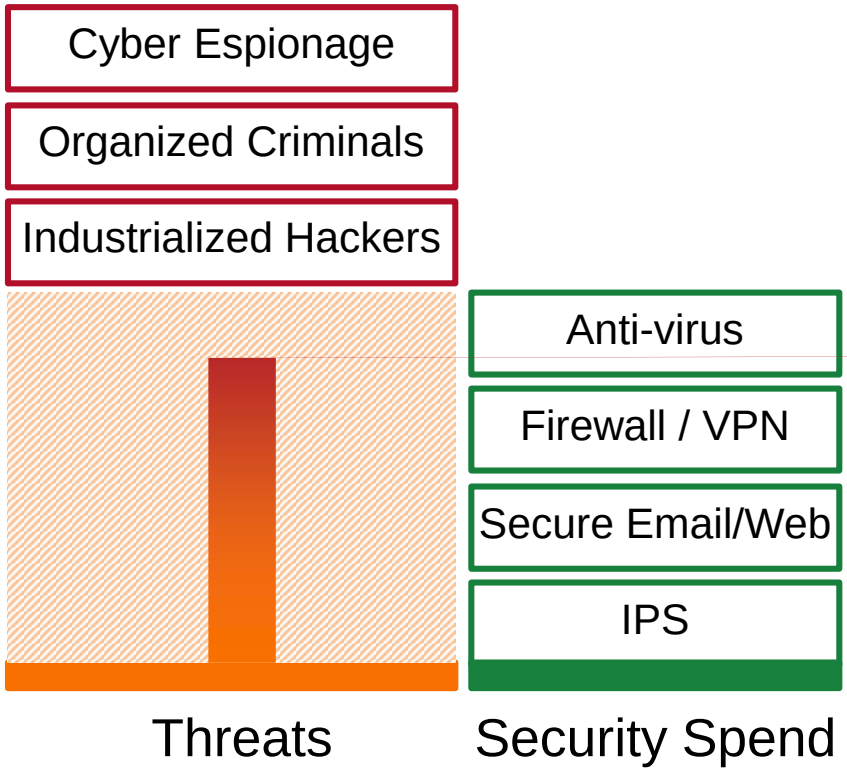
The Threats Have Changed

2001



Security Spending Hasn’t

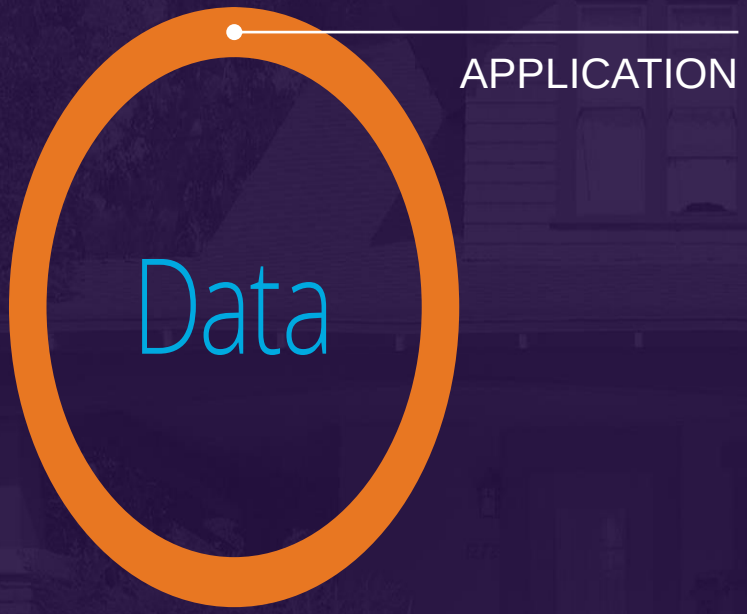
2016



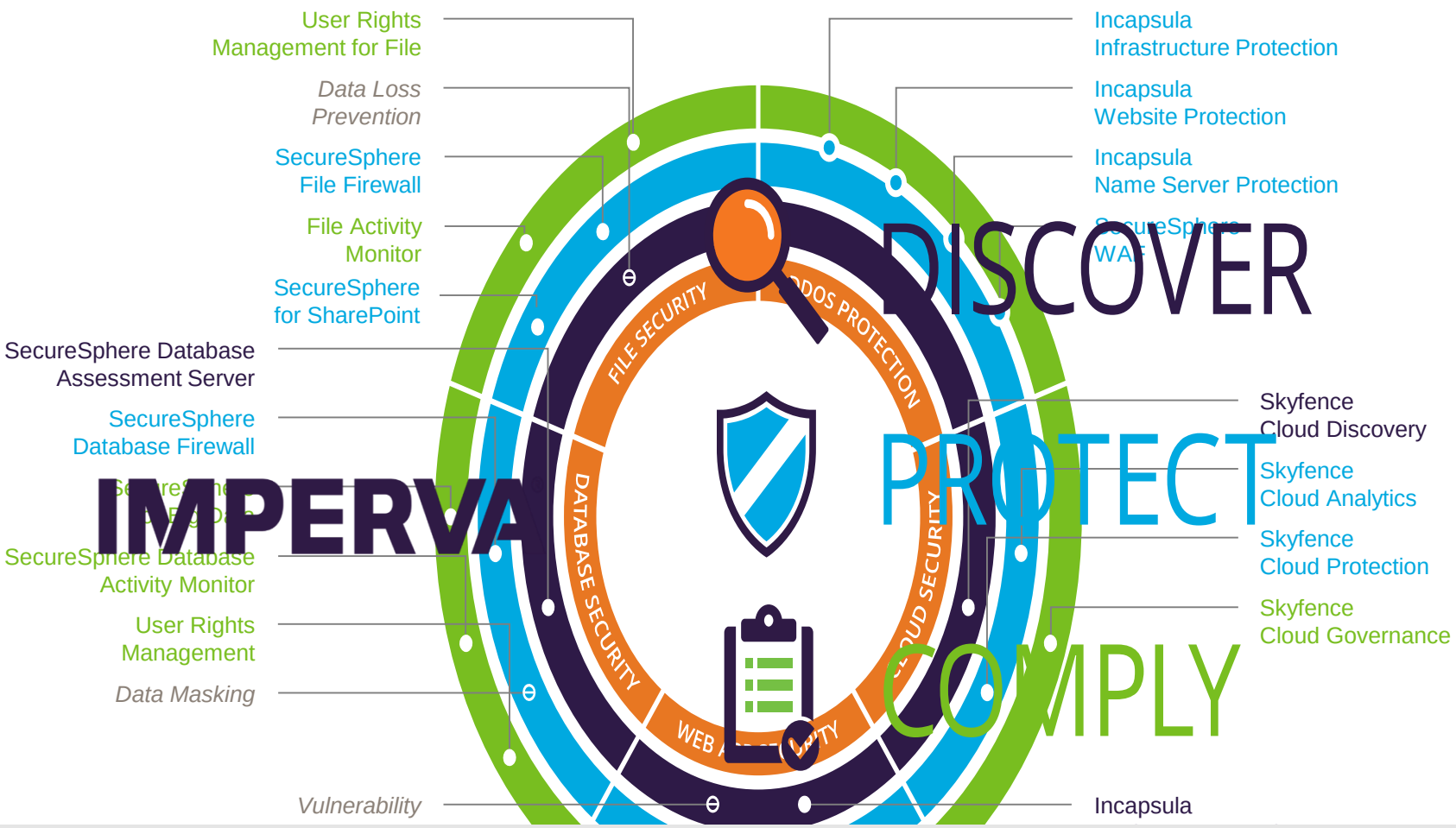
Sources: Gartner, Imperva analysis


Traditional
security

Protect what's INSIDE



- Protects structured and unstructured data where it resides: databases and file servers
- Protects where it’s accessed: Web applications
- Guards against both outside threats and internal actors


User Rights Management for File
Data Loss Prevention
SecureSphere File Firewall
File Activity Monitor
SecureSphere for SharePoint
SecureSphere Database Assessment Server
SecureSphere Database Firewall
SecureSphere Database Activity Monitor
User Rights Management
Data Masking
Vulnerability
Incapsula Infrastructure Protection
Incapsula Website Protection
Incapsula Name Server Protection
SecureSphere WAF
DISCOVER
PROTECT
COMPLY
IMPERVA
FILE SECURITY
DDOS PROTECTION
DATABASE SECURITY
CLOUD SECURITY
Skyfence Cloud Discovery
Skyfence Cloud Analytics
Skyfence Cloud Protection
Skyfence Cloud Governance
Incapsula


Protecting
DATA AND APPS
is exactly what Imperva does

IMPERVA®

Questions ?