

BOOLE™
s e r v e r

 **SecureGrade™**

www.securegrade.com

The Data-Centric Approach

security as a business enabler



 System Integration
& Security Software Technology

Malcolm Gardner BEng (Hons) CEng MIET
Technical Sales Director - SecureGrade

Contents

- **Context**
- **Data-centric Security**
- **Implementing Data-centric Security**
- **Conclusions and the Future**

Context

Context

The IDC forecast study 2011

- in 2011, >1.8 zettabytes created and replicated
- 9x increase in 5 years
- < 1/3 has any protection
- ~ 1/2 of information that should be protected is protected.

Data challenges not just related to volume

- Nature of information
- Importance of information
- Regulatory attention.

Compliance is increasingly important.

- DPA
- ISO 27001
- PCI-DSS
- SRA OFR.



1,000,000,000,000,000,000,000
ZiB

"The digital information created by every man, woman and child on Earth 'tweeting' continuously for 100 years ."

Protected
Unprotected

Share
Secure

Data availability vs Security

- Business routinely needs to exchange information
- Internal teams
- External business partners,
- Customers
- Authorities.

Not all data is the same

- Different sensitivities
- Different levels of access and security related to the value and sensitivity of content
- Different timescales and persistence

Data Types

Recent research by Forrester:
2 categories of data.

- **Custodial Data** (usually with a legal requirement for it to be protected):
 - Things looked after on behalf of others
 - Personal or financial records
 - Credit card payments
 - Medical records etc
- **Company Secrets** (the 'Crown Jewels' of a Company):
 - High Value IP
 - Business Plans
 - Financial projections
 - Designs
 - Legal material etc.

- There tends to be a focus on protecting Custodial Data
 - Custodial data attracts legislation
 - PCI-DSS
 - Threat of significant fines from ICO – up to **£500,000**
- However...
 - Loss of Company Secrets is **4 x more likely** to happen
 - **10 x more costly** than the loss of Custodial data
 - Malicious theft of information is 10 x more costly than accidental loss

FORRESTER Making Leaders Successful Every Day

FORRESTER

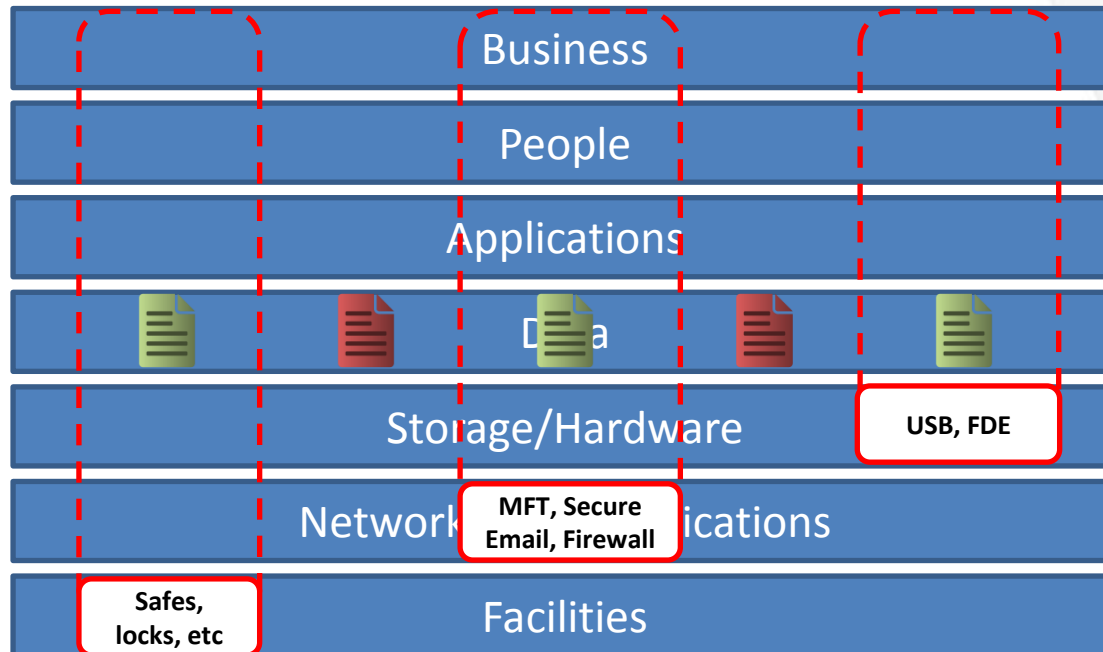
Compliant does not mean secure

- **Increasing Regulatory and Compliance Pressure**
 - E.g. Data Protection Act came into force on last year.
 - Up to £500,000 fine
 - Enforcement notices and prosecutions
 - Customer Pressure.
- **Compliant Doesn't Mean Secure**
 - Company secrets often not covered
 - The average data breach cost £1.9 million in 2010
 - Symantec and Ponemon Institute.
- **Secure Doesn't Mean Efficient**
 - Cost to business efficiency of implementing security plans
 - But efficient shouldn't mean complacent
 - The holy grail is: security measures enhance business performance
 - ...or at the very least are transparent to users

Data-Centric Security

Traditional Approaches

- Focus on securing storage, transport or facilities
- Try to map boundaries up to data and people



Traditional Approaches

- Solutions lead by technology areas
- All very important, but hard to integrate and coordinate



Whole device encrypted. Prevents loss if device lost or stolen. Files unprotected when they leave the device.

Perimeter Security & Device Control

Prevents unauthorised access to systems. Has no cognisance of individual files and what happens to them.

Device Encryption

Individual files are secured for storage and movement. File is decrypted to be used. No granularity of access or control.

File Encryption

Managed File Transfer

Secure file sharing requires the correct level of access for the recipient and authentication of the recipient.

Policy Enforcement

Manages not only who can access data, but what can be done with that data.

File encrypted and transferred to recipient. Allows transfer of larger files as well as smaller. File is unprotected both before and after transfer.

Rights Management

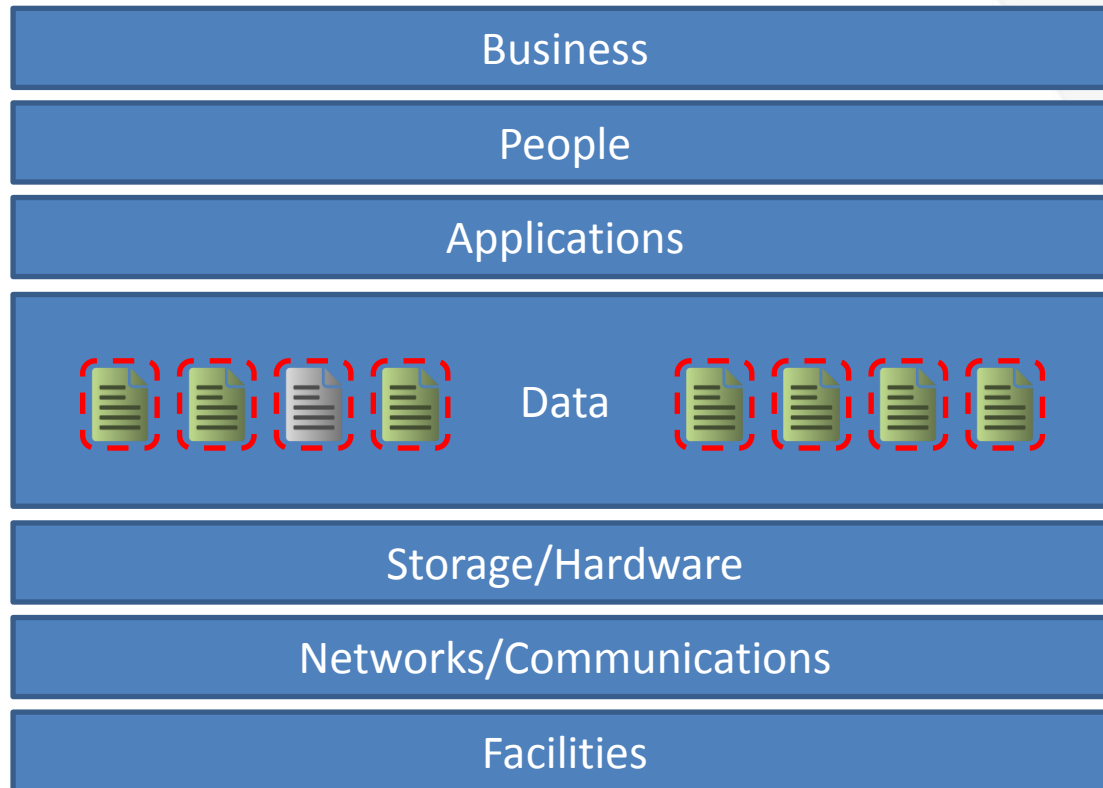
Secure records that record each access detail, safe from any interference are core features of any auditing tool.

Auditing

Data Centric Security – a powerful philosophy

Traditionally IT security focuses on securing storage, transmission, end points & perimeters.

Data Centric Security focuses on the data itself, wherever it is & however it is used.



Data Centric Security – summary

- **Old-style security secures laptops, email, servers, USB keys, etc.**
 - Fine when a file is on it, or on it's way
 - You lose control of data once it reaches intended recipients
 - Hard and costly to implement, integrate and use coherently within a business.



- **Secure the data itself, wherever it is & however it is used.**
 - Security moves with the file
 - Safely and confidently share data with 3rd parties, partners, customers, etc
 - Protect sensitive information from theft and negligent disclosure
 - Plus: reduce cost and increase speed of information delivery.



Implementing Data-Centric Security

Approaches

- **Number of approaches, e.g.**

- Encrypted zips
- MS ERM
- Adobe Lifecycle
- Credant
- Boole Server



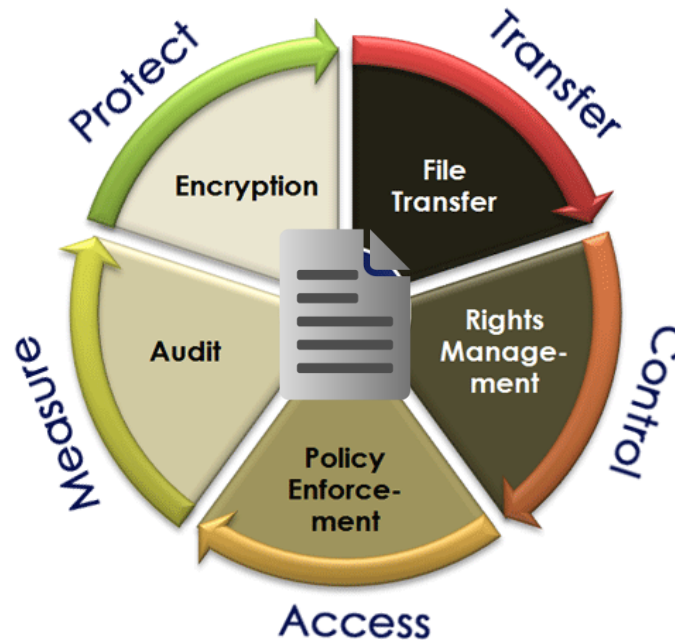
- **Focus on files and some on text as well**
- **Use internet to connect files and authentication**
- **No silver bullet**
- **Build protection**
 - Protect data
 - Authenticate
 - Apply rights
 - Manage distribution
 - Store
 - Collaboration

Data Centric Security – opportunities

Some interesting opportunities arise once you adopt an always-secure data-centric approach...

Protect data from unauthorised access, wherever it resides (fixed infrastructure, end points & mobile devices).

Audit every single activity undertaken on secured data and prove regulatory controls are in place.



Securely deliver and share sensitive information beyond your network.

Control and change access to information in real time even after it has been sent out. Restrict functions on secured documents, e.g. print, copy, save as, print screen.

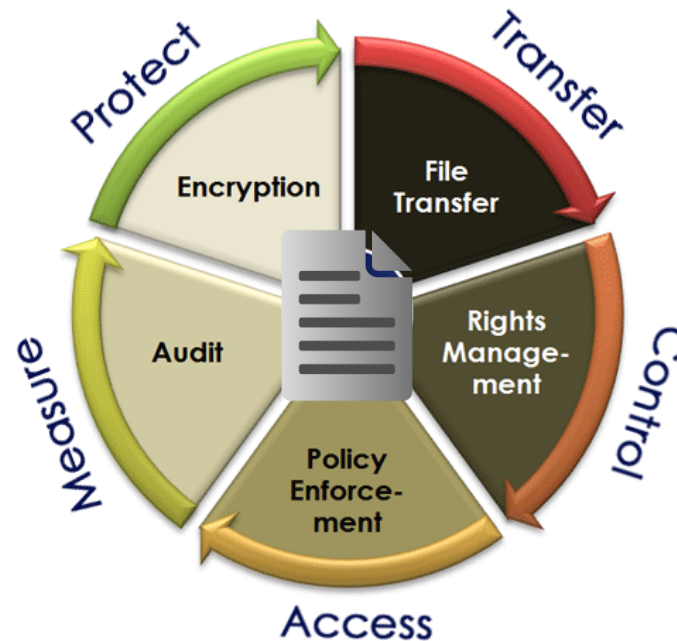
Revoke access instantly, even after delivery has been taken, no matter where it has ended up.

Data Centric Security – and compliance

Compliance frameworks, e.g. ISO 27001, revolve around risk assessment, controls, review and evidence of regimes. The facilities offered by a data-centric security solution can be mapped across to many compliance frameworks.

Protect requirements for strong encryption of sensitive data, and protection of data at rest.

Audit requirements for tracking documents across their life, requirements for monitoring the actions of users.



Securely requirements for protection of data in transit.

Control requirements for controlling who can do what to sensitive information.

Revoke requirements relating to the management of incidents, and personnel.

Combining Sharing and Security

Security & Sharing Platform

providing secure store,
transfer, collaboration &
rights management



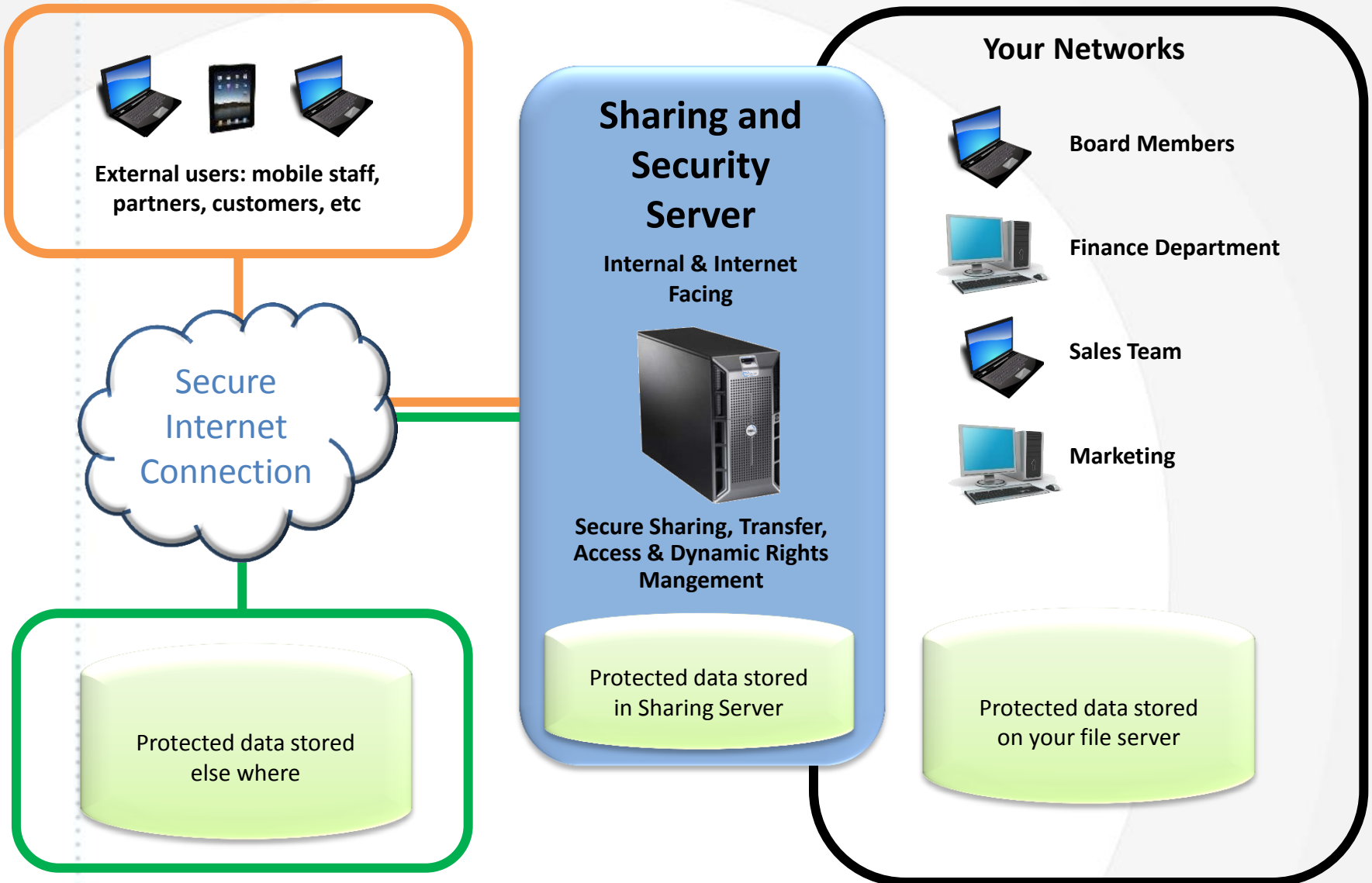
External Users

suppliers, customers, mobile
workers etc on
clients &/or agents.

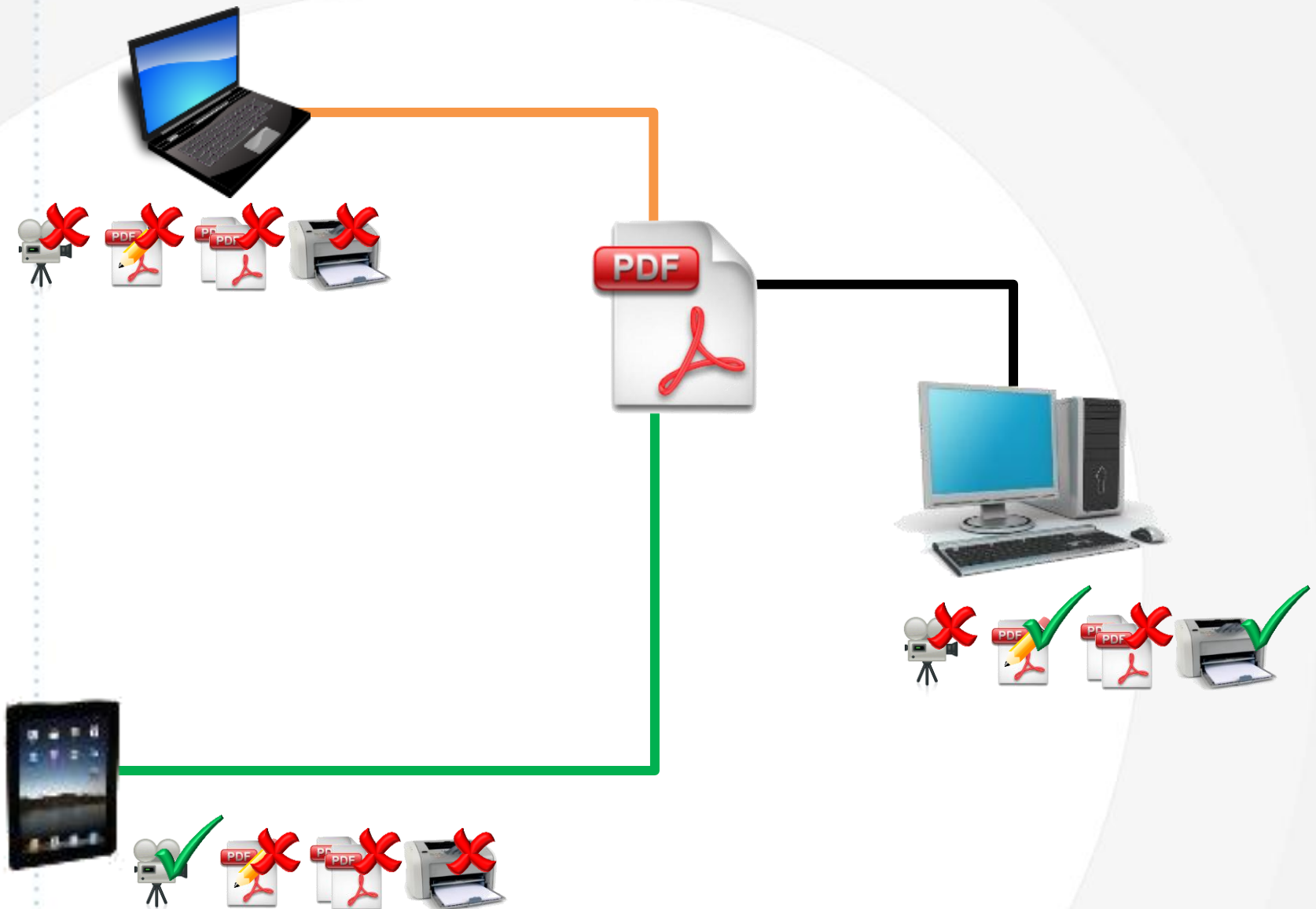
Internal Users

internal staff on
company network on
clients &/or agents.

Extending Protection, inviting collaboration

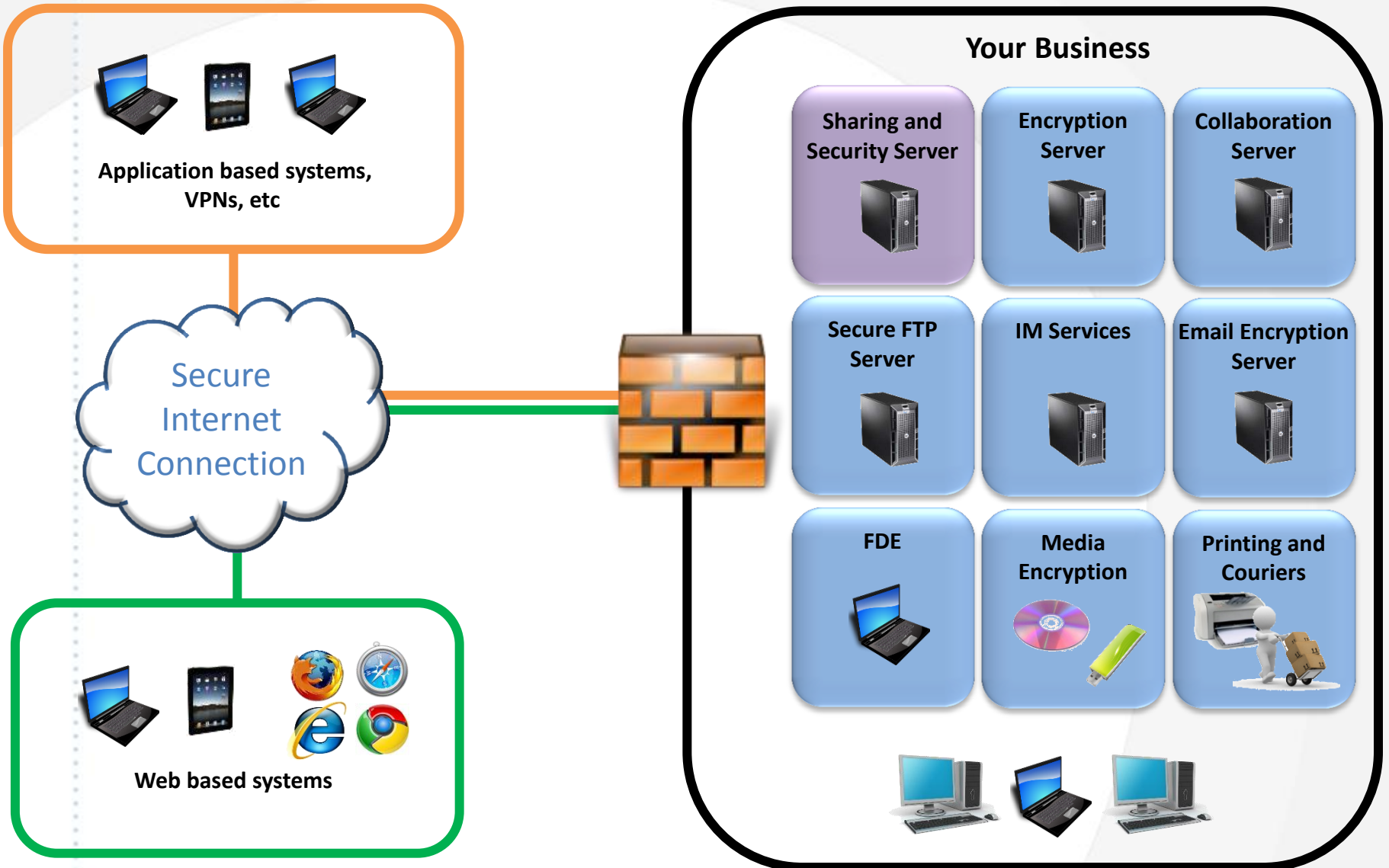


Different Users Different Rights

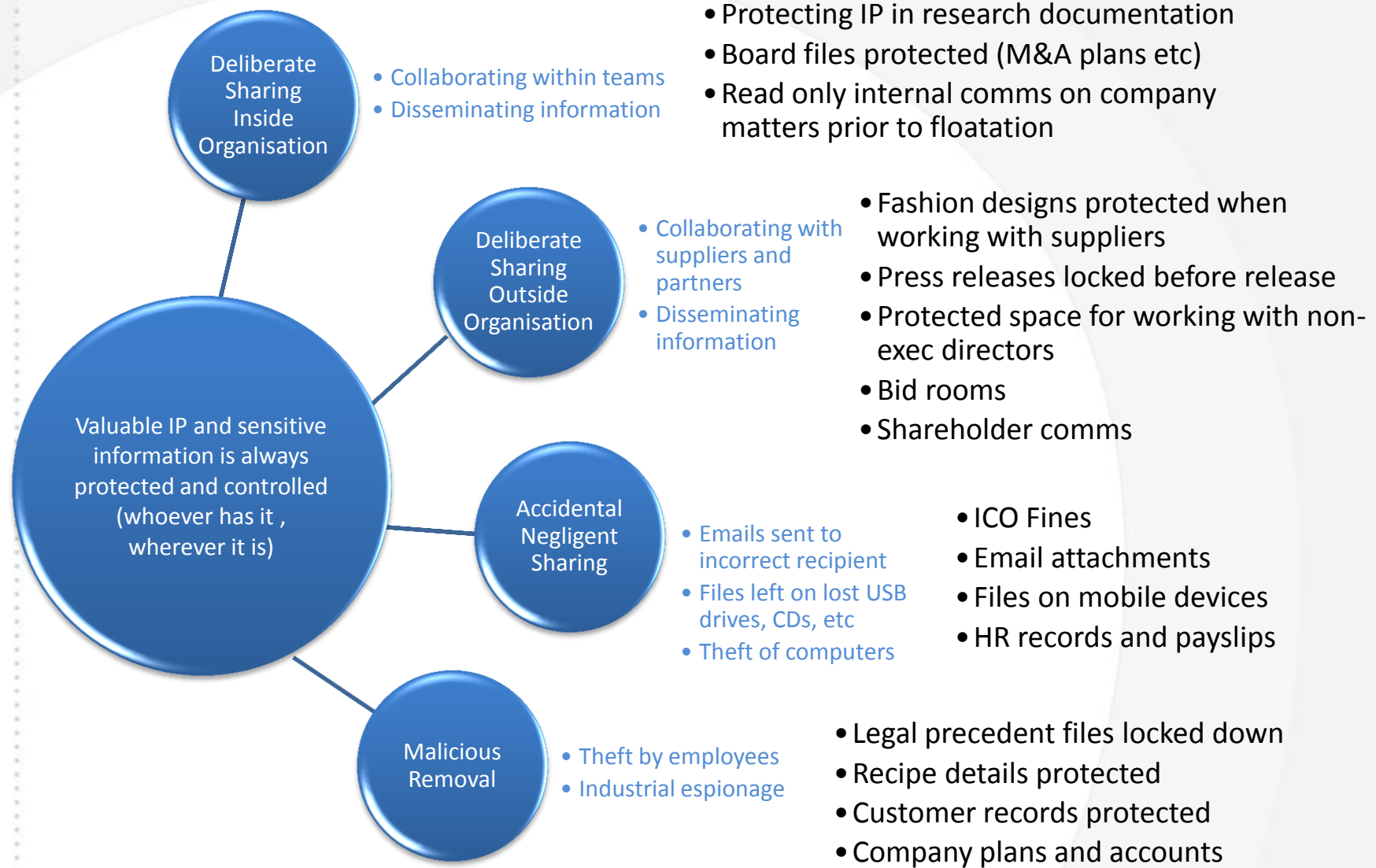


28-Sep-11

Complementing and Replacing



Free data up to contribute to the bottom line... ... and protect your valuable assets



Summary and Conclusion

- Compliance is a major spend within the security budget...
 - ... but does not necessarily equal secured data
- Don't forget critical secrets that confer long-term competitive advantage
- Consider the business requirements that lead to information risks
- Take a strategic view that means the business is more efficient using secure systems
- Select approach and systems that share this world view
- Consider data-centric security technologies that provide a unified platform to protect all types of data
- They should specifically:
 - accommodate unstructured information
 - provide the correct level of access to necessary parties
 - place emphasis on retaining control of information at all times
 - including throughout any collaboration processes or sharing
 - Secure data with persistently applied measures wherever it is used, sent or stored.

The Future

- True role based authentication
 - Further emphasis on device independence
 - Greater use of web apps
 - Persistent single personal identification
 - Cloud...
 - DLP...
 - Increasing emphasis on compliance
 - Increasingly savvy customers
 - The Xbox generation hit the workplace...

