

Data Protection 101

Successes, Fails, and Fixes

Who am I?

- Peter Teoh @pteoh PTzero
- Jack of all trades (master of none?)
- Experience with DLP

What is Data Protection?

- Data Protection is also known as Data Loss Prevention (DLP). It is the discipline of protecting your organization's confidential data assets from being disclosed to unauthorized parties.
- Protect data
 - At Rest
 - In Motion
 - In Use

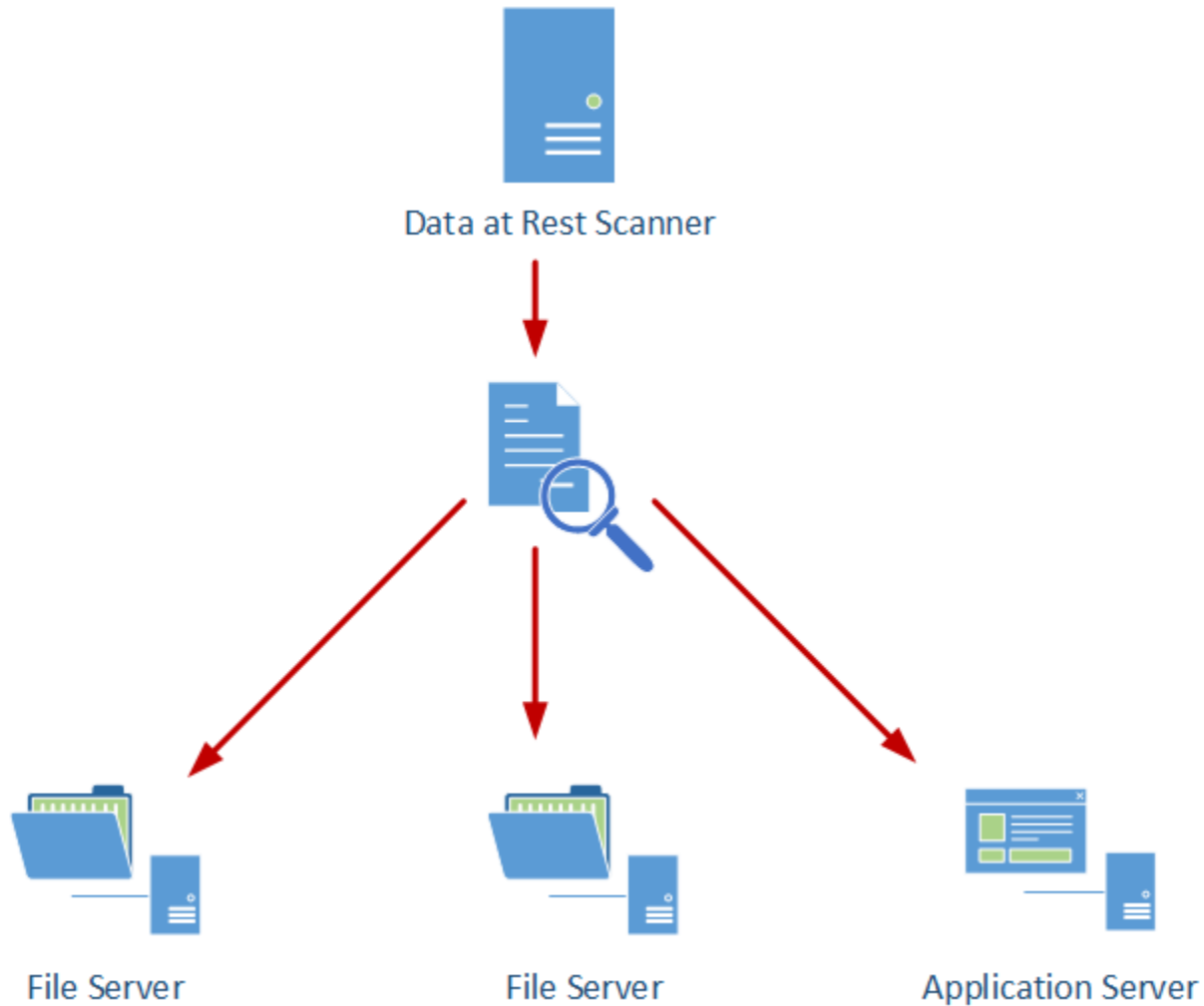
Data Protection Recipe for Success

- Know your data!
 - Know what type(s) of data you're protecting.
 - Know where your data should and shouldn't reside.
 - Know who should have access to data.
 - Know what constitutes acceptable use.
- Policies are your friends.
 - Define policies around proper handling of data.
 - Do your policies comply with legal and regulatory requirements?
- Don't forget training!

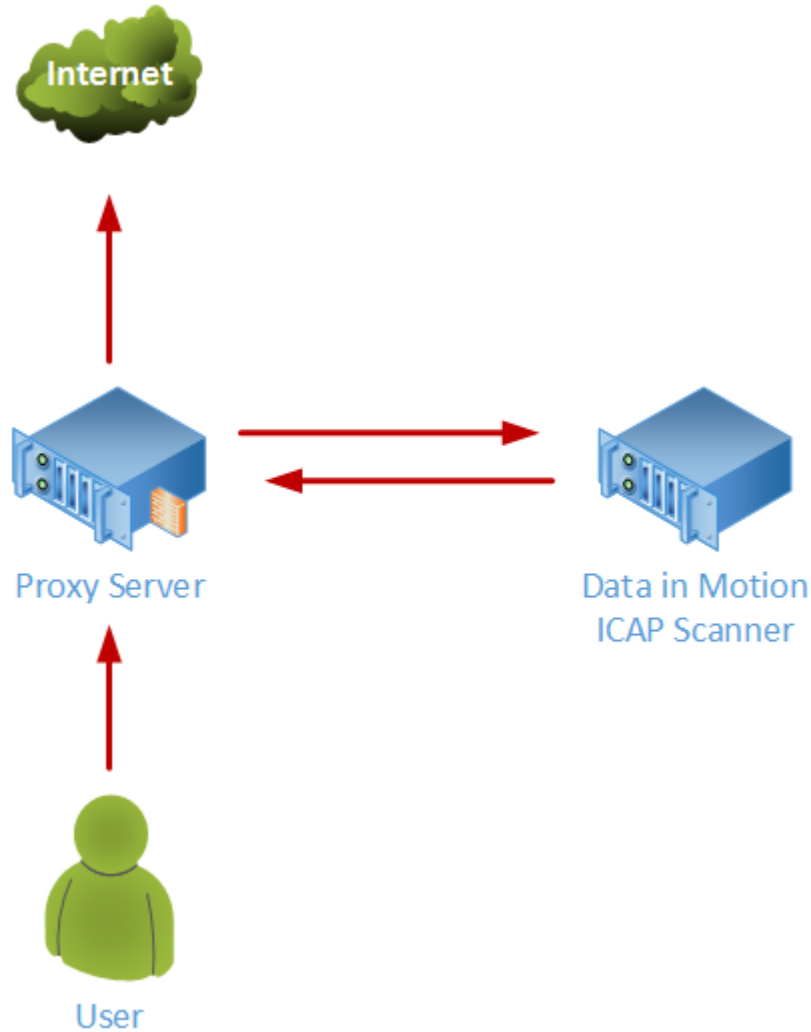
Data Protection Recipe for Success

- Plan your incident response.
 - What happens when you detect data leakage?
 - Set reasonable and appropriate thresholds.
- Configure scanners for:
 - Data at Rest
 - Data in Motion
 - Data in Use

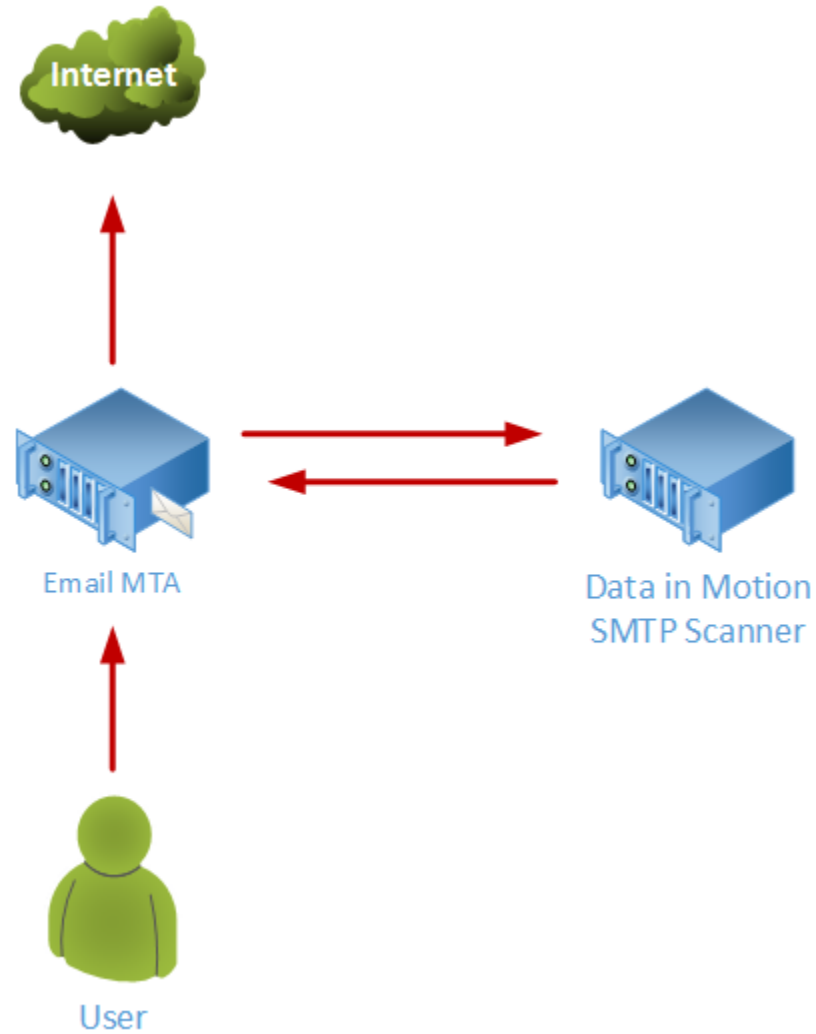
Data at Rest



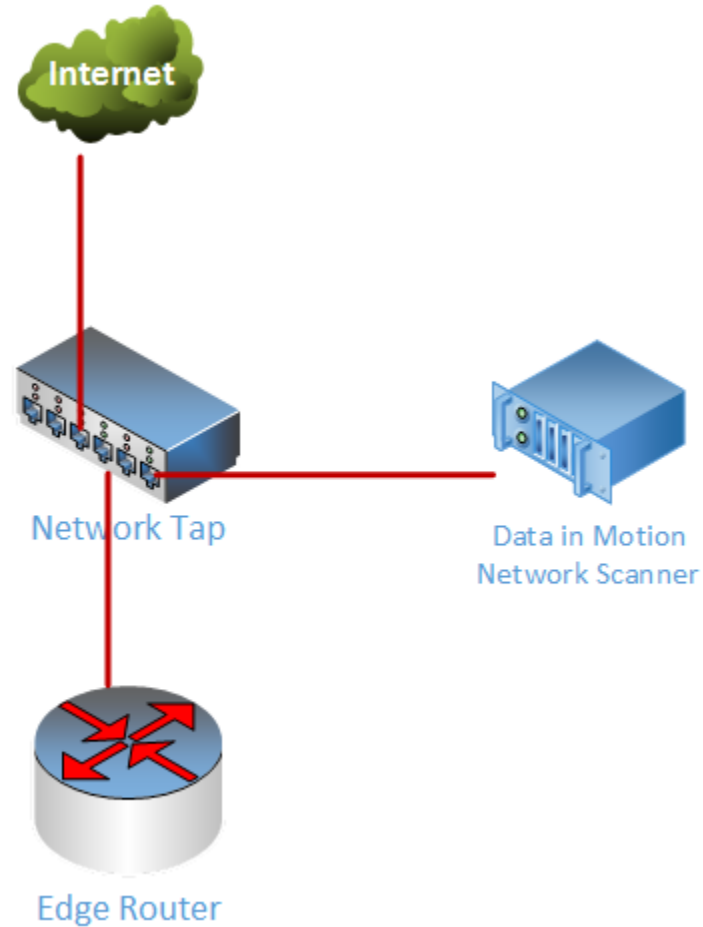
Data in Motion (Web)



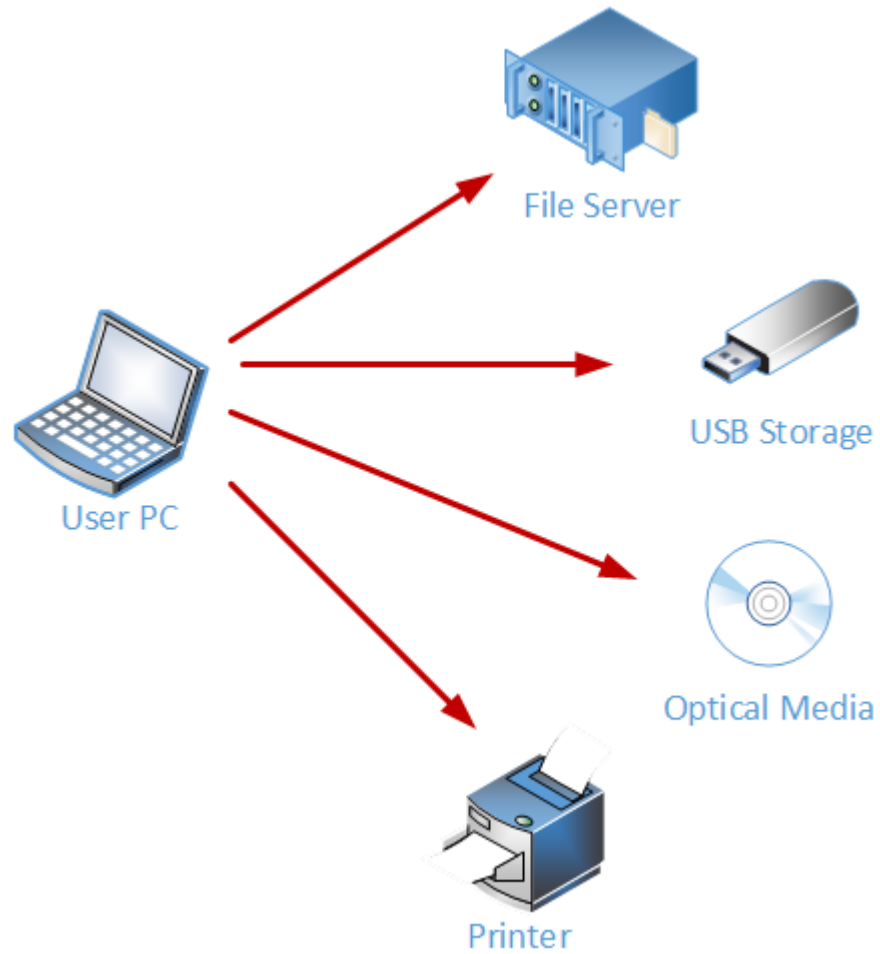
Data in Motion (Email)



Data in Motion (Network Tap)



Data in Use



Data Protection Technologies

- Pattern matching
 - Basic method to recognize account numbers, etc.
 - Standard watermark for confidential documents
 - Pros and Cons
- Exact data matching
 - Index your known confidential data, both structured and unstructured
 - Match on combinations of fields
 - Pros and Cons

Data Protection Fails

- Pattern matching produces false positives
- Encrypted data
- Split data into fragments, e.g.:
 - Breaking 9-digit SSNs into separate files
 - Breaking down documents into small chunks
- Low-and-slow leakage
- Screen captures

111-22-3333
212-88-5555
375-12-3456
182-99-8989
288-22-8888
399-33-6666

Splitting up a list of SSNs into separate files will defeat exact data match

111-22
212-88
375-12
182-99
288-22
399-33

3333
5555
3456
8989
8888
6666

Data Protection Fixes

- Defeating encryption
 - SSL Intercept
 - Block or log encrypted files
- Combine pattern match and exact data match technologies
 - Set rules with thresholds
- Log all detected events

Data Protection Fixes

- Use Big Data techniques to aggregate events
 - Correlate low-and-slow leakage
 - Risk ranking based on user profile and access levels
 - Track data usage for anomalies (volume)
- Apply enhanced user/workstation monitoring to high-risk individuals
- Look at doing OCR on image files
- Employ data masking

Conclusion

- Policies and organizational commitment needed.
- There is no one size fits all solution.
- Balance aggressiveness of controls versus permitting business to run.
- You may not be able to eliminate data leakage but you can mitigate the risk.
- Think beyond traditional Data Protection techniques.

Q&A

Check out

- Queercon
 - Networking events and PARTIES!!!
- Crypto and Privacy Village
 - New for DEF CON 22

Peter Teoh

Twitter: @pteoh
google.com/+PeterTeoh
DEF CON Forum: PTzero