

A decorative graphic consisting of multiple parallel, wavy lines in various colors (purple, blue, orange, grey, green) that flow from the left side of the slide towards the right, creating a sense of movement and connectivity.

# Securing File Data in a Distributed or Mobile World

Chris Winter  
SafeNet Inc.

# SNIA Legal Notice



- ❑ The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- ❑ Member companies and individual members may use this material in presentations and literature under the following conditions:
  - ❑ Any slide or slides used must be reproduced in their entirety without modification
  - ❑ The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- ❑ This presentation is a project of the SNIA Education Committee.
- ❑ Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- ❑ The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

**NO WARRANTIES, EXPRESS OR *IMPLIED*. USE AT YOUR OWN RISK.**

# Agenda

- ❑ Why data security is needed
- ❑ What data needs to be secured
- ❑ Where file data resides
- ❑ What threats exist against file data
- ❑ Distributed file data
- ❑ Mobile file data
  
- ❑ Conclusion

# Why data security is needed

- ❑ Perimeter defenses are ineffective today according to security professionals

- ❑ 31% acknowledged they have been breached

- ❑ Only 10% of security industry is

- ❑
    - ❑

- ❑ 59% said that if a breach occurred, high value data would not be safe

- ❑ 66% believe they will suffer a breach within the next 3 years

## Quick Show of Hands:

How many of you have experienced a data breach in your organizations?

# Why data security is needed

---

- ❑ 95% continue to invest in and employ the same data security strategies (Network perimeter security)
- ❑ 35% state they know their security investments are being deployed to the wrong technologies
- ❑ 20% would not trust their own personal data to their own networks

## So what does all this mean?

- ❑ We need to accept that breaches WILL happen and once they do, the only protection is to secure the data itself
- ❑ **The new perimeter is the data itself – we must Secure the Breach**

# Dover Castle ca. 1216 – never breached



All the really important stuff was in the keep

Multiple perimeters

# What data needs to be secured

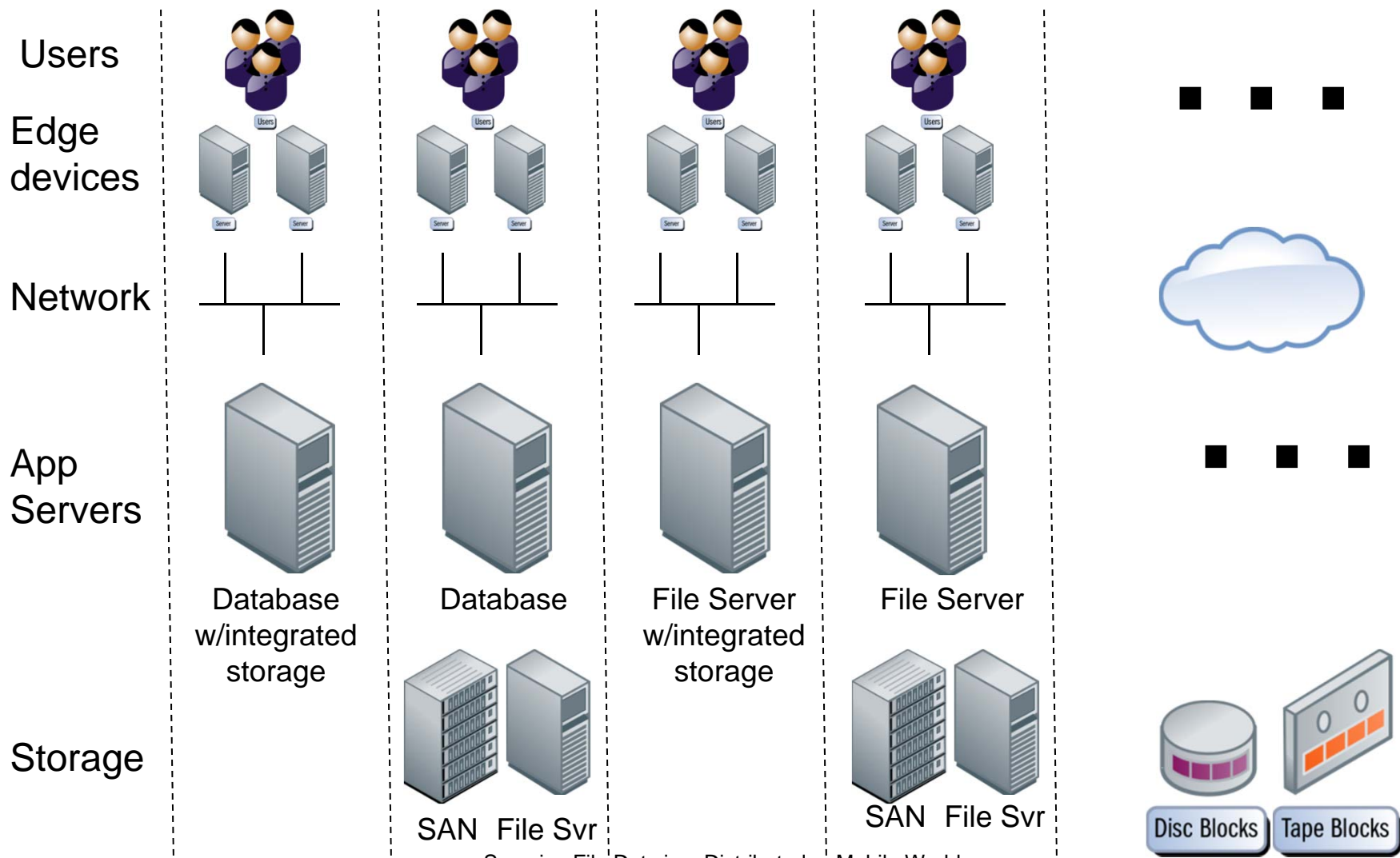
- ❑ Typically there are four categories of file data that need to be secured:
  - ❑ Classified Information
    - ❑ Governmental, Military, Intelligence - strict hierarchical schemes, etc.
  - ❑ Regulatory Compliance
    - ❑ Current: HIPAA, PCI, PII, etc. – binary – no shades of gray
    - ❑ Future ?: GDPR (General Data Protection Regulation), Right to be Forgotten
  - ❑ Confidential information
    - ❑ Intellectual property
    - ❑ Proprietary information
    - ❑ Competitive data, etc.
  - ❑ Anything else for any other reason
    - ❑ Whenever there is a need, whatever it is, good or bad!

# Does it ALL have to be secured

- ❑ It depends on a number of factors:
  - ❑ Identification
    - ❑ Do you know where ALL your critical data may reside
  - ❑ Relevance
    - ❑ Is it possible to segregate relevant from irrelevant
    - ❑ Can you be sure you can identify ALL the relevant data
  - ❑ Quantity of data
    - ❑ Column level encryption
    - ❑ Tokenization / Obfuscation
    - ❑ Deduplication, Compression before securing
  - ❑ Impact of revelation, loss, or misuse
    - ❑ Can you afford the immediate cost
      - ❑ Monetary penalties, business restrictions
    - ❑ Can you afford the longer term cost of loss of reputation



# Where file data resides in the datacenter



# Where file data resides

- ❑ In main datacenter(s)
  - ❑ Application server
  - ❑ NAS/File server
  - ❑ User
  - ❑ Backup
  - ❑ Archive
  - ❑ Virtual
    - ❑ Clone
- ❑ Managed from multiple data centers
  - ❑ Cloud (Public, Private, Hybrid)

**Quick Show of Hands:**

How many of you know the location of EVERY clone or snapshot of your VMs?

# Where file data resides

- ❑ Distributed locations, remote offices
  - ❑ App server
  - ❑ NAS server
  - ❑ User desktop

} Computer-local file system or  
remote file system in main  
datacenter over VPN
- ❑ Backup device – local/remote tape or disk, external drives
- ❑ Virtual Machines – when not running
  - ❑ Clones, snapshots

# Where file data resides

- ❑ Mobile – two types
  - ❑ User mobile device – local file system
    - ❑ Support for local apps may not be possible
    - ❑ USB drive, external
  - ❑ Enterprise
    - ❑ Secure
    - ❑ Encrypted
- ❑ Mobile devices are often used down
- ❑ Mobile devices are often used down
- ❑ Mobile devices are often used down
- ❑ Home backups, cloud backups, USB sticks, smartphones
- ❑ With BYOD, this problem goes exponential!



## Quick Show of Hands:

How many of you  
make backups of your  
company data at home  
or on USB?

# What threats exist against file data

---

- ❑ Assuming all file data that is critical is encrypted:
- ❑ Distributing to remote locations can expose centralized keys
- ❑ Distributing to mobile devices can expose data as well as keys
- ❑ Database reports and extracts
  - ❑ Written to desktops, mobile devices, removable storage, etc.
  - ❑ Data leakage when further distributed via email, etc.
- ❑ Data exposure to unauthenticated people
- ❑ System administrators posing as authenticated users
  - ❑ **80%+ of all actual breaches are internal**

# Distributed File Data – remote access

- ❑ File data in a central datacenter can be accessed remotely with a high level of security and auditability
  - ❑ VPNs, Two Factor Authentication, etc.
- ❑ Centralized access results in good access control, policy enforcement, auditing and reporting
  - ❑ Alerting essential for real time response and prevention
  - ❑ Auditing and reporting essential for post mortem investigations and compliance evaluation
- ❑ End points can be authenticated in real-time
  - ❑ Varying levels of authentication depending on user, platform, location, information accessed ,etc

# Distributed File Data - inbound

---

- ❑ Moving or copying file data from remote sites to datacenters can be managed with careful planning
  - ❑ Daily replication/copy to HQ over secure tunnels
  - ❑ Backups to HQ over secure tunnels
- ❑ File data can be re-encrypted as it arrives
  - ❑ Depending on policy, etc.
  - ❑ Key versioning and tracking necessary

# Distributed File Data - outbound

- ❑ Moving or copying file data from a datacenter to a distributed or remote location is problematic
  - ❑ Cannot use same encryption key as primary file data
    - ❑ File data usually encrypted on a per-share or per-folder basis rather than per-file
    - ❑ Means file must be duplicated and encrypted with a different key before sending
    - ❑ Means the key management system must track multiple keys per file (like versioning) to support secure destruction
  - ❑ Once file data is remote, access and auditability is a problem
    - ❑ Key exchange with remote location exposes key
    - ❑ Offline access to file bypasses real-time authentication
  - ❑ Detecting file data changes when file is returned to datacenter
    - ❑ Results in multiple copies of file data
      - ❑ With multiple keys



# Mobile File Data – even more problematic

- ❑ Moving or copying file data from a datacenter to a mobile device is even more problematic:
  - ❑ Loss of mobile device
    - ❑ Can be mitigated with FDE (Self Encrypting Drives)
  - ❑ No control over who, when or where data is accessed
    - ❑ Only if online authentication is mandatory (not possible in many situations)
  - ❑ Pre-upload is normally required
    - ❑ Copy files onto device before leaving for business trip
    - ❑ Means keys must also be pre-loaded
  - ❑ Duplication of file data to same or alternate mobile devices
    - ❑ Including keys
  - ❑ Saving of cleartext file data to removable devices

# Conclusions

- ❑ We need to accept that network perimeter breaches WILL happen – the new perimeter is the data itself
- ❑ Different file data categories need different protection schemes
- ❑ An insider is your biggest threat for large data breaches (but you must also protect against intrusion)
- ❑ Mobile devices pose the biggest management challenges
- ❑ A centralized reporting and auditing capability is important
- ❑ A centralized alerting capability is essential
- ❑ File encryption alone cannot succeed without fully integrated authentication, access control, and Enterprise Key Management
- ❑ **We must Secure the Breach**

# Attribution & Feedback

The SNIA Education Committee thanks the following individuals for their contributions to this Tutorial.

## Authorship History

Name/Date of Original Author here:  
Chris Winter - Feb 15<sup>th</sup>, 2013

### Updates:

Chris Winter – Feb 18<sup>th</sup>, 2013

Chris Winter – Feb 24<sup>th</sup>, 2013

Chris Winter – Mar 9<sup>th</sup>, 2013

Chris Winter – Mar 17<sup>th</sup>, 2013 

Chris Winter – May 29<sup>th</sup>, 2013

## Additional Contributors

Trish Reilly  
Gianna DaGiau

*Please send any questions or comments regarding this SNIA Tutorial to [tracktutorials@snia.org](mailto:tracktutorials@snia.org)*