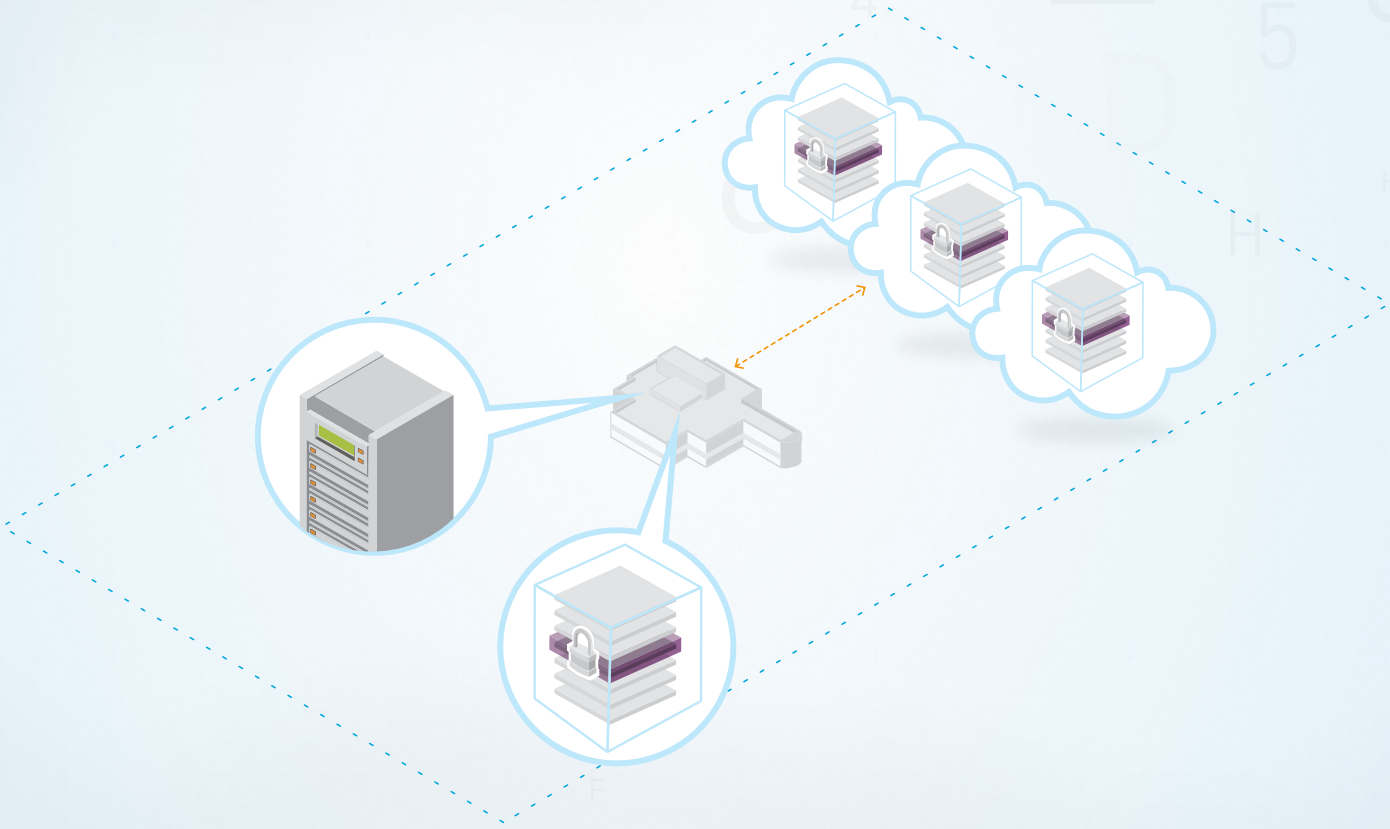


Data Center Encryption Survey

Executive Summary

Securing the Path to Consolidation in Today's Data Center

SafeNet®

THE DATA PROTECTION COMPANY

Overview

Many want to make data center consolidation happen, but few have actually done so. While cloud offerings and virtualization have opened up a path for realizing the benefits of consolidation, many organizations are encountering significant hurdles in this journey. A SafeNet survey of more than 580 IT and security professionals explored these trends.

In a global market that is increasingly fluid and competitive, organizations have to continue to ensure that they're getting the most value from their IT investments.

Consequently, IT and business executives continue to pursue data center consolidation by reducing the number of physical data center sites, expanding the use of virtualization, and adopting cloud initiatives. How's it going? The SafeNet survey revealed several important takeaways:

- **Encryption and key management will unlock the potential of consolidation and cloud.** Data center consolidation was a high priority for many respondents, but the survey also indicated that there is a significant gap between attaining that objective and current realities. The survey results highlight the fact that security efforts, like employing encryption and managing cryptographic keys more securely and effectively, are a critical prerequisite to data center consolidation and cloud migration. Challenges in addressing these security requirements may be a contributing factor to the slower progress in consolidation efforts, including moving workloads from physical machines to virtualized systems.
- **Why we're not there yet.** In spite of the fact that 73% of survey participants recognized that management efficiency and cost saving were key advantages of data center consolidation and virtualization, they are still delaying decisions on consolidation projects—citing technical difficulties at an astounding 53%. Further, while a different study found that two-thirds of workloads running on x86 servers are now virtualized[1], only one-fifth of respondents indicated they are currently doing any encryption in their virtual environments.
- **Those who can combine cloud with security and compliance will win.** Success in the cloud requires a focus on security, including addressing baseline security controls, such as identity and access management (IAM) and anti-virus, as well as controls like encryption and key management. Those enterprises that can address these requirements will be able to realize the competitive advantages of more fully leveraging consolidation, virtualization, and the cloud. For the service providers that can assist enterprises in these efforts, huge market opportunities await.

1 ServerWatch, "Taking Stock of the State of the Server Virtualization Market", Paul Rubens, August 5, 2013, http://www.serverwatch.com/server-trends/the-state-of-the-server-virtualization-market.html

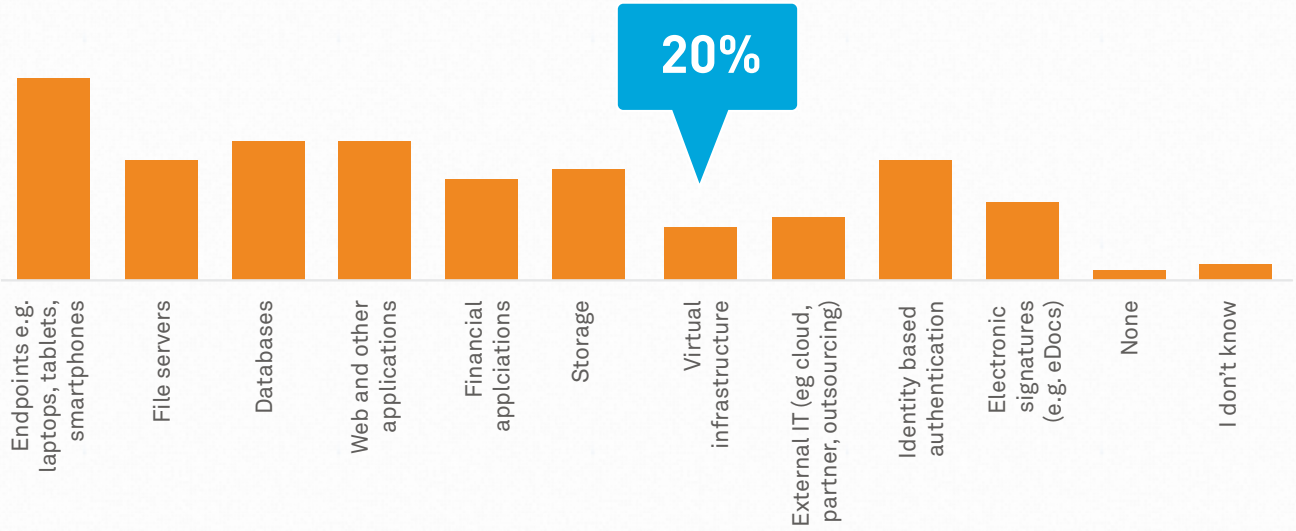
The survey results highlight the fact that security efforts, like employing encryption and managing cryptographic keys more securely and effectively, are a critical prerequisite to data center consolidation and cloud migration.

Key Statistics

What's Virtualized Isn't Being Encrypted

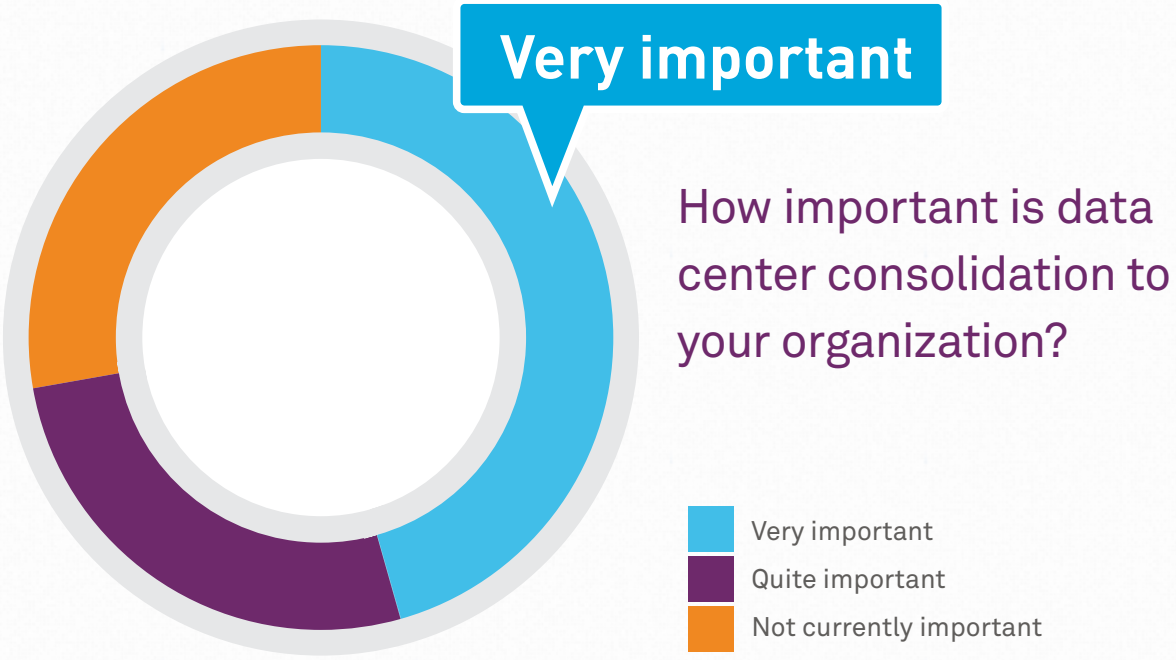
In spite of the massive utilization of virtualization technologies today, only one-fifth of respondents are currently encrypting data in virtualized environments.

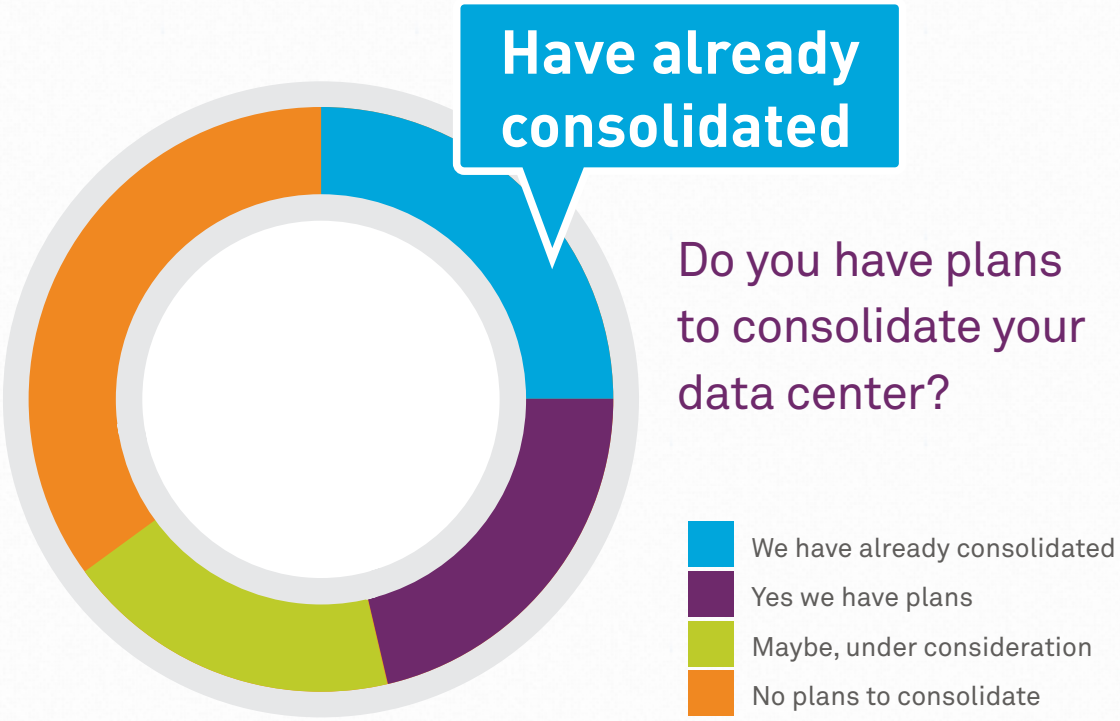
73% recognized that management efficiency and cost saving were key advantages of data center consolidation and virtualization



Consolidation: A Goal Out of Reach?

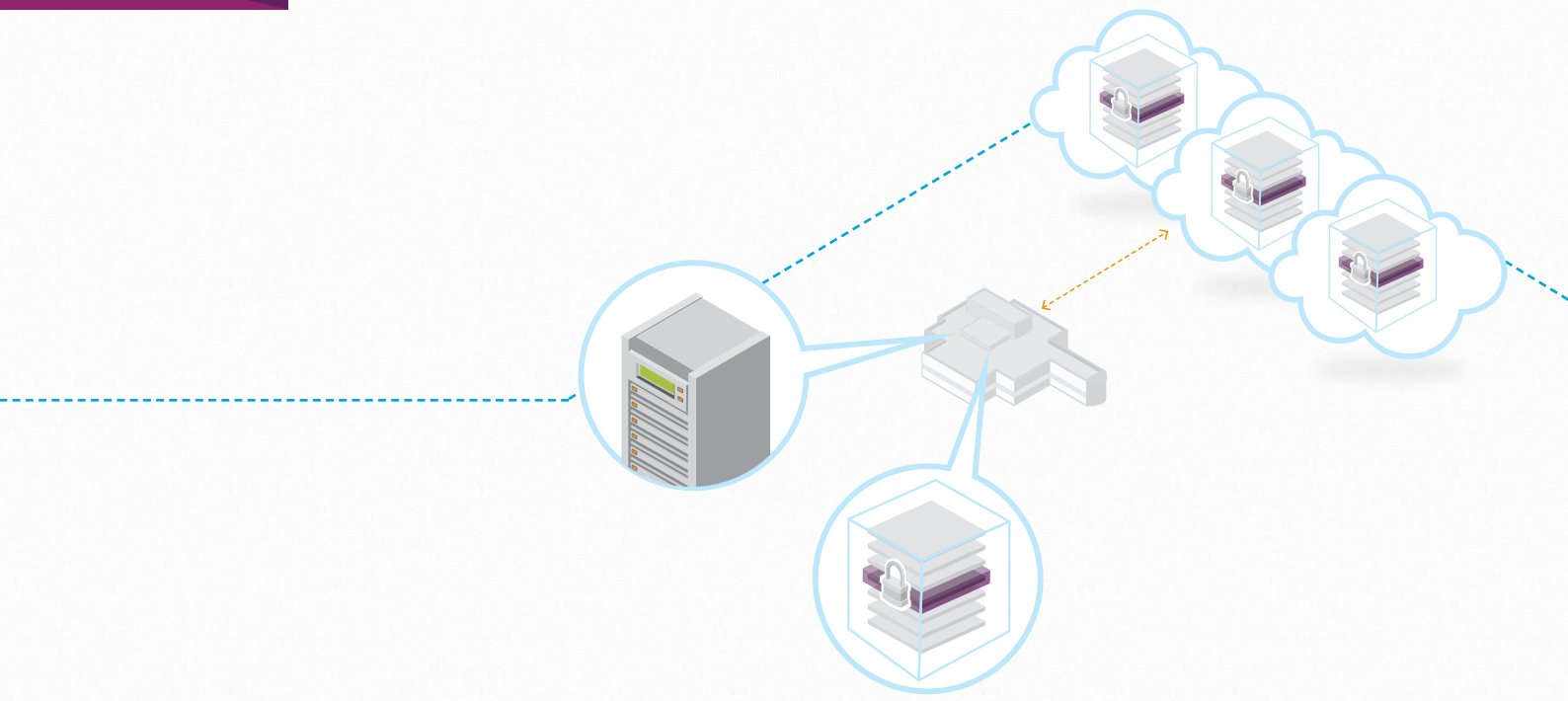
About three-quarters of respondents said data center consolidation is either very or quite important, but less than one-quarter have actually done anything about it.





Why we're not there yet

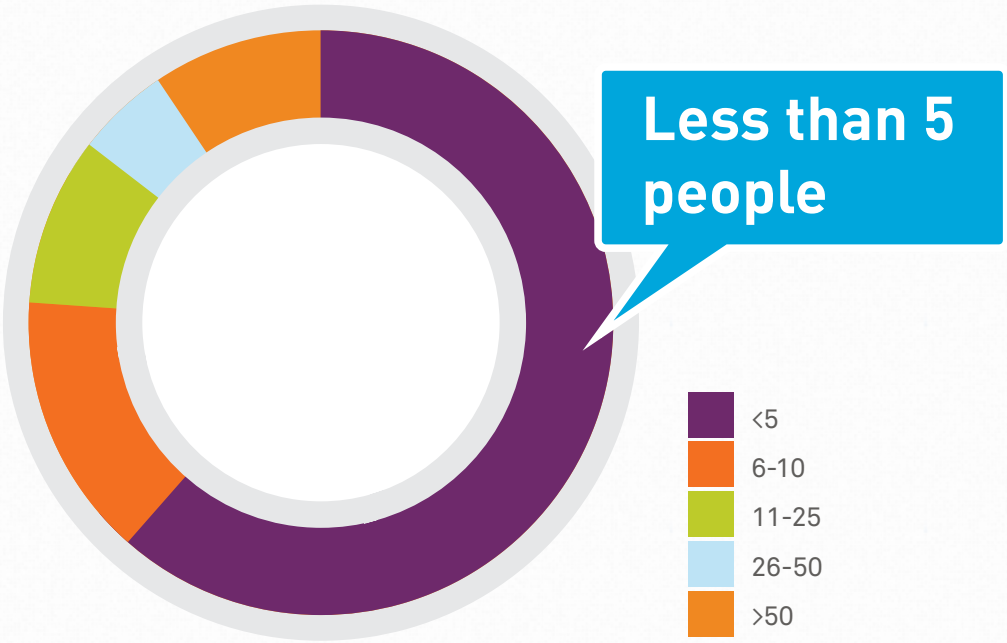
53% cite technical difficulties as the cause of delay in decisions on consolidation projects



So Much, Managed by So Few

The survey revealed that encryption teams have to support many forms of encryption, many encrypted applications, and many encryption tools. However, the survey also showed one thing there isn't a lot of: staff members. Well over half, 58.2%, indicated that globally they have less than five people involved with encryption management.

How many people are involved in the management of your encryption globally?

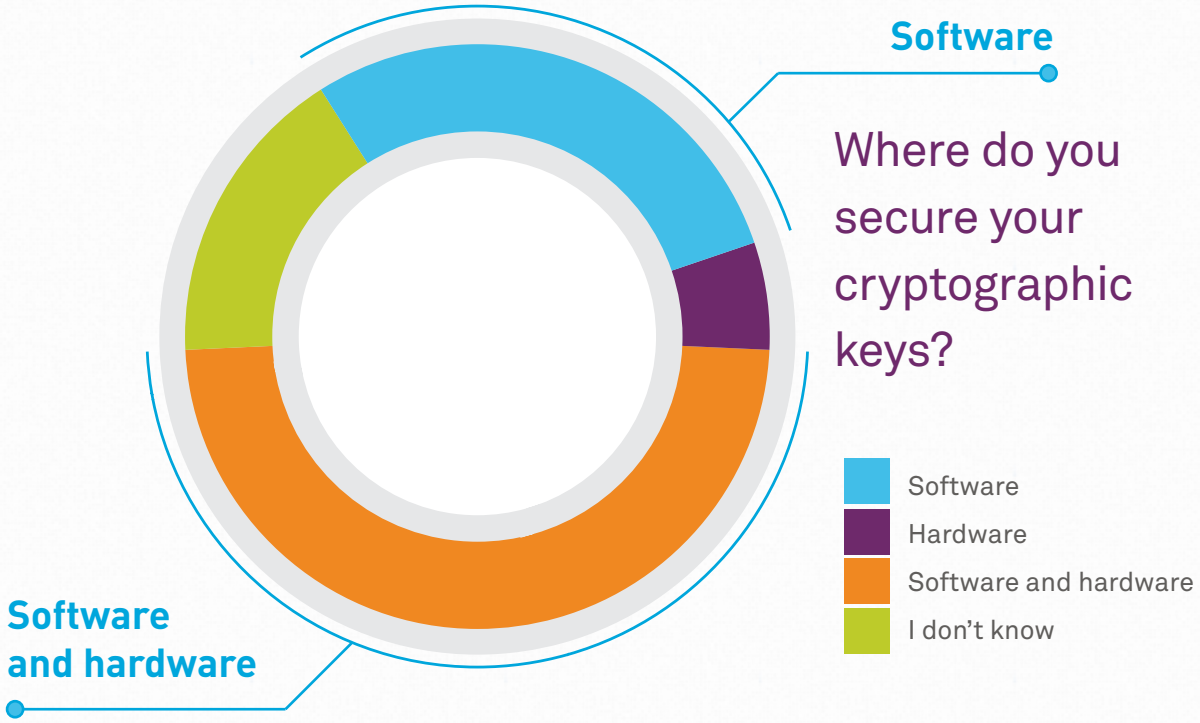


The survey revealed that encryption teams have to support many forms of encryption. More than half of respondents are using between one and three different encryption tools.

Keys Being Left Under the Door Mat

Encrypted data is only as secure and available as the keys used to encrypt it. For instance, when keys are stored in servers, they are susceptible to compromise and loss, which exposes sensitive encrypted data to those same risks. To address these gaps, organizations will increasingly need to leverage purpose-built key management platforms that offer robust security and availability. These purpose-built platforms allow users to store and manage keys in hardware, where they are more protected and controlled.

However, currently around three-quarters of respondents store at least some encryption keys in software—the IT equivalent of leaving house keys under the front door mat.



The Must-have When Sourcing Solutions: Compliance and Security

When sourcing business applications, 74% of respondents are looking for solutions that support compliance and security. One clear reason: Of that group, 59% are currently struggling with auditing their current data center estates.

What do you look for when sourcing new business applications?

Conclusion

With multi-layer encryption and centralized key management, organizations can accelerate their cloud, virtualization, and data center consolidation initiatives, while retaining the controls they need to protect sensitive data, adhere to internal security policies, and comply with regulatory and government mandates. The service providers and cloud vendors that can deliver solutions that further these objectives will be able to capitalize on significant market opportunities.

About the Survey

This white paper draws from a survey that SafeNet conducted in Fall 2013. The survey polled more than 580 individuals. Respondents were comprised of security and IT executives from a range of industries, including financial services, healthcare, technology, media, consumer packaged goods, retail, and more. Survey respondents had a truly global makeup, with more than 50 countries represented.

About SafeNet

Founded in 1983, SafeNet, Inc. is one of the largest information security companies in the world, and is trusted to protect the most sensitive data for market-leading organizations around the globe. SafeNet's data-centric approach focuses on the protection of high value information throughout its lifecycle, from the data center to the cloud. More than 25,000 customers across commercial enterprises and government agencies trust SafeNet to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments.