Enterprises Are Breaking Down Obstacles to Cloud and Compliance

Executive Summary
Introduction

For security professionals, the numbers don't lie. According to the Breach Level Index (breachlevelindex.com), in 2013, about 68,000 records were lost or stolen every hour. That equates to 595 million records for the year—and that’s only counting the 56% of reported breaches that actually disclosed numbers.

Given these statistics, there is growing recognition that breaches are inevitable, which is why encryption is increasingly coming to the fore. With encryption, organizations can effectively “secure the breach”—safeguarding specific sensitive assets even when other defenses fail. As organizations begin to expand their encryption usage, several realities become readily apparent:

- Encryption, and perhaps most critically, cryptographic keys, can’t be managed in a disparate, siloed fashion.
- The increasing adoption of cloud services and continued demands for compliance will only intensify the need to manage encryption and keys in a formal, centralized way.
- Leveraging hardware security modules (HSM) as well as standards like the OASIS Key Management Interoperability Protocol (KMIP) will become foundational requirements for central, enterprise-wide key management.

How are organisations contending with these realities as they seek to meet the need for more widespread encryption? This executive summary draws on an extensive survey to provide an update.
Finding #1: Ready or Not?  
The Tentative Step into the Cloud

The survey looked at the degree to which respondents have started to leverage cloud-based services, and the numbers tell two stories. On one hand, for the majority of respondents, the cloud is a reality. 62% are currently either experimenting with the cloud or running a combination of on-premise and cloud-based services. On the other hand, the percentage of respondents that are taking this hybrid approach is about equal to the percent that are not using the cloud at all.

Studies make clear that specific security concerns and challenges continue to put the breaks on cloud adoption, and limit the potential use cases. While the benefits of the cloud are unassailable, many organisations aren’t ready to make the plunge. When they do make the move, they are taking a hybrid approach so they can harness benefits where possible, while retaining control and visibility of on-premise security and infrastructure for their sensitive data and transactions.
Finding #2: The Compelling—and Growing—Need to Streamline Encryption and Key Management

As the move to the cloud continues, it is clear that more sensitive assets will ultimately find their way to the cloud, and when they do, encryption will need to be employed. In fact, of those taking a hybrid approach currently, 30% are already doing encryption in the cloud.

For enterprise IT and security teams, the number of encryption implementations seems poised to expand—and there's already plenty to manage as it is. The survey amply illustrates this point, with seven forms of encryption employed by 30% or more of respondents. Plus, there's more on the way: Between 44 and 49% say they're likely or very likely to implement encryption technology, data protection in the cloud, and/or storage encryption in the next 12-24 months.

For many organisations, this expanded use of encryption is going to pose some increasingly vexing challenges. Too many organisations are managing each encryption implementation in a siloed fashion, a model that simply doesn't scale as more users, use cases, and environments need to be supported. In particular, managing keys in a disparate, isolated fashion is difficult and time consuming, which means costs spiral upwards, policies can't be enforced consistently, or short cuts are made that can jeopardise security mechanisms. Overall, only 22% have key management that offers central policy administration currently, and as we'll detail later, that is increasingly going to be untenable for many organisations.
Finding #3: Compliance a Key Motivator for Strong Key Management

While it has been said before, it bears repeating: compliance does not equal security. In the U.S., mammoth breaches of retailers that are claiming to be compliant with PCI DSS offer just one recent and vivid illustration. With that said however, it appears those concerned with addressing regulatory and privacy mandates are being motivated to implement measures that those unconcerned with compliance are far less likely to do.

The survey looked at respondent's main reasons for doing encryption. Those who say the main reason for encryption is compliance are 2.7 times more likely than others to implement strong key management with audit controls—a vital capability not just for establishing compliance but overall security. Of that group, 43% have key management with audit controls. Of those who don’t say compliance is a main factor, only 16% have these audit controls. Further, this group not concerned with compliance is 50% more likely not to have a key management solution at all.

Those who say the main reason for encryption is compliance are 2.7 times more likely than others to implement strong key management with audit controls.
Finding #4: The One Key Capability that Separates the Key Management “Haves” from the “Have-nots”

The survey examined what key management capabilities respondents had in place, and through the details provided, some clear patterns emerge. Overall, 22% say they have key management that enables central policy administration. When it comes to key management, these organisations can be viewed as the “haves”, groups with an abundance of critical security controls, while all others are the “have nots.” Compared to all others, those with central policy management capabilities are:

- Three times more likely to have central logging.
- Over four times more likely to have separation of duties.
- Almost five times more likely to have secure logging.
- More than three times more likely to have audit controls.

As strong a picture as these numbers paint, this doesn't appear to be a message that is widely understood among today's management teams: Only 13% say they’re very likely to deploy enterprise key management—which is an essential way to establish central policy enforcement—in the next two years.
Conclusion

As organizations look to secure the breach and expand their encryption adoption, enterprise key management platforms will need to become a priority for many more organisations. It is only through this vital capability that organisations will be able to establish the controls they need to ensure compliance and establish an effective security framework. Further, this capability will be increasingly vital as organisations seek to scale their encryption capabilities to support additional use cases and environments, including the cloud.

In fact, the numbers would indicate that those with central policy management are already more likely to benefit from the cloud. Those with central policy management currently are over 25% more likely to be experimenting with the cloud or using a combination of cloud and on-premise today.

About the Survey

To gain a better picture of how organisations are contending with the evolving threat landscape, SafeNet undertook an extensive survey of the readers of Secure Computing Australia. More than 280 security professionals from Australia, the Asia Pacific, and India participated.

For more information on the breach statistics cited earlier, and to conduct a risk assessment for your own organization, be sure to visit the Breach Level Index site at breachlevelindex.com.

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.