THE
DATA
PROTECTION
COMPANY

The Current State of Encryption and Key Management

Where Security Gaps Persist—and Strategies for Addressing Them

WHITEPAPER

Executive Summary

While encryption has been employed for decades, much has changed recently, and more change is sure to come. In recent years, the use of encryption has continued to increase, but so too have the number and scope of threats. Where is encryption being employed today and why? Where do security practitioners see encryption's usage increasing? What do current usage trends tell us about existing security gaps, and how should those weaknesses be addressed? This paper draws from an industry survey to provide an overview of how organisations are using encryption today, and, based on these findings, it offers objective guidance into some of the best practices that can help organisations strengthen security and address their most pressing security gaps.

Introduction

Organisations in just about any industry and of any size have sensitive information that must be secured. In this endeavour, the penalty for failure can be high, with loss of business reputation and profits, job security, and even national security all being potential risks. While this may sound like hyperbole, consider one example:

> In 2011, one employee within a large security organisation was duped by a spear phishing attack, and opened a malicious file. That single compromise led to a series of attacks that ultimately resulted in the theft of sensitive intellectual property. The proprietary code that was stolen was subsequently used to launch attacks at several prominent customer sites—including major military defence contractors—with every indication being a sophisticated entity with geopolitical objectives was behind the coordinated attack.

Whether the primary objective is to combat increasingly sophisticated cyber attacks or ensure compliance with internal policies or regulatory mandates, encryption can play a critical role. In fact, while encryption methodologies have been around for decades, their use has expanded dramatically within the past few years. Today, in any single organisation, network traffic, fields in databases, tape libraries, mobile devices, and a host of other assets and systems may be encrypted. Further, as organisations increasingly leverage private and public cloud architectures and delivery models, encryption is increasingly a requirement to ensure sensitive assets remain secured in dynamic, multi-tenant environments. It is important to note that, as each new encryption platform is deployed, more cryptographic keys are introduced—and these keys must be secured and managed across their lifecycle, which can span years.

This paper looks at the current state of encryption and key management in organisations across Europe and the Middle East. Leveraging a survey conducted by SafeNet and SC Magazine, the paper offers a useful look at why, when, and how organisations are using encryption and cryptographic key management. The paper then describes some of the most significant security gaps that exist in many organisations, and it reveals some of the key strategies for addressing these gaps.

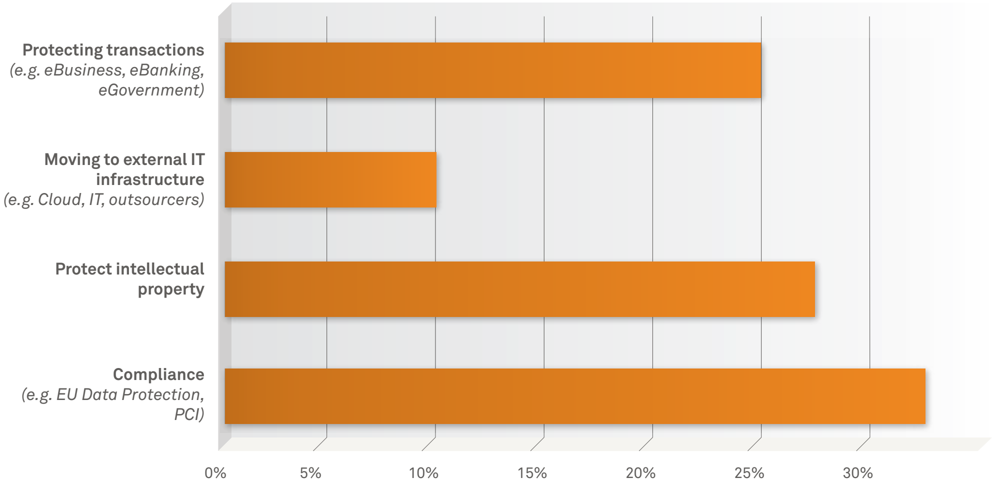
Current Encryption Status and Plans

In the following sections, we look at some of the most significant findings drawn from the survey, and offer some perspectives on the most important implications that can be drawn from these findings.

Reason for Encrypting: Key Findings and Implications

At a high level, there are three key objectives that are driving encryption deployments today. When respondents were asked what the primary reason for encryption was, the responses were split fairly evenly across compliance (34.1%), protecting intellectual property (28.8%), and protecting transactions (25.8%).

What is your primary reason for encrypting?



Organisations are using encryption for several key reasons, with compliance, protecting intellectual property, and protecting transactions being the most common

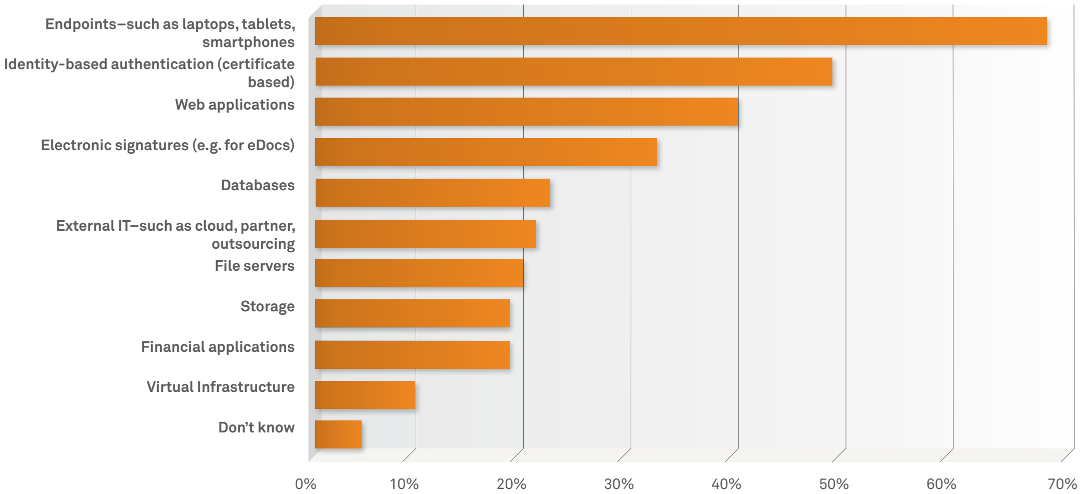
Today, only about 11% of organisations surveyed indicated that the primary reason for doing encryption was to secure data that is moved to external IT infrastructures, for example, to a cloud provider. However, as we'll see below, 22.1% of respondents are currently doing this type of encryption, and, as organisations continue to migrate more strategic assets and services to the cloud, this encryption use case is sure to expand substantially in the coming months.

Given the broad array of encryption technologies and approaches available, and their respective capabilities, strengths, and weaknesses, it stands to reason that the objectives of encryption have a significant influence on the type of encryption employed. The statistics uncovered by the survey indicate some clear trends in this regard. For example, for those who are using encryption to address compliance objectives, respondents were more likely to do database encryption and file server encryption than other organisations in the survey group. In businesses doing encryption for compliance objectives, 31% use database encryption and 29% use file server encryption, compared to 21% and 17% respectively in other organisations. In addition, those companies looking to protect transactions are far more likely to use encryption for identity-based authentication (62% vs. 45%) and electronic signatures (50% vs. 30%) than other respondents.

The Implications

These results make clear that the specific objectives and characteristics of an organisation's encryption deployments will be wholly unique to each organisation—and that's a good thing. Encryption, like any other security methodology, is just a tool, and encryption deployments will only be successful when the right tools are applied in the right way to address the appropriate security goal.

How are you currently using encryption today?



When asked how they are currently using encryption, respondents were most likely to cite encryption of endpoints, identity-based authentication, and Web applications.

Encryption Usage: Key Findings and Implications

When respondents were surveyed on the types of encryption their organisations employed, following are some of the key findings in various categories:

- **End point encryption.** Today, 67.6% of organisations surveyed are using end-point encryption, which makes it the most common form of encryption in use currently. This type of encryption is being used to secure laptops, smartphones, tablets, and removable media. When you consider the ubiquity of mobile devices, the high incidence of these devices being lost or stolen, and the increasingly sensitive nature of the assets that these devices house and access, it is clear that mobile endpoints represent a significant exposure for organisations, which is why the use of endpoint encryption is so widespread.
- **Identity-based authentication**. In light of the fact that most organisations have to support an increasingly distributed network of employees, consultants, vendors, and partners, it makes sense that almost half of the companies surveyed (47.6%) are using encryption for identity-based authentication.
- **Backend encryption.** When it comes to encryption in an organisation's backend infrastructure, respondents were fairly evenly split across file servers (20.7%), databases (23.4%), and storage (20%).
- **Virtualisation and cloud.** It is important to note how the use of virtualised and cloud infrastructures is also shaping encryption usage. Currently, 11% of respondents are encrypting their own virtual infrastructure, and 22.1% are using encryption in order to gain control over sensitive assets in external IT environments, whether in the cloud or an outsourced infrastructure.
- **Electronic signatures.** Another very common use of encryption is for electronic signatures, which helps secure eDocs, eBusiness, eGov, and related applications. Over 1/3 of respondents indicated that they are using encryption for these purposes.

The Implications

While the use of endpoint encryption addresses a very real, and increasing, security exposure, it is also clear that encryption in other points—both to secure initial access, and to provide defence in depth to augment these access controls—is also a critical requirement for many organisations.

Cryptographic Keys: Key Findings and Implications

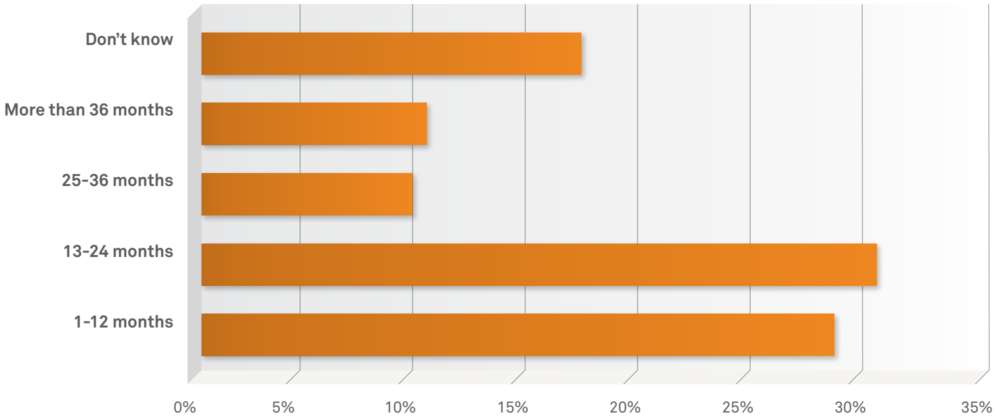
Managing cryptographic keys is a critical effort. If cryptographic keys are exposed, it can negate any of the security and compliance benefits promised by encryption. With that in mind, it is interesting to note the following statistics:

- Only 44% of respondents were very confident that they knew where all their organisation's cryptographic keys were.
- 16% of respondents didn't know how many keys their organisation managed, and 21% manage more than 100 keys.
- Almost half (48.5%) secure keys in software, while 36.8% do so in hardware.
- Only 29.1% rotate keys on a 12 month cycle or less, and 31.2% rotate between every 13 and 24 months.

The Implications

Too often, the efforts and tactics required to secure cryptographic keys aren't fully understood when security teams first embark on an encryption initiative. As the above results make clear, lack of visibility, control, and security of cryptographic keys represents a significant vulnerability in many organisations today.

How actively do you rotate your encryption keys?



When asked about key rotation, about 1/3 of respondents indicated they rotate keys on a 12 month cycle or less.

Encryption Management: Key Findings and Implications

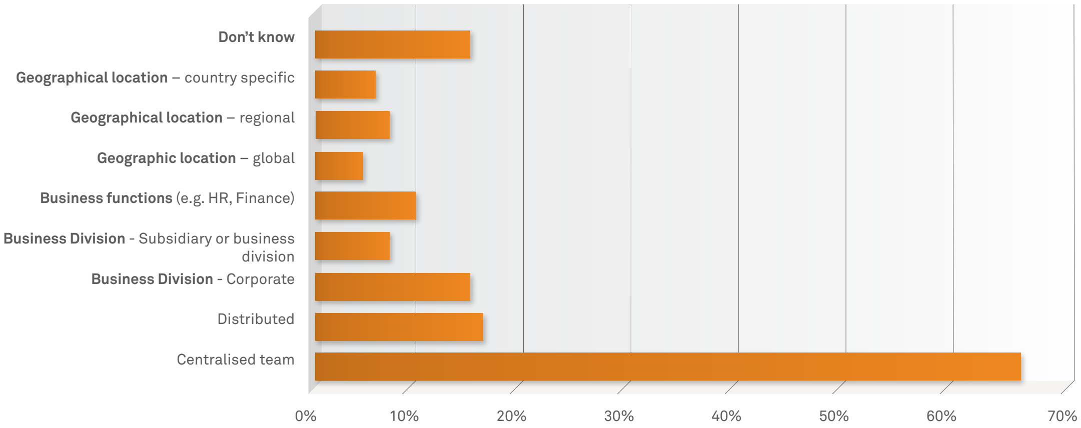
Of the respondents surveyed, more than half, 55.6%, have a central team managing cryptographic infrastructure and policies. By contrast, only 11.1% manage encryption according to business functions (such as human resources, finance, and so on), and only 7.4% manage encryption by each specific country.

While different regions and departments often have specific threats, regulatory and privacy requirements, and usage policies, it seems clear that many organisations still focus on central management of encryption. Given the sensitive, critical nature of encryption deployments, in most cases relying on a central team of security specialists to govern encryption makes most sense.

The Implications

Encryption management is a vital task, and it's one typically entrusted to small, resource-constrained groups within the security organisation. To effectively address their charters, these security teams have to focus on the most pressing security objectives, and find ways to efficiently deploy and manage their security infrastructures.

In your organisation, how do you manage cryptographic infrastructure?



More than 50% of respondents indicated they have a centralised team managing their encryption deployments.

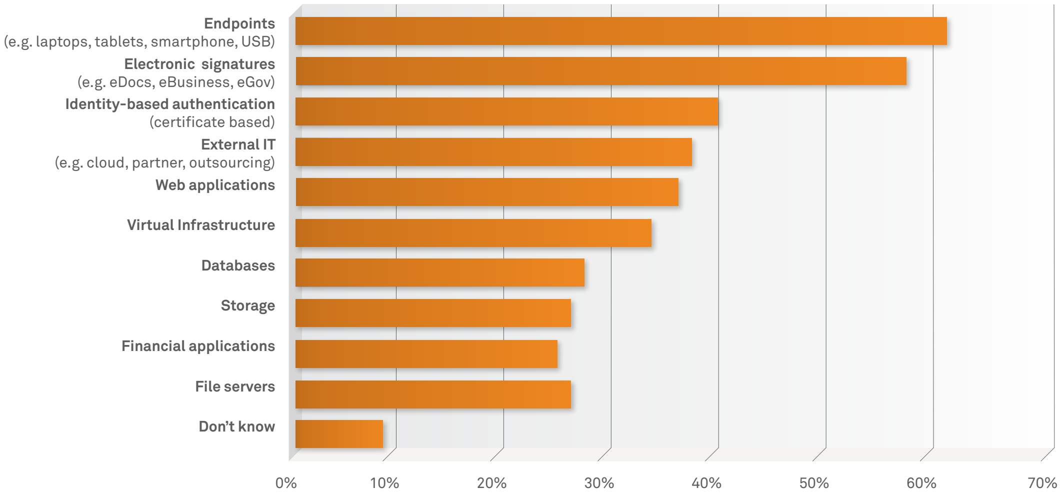
Plans for Encryption: Key Findings and Implications

In our survey, we asked respondents to tell us about their plans for encryption, and one way to sum it up is "more". With few exceptions, when comparing types of encryption currently employed versus areas of planned expansion over the next three years, the numbers increase across encryption deployment types.

Not only does endpoint encryption represent the dominant form of encryption in use today, but it is also the area in which most respondents see their encryption deployments expanding. In fact, 62.2% see their endpoint encryption deployments expanding in the next three years, a far bigger percentage than any other category. Electronic signatures and identity-based authentication represent the next two most prominent areas, with 48.1% and 40.7% of respondents seeing them as a growth category respectively.

Given the rise in the adoption of cloud delivery models, the fact that many see encryption in external IT a growth category makes sense. Comparing respondents who currently do encryption in this area, with the number that see it as an area of growth, we see an increase from 22.1% to 38.5%. Similarly, a significant percentage of respondents expect to see expansion in the area of encrypting the virtual infrastructure, which also seems a clear direction based on the increased adoption of virtualisation technologies. In fact, when comparing the statistics for current usage versus planned expansion, this category has the biggest increase, with 11% currently doing encryption in this area, and 34.1% seeing it as an area of growth.

In which areas do you see your encryption deployment expanding over the next three years?



When outlining their plans for encryption growth, endpoint encryption, electronic signatures, and identity-based authentication were the three most commonly cited categories.

The Implications

When exploring encryption plans, we see there will be more—both more of the same and more of the new. Using encryption to secure endpoints, identity-based access, and electronic signatures represent traditional uses of encryption—and areas where growth will continue. These results also make clear that virtualisation and cloud deployments will have significant implications for security teams, representing a new and rapidly emerging requirement for encryption.

Implementation Strategies

Given the current usage of encryption and some of the trends taking shape, there are several key strategies security management should look to focus on in the coming months. The following sections outline some of the most important strategies executives can employ in order to effectively achieve their objectives.

Centralisation of Administration

As outlined in the prior section on plans for encryption, pretty much across the spectrum, the use of encryption is expected to increase as organisations continue to address their regulatory mandates and security policies. In direct opposition to this trend toward more, however, is the fact that most IT and security organisations have to contend with less: smaller staff sizes, reduced budgets, and less time. In fact, 69.1% have a team of five or less to manage encryption and 84.5% have teams of 10 or less.

For these small security organisations to contend with increased encryption demands, administrative efficiency will be a vital imperative. As opposed to having security functions distributed across departments and geographies, most organisations will be well served by centralising encryption management, both from an efficiency and a security standpoint. This includes managing encryption administration and policies, not only across distributed geographies, but across both internal and cloud deployments as well. Further, organisations need to be able to start centrally managing policies across disparate encryption technologies, including those for encryption on end points, databases, storage platforms, and so on.

Encryption for Securing Sensitive Assets in Virtual Environments

As outlined earlier, the use of encryption to secure sensitive assets in virtualised and cloud environments is expected to increase substantially. That's because, as sensitive assets are migrated to virtualised resources, a host of challenges can be presented. For example, many virtual environments have shared resources with multiple tenants, which can present risks of unauthorised users gaining access to sensitive assets. Limited visibility, the mobility of assets, and administrator privileges can also be difficult to contend with in virtual environments.

For organisations that have to comply with the Payment Card Industry Data Security Standard (PCI DSS), encryption will also be a critical means for adhering to such regulations as 3.4, which requires the security of stored cardholder data. In the past, organisations were able to avoid the use of encryption by applying so called "compensating controls", that is, employing such measures as physical isolation, tighter management controls, and IPS level functionality. However, those organisations that employed these types of compensating controls, and who are now looking to migrate PCI-regulated data into virtualised environments, now confront a significant obstacle: Quite simply, the notion of physical isolation goes away in a virtualised environment. Consequently, when organisations undergo their mandatory annual reviews, control requirements may not be met, and encryption may be unavoidable in order to address this specific requirement.

To ensure compliance and effectively secure sensitive data in virtualised environments, organisations need to leverage proactive, robust security controls enabled by encryption. This includes employing encryption in the following areas:

- **Instance encryption.** By encrypting virtualised instances, organisations can guard against a host of vulnerabilities. For example, this type of encryption significantly reduces the number of ways users can get sensitive data off physical images. It also enables organisations to enforce the separation of duties required.
- **Data level encryption.** Through database and application encryption solutions, organisations can more granularly apply security policies to specific subsets of data, for example at the column level in a database. This represents a way to have data secured as it progresses through workflows, and represents an ideal complement to instance encryption.

Secure, Efficient Key Management

Leverage Hardware

As outlined earlier, only 36% of survey respondents reported that they secure keys in hardware, and only 44% were very confident that they knew the location of their keys at any given time. This poses significant risks, and potentially negates many of the security benefits of encryption.

In most organisations, servers play a fundamental role in encryption, acting as a central repository for cryptographic keys. As a result, a breach of these systems can compromise the integrity of the entire infrastructure. Too often, general purpose servers are used, which store keys in software, leaving memory unprotected and keys in clear text. Consequently, keys can be exposed by malicious administrators, software exploits, and a host of other threats. For example, when keys are stored in software, an attacker needs only to find a copy of the server's backup files and can then exploit a number of vulnerabilities.

On the other hand, purpose-built encryption appliances and hardware security modules (HSMs) can digitally sign hardware-based backups and apply physical security mechanisms to keys. Applications communicate with keys stored in the appliance or HSM via a client—but keys never leave the devices. By leveraging these specialised platforms, many organisations can address a significant gap in their defences.

Centralise Keys

Because keys are held on disparate, general purpose systems—often on the very systems containing the sensitive data—they are vulnerable to theft and misuse. And the more locations keys reside in, the more pervasive an organisation's risks. In addition, as keys are backed up, if they are, they often aren't secured in transit, which leaves them further exposed.

Centralise Key Administration

Administrative efforts such as key rotation can help strengthen security, however, this key rotation has to happen securely and efficiently. To be practical, enterprise key management needs to represent a move to a point in which keys are centrally managed across the enterprise, including across heterogeneous database platforms, application environments, endpoints, cloud deployments, and more. Following are several benefits of this approach:

- **Decreased exposure of keys.** Centralising key management offers fundamental advantages in security as it limits the number of locations in which keys reside, minimising the potential for exposure.
- **Consistent policy enforcement.** Centralised key management makes it practical for administrators to more consistently enforce corporate standards and policies across the organisation. For example, an administrator can set user credentials and policies around a specific asset once, and then ensure those policies are effectively employed, whether that data is saved to a database server, mainframe, or laptop.
- **Streamlined administration.** At the same time, centralised key management also streamlines administration, enabling administrators to make changes and updates once, and have them propagated across all pertinent areas.
- **Encryption efficiency.** This also represents a more efficient model: As opposed to point encryption, where data on one platform would have to be decrypted and re-encrypted when it is transmitted to another platform, a specific asset can be encrypted once, and distributed to multiple systems, and only need to be decrypted when an authorised user needs access to it.
- **Unified auditing and remediation.** Finally, having all keys centralised also can significantly streamline auditing and remediation by housing audit logs that encompass all key-related activities.

Within this context, the key management interoperability protocol (KMIP) standard, which was ratified in 2010, represents a significant development. The KMIP standard was developed by the Organisation for the Advancement of Structured Information Standards (OASIS). KMIP was developed in order to establish a single, comprehensive protocol for standard communication between key management servers and the enterprise-wide cryptographic clients that use these keys. By leveraging technologies that adhere to the KMIP standard, organisations can begin to centralise key management for a number of disparate encryption platforms that may currently be deployed in the enterprise.

Need for Persistent, Data Centric Encryption

Make no mistake, the end point encryption and authentication approaches that are common today will remain critical endeavours. However, to combat the advanced threats plaguing organisations, many security teams need to augment these mechanisms with additional layers of security that focus on specific assets in a more granular, persistent fashion.

These encryption mechanisms need to enable administrators and end users to employ encryption in a granular way, both by user and group permissions, asset type, and specific asset. This means being able to encrypt a credit card column in a database, and potentially a spread sheet with sensitive payroll information. An added benefit of this approach is that the more granular encryption, the more granular an audit trail is for compliance, monitoring, and remediation. Following are several encryption requirements:

- **Persistent.** Encryption needs to be enforced persistently, so that, if a sensitive file is emailed, saved to a flash drive, stored in a cloud-based application, or transported anywhere else, security policies will remain in effect.
- **Top-down policy enforcement.** Administrators need to enforce policies in a top-down manner, so corporate-wide policies can be applied consistently and cohesively across the enterprise, and down to the specific asset and user level.
- **End user transparency.** To maximise adoption, enterprises need to employ encryption in a way that is completely transparent to end users, ensuring optimal security and productivity.

Conclusion

As the survey results outlined above indicate, security teams should be gearing up for more in terms of encryption—more use cases, more deployments, and more cryptographic keys to manage. To support this growth, both securely and cost effectively, security teams will need to realise improved efficiencies—particularly in terms of administration and policy enforcement. Toward this end, leveraging central key repositories and management platforms that support disparate encryption deployments and technologies will be increasingly invaluable.

About the SC Magazine/SafeNet Survey

The findings in this white paper are drawn from a survey conducted by SC Magazine and SafeNet in late 2011. Survey respondents represented organisations from a range of industries, including high technology, financial services, higher education, government agencies, and health care. More than 300 individuals from across Europe and the Middle East participated in the survey.

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 organisations 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.

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/connected