SafeNet

THE
DATA
PROTECTION
COMPANY

SECURE THE BREACH

A NEW SECURITY REALITY:
THE SECURE BREACH

For more information,
please visit:
www.securethebreach.com

Breach Prevention: The Root Cause of the Data Breach Epidemic

According to the 2014 Verizon Data Breach Investigations Report there were 63,437 reported security incidents and 1,367 confirmed data breaches in 2013. This total represents the highest amount of data breaches over the entire ten-year range of this study.[1] According to Forrester Research, security spending in 2013 represented 17.5% of total IT spending.[2]

"Face reality as it is, not as it was or as you wish it to be."

– Jack Welch, former CEO, General Electric

These statistics summarize today's reality in IT security: security is consuming a larger share of total IT spending, but security effectiveness against the data-breach epidemic is not improving at all. The root cause of this trend is captured in the spirit of Jack Welch's quote: enterprises are not investing in security based on reality as it is; they're investing based on reality as it was: a bygone era where hackers were glory-seeking vandals, sensitive data was centralized, and the edge of the enterprise was a desktop PC in a known location. And in this reality, network firewalls and other network perimeter "breach-prevention" technologies were good enough.

Unfortunately, yesterday's "good enough" approach to security is obsolete in an age where data is distributed across and beyond the enterprise, and hackers whether skilled criminals or insiders – both malicious and accidental – are a constant threat to data compromise. The largest organizations have fallen victim to data breaches. According to **SafeNet's Breach Level Index** there were 1,056 data breaches and more than 575 million data records lost or stolen in 2013. Moreover, the tally for records lost or stolen is already up to 760,044,022 million for 2014.[3]

There is nothing wrong with network perimeter security technologies – they are an added layer of protection. The problem is, many enterprises today rely on them as the foundation of their data security strategy and unfortunately there is really no fool-proof way to prevent a breach from occurring. Alarmingly, market trends show that the lion share of organizations have no plans of changing this approach. According to IDC, of the $32 billion enterprises spent on security technology in 2013, more than 26% ($8.4 billion) was invested in network perimeter security. Additionally, through 2017 they project a 7.1% growth rate of organizations investing in methods to prevent the breach. [4]

SafeNet's Breach Level Index tracks publicly disclosed breaches and allows organizations to do their own risk assessment. By providing a few simple inputs companies can calculate their risk score and overall breach severity level.

If IDC's projections are accurate and breach-prevention technology continues to consume a growing and disproportionate amount of enterprise-security investment, the enterprise data-breach epidemic will be as prevalent as ever in 2017. In fact, it will likely be much worse than it is today, because while enterprises invest in reality as it was, adversaries are thriving and innovating in reality as it is.

[1] http://www.verizonenterprise.com/DBIR/2014/

[2] Forrester Security Survey Q2-2013

[3] http://www.breachlevelindex.com

[4] IDC, Worldwide IT Security, Products, 2013 – 2017 Forecast and 2012 Vendor Shares: Comprehensive Security Product Review, December 2013

From Breach Prevention to Breach Acceptance

The Verizon report indicates that insider threats have been increasing over the last couple of years. So by definition, breach prevention is an irrelevant strategy for data protection because every organization already has potential adversaries inside the perimeter. Disregarding these internal threats not only invites blatant misuse but also fails to protect against accidental carelessness. Even non-malicious behaviors such as bringing work home via personal email accounts, lost devices, storing data on USB drives and unknowingly sharing passwords are a few examples of how easy it is to innocently leak sensitive data.

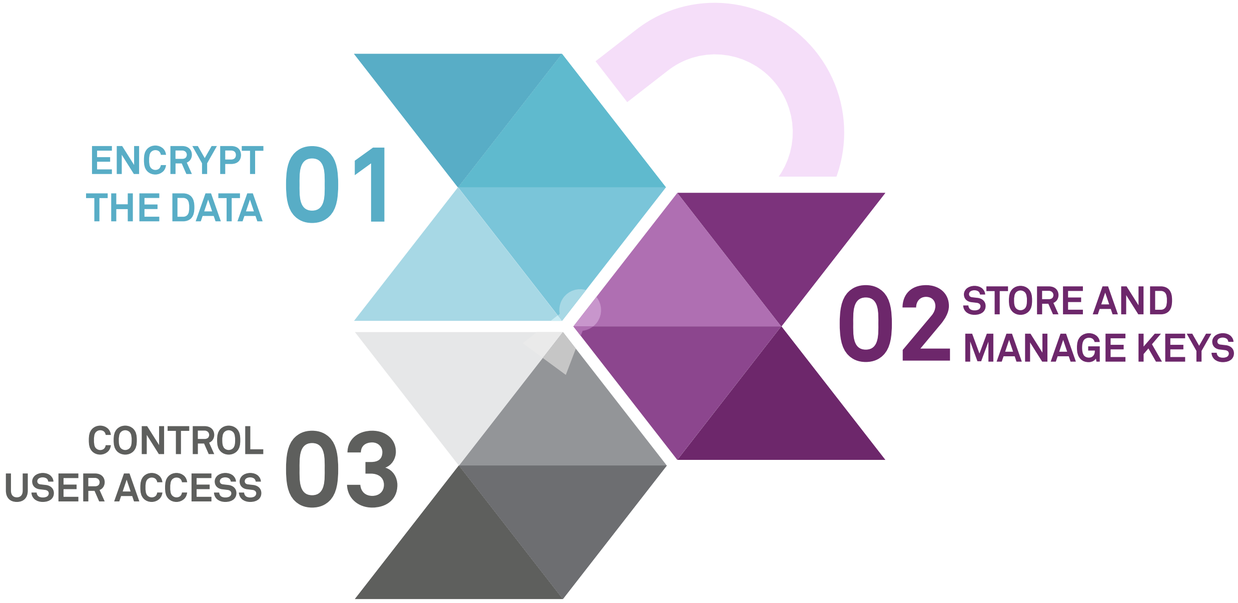
The numbers do not lie – whether internal or external, breaches are inevitable. In today's environment, the core of any security strategy needs to shift from "breach prevention" to "breach acceptance." And, when one approaches security from a breach-acceptance viewpoint, the world becomes a relatively simple place: securing data, not the perimeter, is the top priority.

Securing the data is a challenging proposition in a world where cloud, virtualization and mobile devices are causing an exponential increase in the attack surface. Many organizations might be inclined to address this problem with a 'containment' strategy - limiting the places where data can go, and only allowing a limited number of people to access it. However, this strategy of "no" – where security is based on restricting data access and movement – runs counter to everything technology enables today. The mandate today is to achieve a strategy of "yes," which is built around the understanding that the movement and sharing of data is fundamental to business success.

Once you implement the technology and controls required to mitigate human error and decrease adversary ROI, you substantially decrease the risk of incurring a data breach.

From Breach Acceptance to Securing the Breach

It's one thing to change your mindset. It's another to implement a new approach to security across an organization. While there is no "one size fits all" prescription for achieving the Secure Breach reality, there are three steps that every company should take to mitigate the overall cost and adverse consequences that result from a security breach. Encrypt all sensitive data at rest and in motion, securely manage and store all of your encryption keys, and control access and authentication of users. By implementing each of these three steps into your IT infrastructure, companies can effectively prepare for a breach, and avoid falling victim to one.



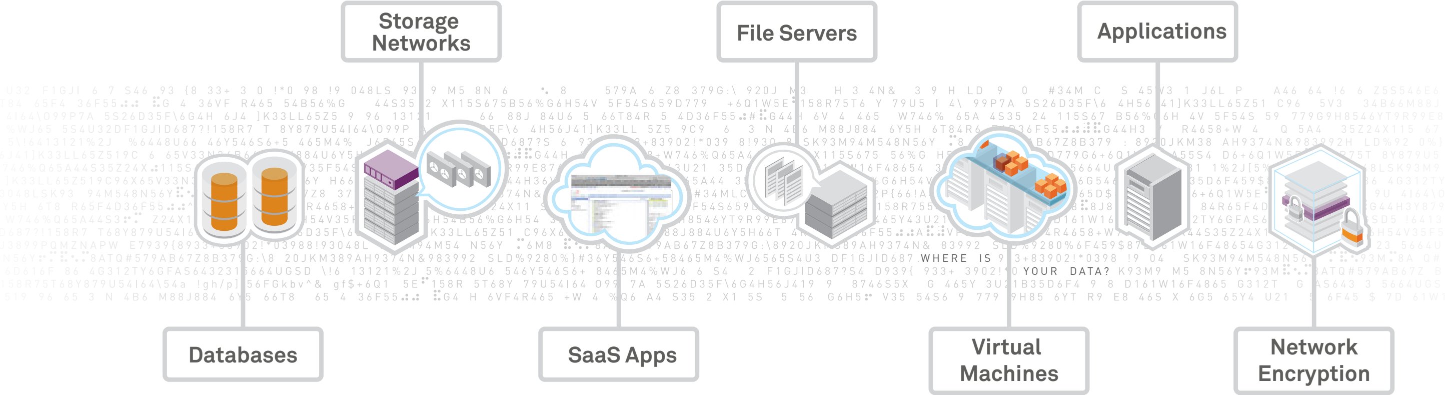
SafeNet
3 Step Approach

ENCRYPT THE DATA

01: Where is your data?

Adversaries are after your data; take the time to identify all emerging threats to your organization. You should move your security controls as close as possible to the data. By embedding protection on the assets themselves you ensure that even after the perimeter is breached, the information remains secure.

Locate and prioritize your most sensitive assets and repositories. Start with the data center; search your storage and file servers, applications and data bases. Whether structured or unstructured, data that exists in physical, virtualized and cloud environments can all be encrypted. Review normal business activity both within and beyond the enterprise, and understand how it maps to the underlying technology infrastructure.



760,044,022

MILLION RECORDS LOST SINCE 2013

-Breach Level Index

www.breachlevelindex.com

Do not overlook the network traffic flowing from branch offices to headquarters or any other offsite locations. Once this data leaves the confines of your organization, you no longer have any control over it. Cyber criminals are standing by to easily and cheaply ‘tap’ your fiber optic cables. Aside from malicious attempts there are also genuine risks of transmission to wrong locations. However, these risks can be eliminated and security assured, by automatically encrypting the data while it’s in motion.

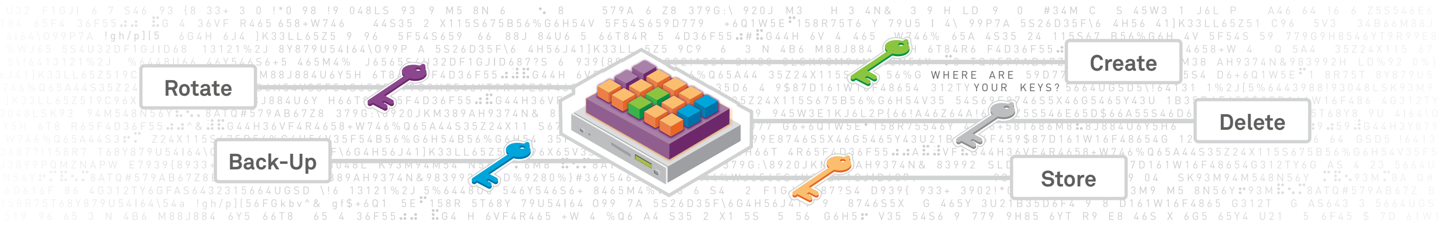
This is not an entirely new concept – the promise of data encryption is familiar territory for most security professionals. However, the technological capability to encrypt data on an enterprise scale, in a centralized way that does not disrupt the flow of business, is relatively new. It can be done. By managing and storing your keys centrally, you can streamline your encryption infrastructure for auditing and control.

STORE AND MANAGE KEYS

02: Where are your encryption keys?

At the heart of any data encryption solution are the secret cryptographic keys used for encrypting and decrypting sensitive data. Lost or stolen keys can take down the entire data and security infrastructure.

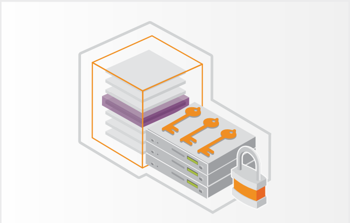
The volume and variety of data that needs to be encrypted in a secure breach environment involves potentially millions of encryption keys. When each of these components has isolated, disconnected key management, it becomes nearly impossible for an organization to adequately protect the keys. Since keys are being stored in a variety of places, often on the very systems containing sensitive data, they are vulnerable to theft and misuse. Furthermore, backed up keys are not being secured while in transit, leaving another area of exposure.



A crypto management platform enables centralized management of the entire key lifecycle across the extended enterprise. On-going rotation, storage, backup, deletion and creation of keys is required to avoid security vulnerabilities leading to exposed data. To further strengthen security, you should also consider safeguarding the key storage container. Software key wrappers do not protect the encryption keys as well as hardware-based options; therefore vaulting your keys in a hardware security module (HSM) will give you an added layer of protection.

Remember, encryption is only as strong as its crypto management platform. By adhering to the following guidelines, you can store and manage your keys effectively:

- Build a foundation providing a trust anchor for the implementation of encryption enterprise wide. This foundation handles important tasks including secure key generation, storage, archiving and termination.
- Implement enterprise key management to create and enforce policies during the life of a key and its use, and to ensure the keys are available to the information and applications across the enterprise.
- Limit access to your cryptographic keys. Enact a separation of duties policy, whereby administrators can manage data resources, without having access to the information inside those files.



Vaulting your keys in a hardware security module (HSM) will give you an added layer of protection

CONTROL USER ACCESS

03: Who is accessing your data?

Good crypto management will safeguard your sensitive data, but you also need to control who has access to it. The proliferation of mobile devices and cloud-based applications are creating points of vulnerability, warranting more stringent internal controls. Organizations need to know that their networks are secure and that user identities are not only protected, but authorized. Strong authentication will block unauthorized access and hold authorized individuals accountable for their usage of digital resources.

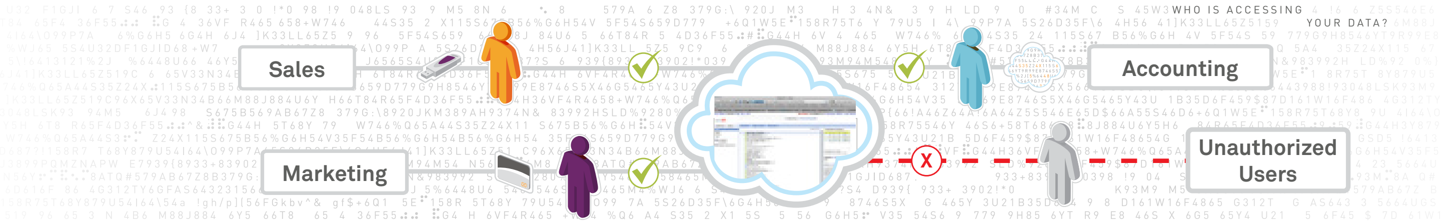
Relying on a simple username and password creates a false sense of security. This is not a strong method for protecting you, your company, your data or your customers. Passwords are considered the most vulnerable form of authentication as they can be easily hacked, stolen, copied or shared. Strong authentication requires users to login to online resources with something they know – a username – combined with something they have – such as a one-time passcode that is generated on a separate token. Only users possessing a combination of both factors will be given access.

Furthermore, by applying different authentication methods to different user groups, organizations can leverage role-based access to prevent the misuse of data and systems by insiders. Software and hardware-based tokens can be administered according to set roles or functions within the organization.

Authentication protects user identities and allows companies to adapt their business to complex environments securely, meeting the challenges of cloud, mobility and escalating threats.

For more information, please visit:

www.securethebreach.com



The Secure Breach Future

The current mass-market perception of data breaches is relatively naïve. Breaches continue to be positioned as sensational events in the headlines, and rarely is there an understanding that not all breaches are the same. In fact, not all breaches are "bad" breaches either.

For example, Zappos and Lockheed Martin received significant negative media attention for their breaches. A few outlets, however, were savvy enough to write positive stories about them, because both had taken sound security precautions to meet regulatory requirements and protect sensitive assets. According to publicly available information, these breaches were, for the most part, secure breaches – intruders penetrated the network perimeter, but they were unable to access valuable data.

As enterprises move into "reality as it is," the ripple effect will be that mass media and the population at large will evolve its perceptions of data breaches. They too will move from a "breach prevention" mindset, to one of breach acceptance. The fact that a breach has occurred will no longer be the "news." Rather, news value will be determined by the answer to this question: "Was it a Secure Breach?" Breaches will become like the weather – major hurricanes will garner headlines; drizzly days will not. All current trend-lines lead to more data breaches. As enterprises are investing significant security dollars to extend the life of the obsolete breach prevention strategy, adversaries are continuing to innovate and thrive. Furthermore, the extension of the enterprise into the cloud and onto mobile devices is greatly increasing the potential attack surface and the likelihood of accidental data exposure or loss. These trends all point to a consistent theme – security needs to be attached to the data, so enterprises can maintain control of the data even when it is deployed in the cloud or on mobile devices, and even when it falls into the hands of adversaries. Trying to keep today's adversaries out of the enterprise through breach prevention is a fool's errand (even adversaries that are not terribly sophisticated). By implementing a three step approach - encrypting all sensitive data at rest and in motion, securely managing and storing all of your keys, and controlling access and authentication of users - you can effectively prepare for a breach. It is being done today, as the Zappos and Lockheed examples show us. It is also a requirement for transitioning from a strategy optimized for "reality as it was" – breach prevention – to a strategy optimized for "reality as it is"– the Secure Breach strategy.

"By implementing a three step approach - encrypting all sensitive data at rest and in motion, securely managing and storing all of your keys, and controlling access and authentication of users - you can effectively prepare for a breach."

SafeNet
3 Step Approach

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.

SafeNet's Breach Level Index

Not all breaches are created equal. Breaches are no longer a binary proposition where an organization either has or hasn't been breached. Instead they are wildly variable—having varying degrees of fallout—from breaches compromising entire global networks of highly sensitive data to others having little to no impact whatsoever. This environment demands a tool that examines breaches on a case-by-case basis to fully understand and indicate their severity.

To accomplish this goal, IT-Harvest and SafeNet developed the Breach Level Index (BLI). The Breach Level Index is designed to provide a simple way to input publicly disclosed information on data breaches and calculate a score indicating breach severity. We invite organizations to do their own risk assessment at: **http://www.breachlevelindex.com**

Contact Us:
For more information on how to Secure the Breach, please visit: **www.securethebreach.com**
For media inquiries, please contact Chad Couser: **chad.couser@safenet-inc.com**

Follow Us via Social Media:
www.safenet-inc.com/connected

For all office locations and contact information:
Please visit **www.safenet-inc.com**