Secure The Breach:
A Step-by-Step Guide for Today's Digital Enterprise
The number of connected things in use is expected to grow to 20.6 billion by 2020.
Securing Your Digital Transformation

The digital world is transforming every aspect of our daily lives, and that includes the way we work. To compete, today’s enterprises are embracing the simplicity and ease of the cloud and SaaS applications, the convenience of mobility and bring your own device, the increased insights from connected devices and the Internet of Things, as well as the need to mine more value from more information with big data and analytics platforms. These are just a few of the emerging technologies that are helping to move business forward, faster.

However, there’s one technology investment that isn’t keeping pace as enterprises undergo their digital transformation—security solutions that are effective against the data breach epidemic.

Sources:
2. IBM [https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN]
3. Ponemon Institute & Gemalto, 2018 Global Cloud Data Security Study [http://www2.gemalto.com/cloud-security-research/]

90% of the world’s data was created in the last two years

43% of all corporate data is stored in the cloud
Your Data is Moving Beyond the Perimeter. So Should Your Security.

Today, it’s important to adapt your security strategy to align with the way your business works. You’re producing, storing, and sharing data in more places. You have more networks, clouds, and devices accessing your corporate resources. You’re faced with more advanced threats as your attack surface sprawls. There are more compliance and regulatory mandates that need to be met to protect sensitive data. And, as your team grows to manage all of this, there’s also greater risk of human error.

Don’t rely on perimeter security alone to address these data security challenges. These traditional security methods simply can’t keep pace with the growing needs of your business. Here’s how to evolve your strategy to effectively prepare for a breach, instead of falling victim to one.

The Belief
94% of enterprises say their perimeter security technology is quite effective at keeping unauthorized users out of their networks.

The Reality
65% of enterprises aren’t confident their data would be secure in the event of a breach.⁴

Sources:
⁴Source: 2017 Gemalto Data Security Confidence Index report
The New Data Security Mindset

More than 1.3 billion records were exposed as a result of data breaches in 2016. It’s time for a fundamental shift in the security paradigm.

Stop pretending that you can prevent a breach. Accept that your organization’s perimeter will be breached and defend what’s really under attack – identities and data.

To do this, you will need to deploy a secure breach strategy that allows you to manage and control user access, while applying security directly to the data. This ensures your sensitive data remains protected and secure - even if the perimeter is breached and high-value assets fall into the wrong hands.
Step 1: Encrypt Sensitive Data

The first step in your secure breach strategy is to protect your sensitive data. To do this, determine where your most sensitive assets reside across your on-premises, cloud, and virtual environments. Search your file servers, applications, databases, and virtual machines for data at rest that must to be protected.

And, don’t forget to consider the network traffic flowing between your physical offices or other offsite locations. Once this data leaves the confines of your organization, you lose control over it. Attackers are ready to ‘tap’ the fiber optic cables, and human error can result in data transmission to the wrong location.

Once you’ve located your sensitive data, encrypt it. Encryption is the critical last line of defense in the event of a breach because it applies protection and controls directly to your data and keeps it secure wherever it goes.

Remember, encryption must be implemented properly to be effective. Be sure to also take steps to keep the encryption keys that can unlock your protected data safe too.

Sources:

51H 2017 Breach Level Index

More than 95% of all breaches in 2017 involved data that was not encrypted.5
Step 2: Own and Secure Encryption Keys

As the amount of data that you need to encrypt grows, so will the number of encryption keys. If you attempt to manage these keys in silos, it can leave them vulnerable to theft and misuse—especially if they are stored with the encrypted data or managed by a third party, such as a cloud service provider.

The next step in your secure breach strategy is to centrally and securely manage and store your encryption keys. Enterprise key management provides a foundation for deploying encryption across your distributed organization. It enables you to centralize the management of important tasks including secure key generation, storage, rotation, back-up, and deletion. You also have the ability to define and control access to your protected information, ensuring you maintain complete ownership and control of your protected data and keys at all times.

For an added layer of high-assurance security, you should consider storing your keys in a hardware security module (HSM). An HSM is a trust anchor that can securely manage, process, and store your cryptographic keys.

Sources:

61H 2017 Breach Level Index

Only 52% of organizations control their encryption keys when data is encrypted in the cloud.⁶
Step 3: Manage and Control User Access

Good encryption and key management will safeguard your sensitive data, but you also need to control who can access it. As your enterprise adopts new technologies such as mobile and cloud applications, increased controls are necessary. After all, relying on a simple user name and password is not an adequate method for protecting you, your company, your data, or your customers.

The final step of your secure breach strategy is to control and manage access to your corporate resources. Access management enables you to verify a user’s identity, assess and apply the appropriate access policy, and enforce the appropriate access controls using single sign on.

Access management enables you to secure the breach by providing:

> **Security:** Apply the appropriate security policy for each access attempt and enforce the appropriate level of trust

> **Visibility:** Know which access controls are applied, track application usage, and know who is accessing which apps and when

> **Scalability:** Add new user groups, apps and policies as needed, eliminate help desk overhead associated with password resets, and centrally define access policies for all of your cloud applications

> **Convenience:** Enable easy access through single sign on (SSO)
Welcome to the Era of the Secure Breach

All breaches are not equal—some are secure, some are not. While it may be difficult to accept that your organization will be breached, it’s not admitting defeat. In the era of the secure breach, you’re only defeated when an attacker gains access to your organization’s sensitive data.

When you execute a secure breach strategy, you not only protect your data in the event of a breach, you also address many of the other security challenges you face across your organization, including the need to:

> **Strengthen security:** Eliminate islands of security and apply a unified strategy to manage access and secure data and identities.

> **Achieve compliance and reduce audit costs:** Get the visibility and holistic reporting you need to meet compliance and regulatory mandates.

> **Reduce IT costs:** Save time and money with proven security processes that can be repeated across your organization.

> **Increase IT and business agility:** With a centrally managed data security platform, IT becomes more nimble and can focus their efforts on new technology projects.
Security Delivered the Way You Want It

Gemalto’s portfolio of SafeNet Identity and Data Protection solutions provides centralized, enterprise-ready data protection across all on-premises, cloud, and hybrid environments. Our centralized and proven access management and multi-factor authentication, encryption, and enterprise key management solutions ensure your business keeps data secure even when the perimeter is breached.

Solutions are available to be deployed on-premises or on demand from the cloud. And because they integrate with a growing ecosystem of today’s leading technologies, your data will stay secure now and into the future as your business continues to undergo its digital transformation.

To learn more, connect with us:

- Facebook
  https://www.facebook.com/GemaltoSec/
- LinkedIn
  https://www.linkedin.com/showcase/5782/
- Twitter
  https://twitter.com/gemaltosecurity?lang=en
- YouTube
  https://www.youtube.com/user/SafeNetInc
- Blog
  https://blog.gemalto.com/supercategory/security/
ABOUT GEMALTO’S SAFENET IDENTITY AND DATA PROTECTION SOLUTIONS

Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions—from the edge to the core. Gemalto’s newly expanded portfolio of SafeNet Identity and Data Protection solutions enables enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.