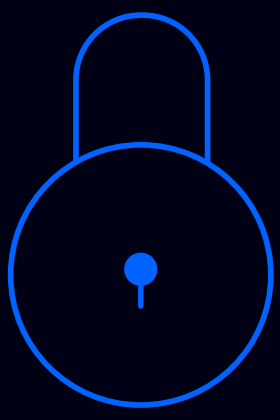
Why pervasive encryption is the future of data security



THE TRUTH ABOUT DATA BREACHES

#1: They're costly.

A recent Ponemon study[1] found that the average cost of a breach in 2017 was $3.6 million.

#2: It's not a matter of if, but when.

That same study found that the likelihood of an organization experiencing a data breach of more than 10,000 records in the next two years is 27.7% (That's up from 25.6% in 2016[2])

#3: Your data is either encrypted or exposed.

Of the nearly 9 billion records breached since 2013, only 4% were encrypted[3].

WHY ISN'T EVERYONE ENCRYPTING EVERYTHING?

The Ponemon study found that extensive use of encryption was the second-most effective factor in reducing the cost of a breach. It's also one of the only specific technologies mentioned in compliance regulations such as PCI DSS and GDPR.

So why is the number of encrypted records so low?

Encryption is hard.

- It takes a ton of compute power
- It slows down applications
- It's expensive (US regulation compliance costs businesses $1T per year)

That's why most companies practice selective encryption instead of pervasive encryption.

WHAT'S WRONG WITH SELECTIVE ENCRYPTION?

It requires data prioritization and application changes, which require additional skills, resources, and budget.

Here are some of the common questions that organizations struggle with when they take a look at implementing an encryption strategy:

1. **What data needs to be encrypted?**
   - Sensitive data? Only the data needed for compliance?
   - Identification and classification is labor intensive and time consuming.
2. **Where should the encryption occur?**
   - Hardware? Operating system, database level, in application, or on network?
   - There are pros and cons for each, including: level of protection, cost, complexity, time to implement
3. **Who in the organization is responsible for encryption?**

   Many organizations lack an enterprise-wide data encryption strategy. A comprehensive approach to data protection requires a huge investment in time and money to stitch together a collection of point solutions or to open applications and embed encryption directly into the application themselves.

So what's the answer?

Protecting the data at the core of the enterprise starts with

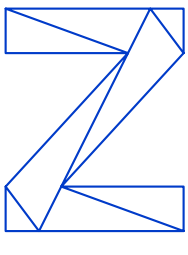
BUILDING A PLAN FOR PERVASIVE ENCRYPTION

How would it work?

Unlike selective encryption, pervasive encryption enables you to implement encryption and protect your data separately from the process of identification and classification. Pervasive encryption protects all the data associated with applications and databases, simplifies the administration through policies, and includes hardware and software changes to pervasively encrypt data without requiring application changes and without negatively impacting SLAs.

Find out how you can build an envelope of protection around all of your data anywhere it resides, with zero application changes.

Are you ready to get started?



[1] "Ponemon Institute, 2017 Cost of Data Breach Study, Global Overview, June 2017"
[2] "Ponemon Institute, 2017 Cost of Data Breach Study, Global Overview, June 2017"
[3] Data from www.breachlevelindex.com