Data Security & Privacy: a VGS Competitive Differentiator

Introduction

In 2021, data security and privacy are competitive differentiators for successful firms. These concepts provide foundational building blocks for ethical business practices. Companies that do not focus on data security and privacy are unsustainable. They tend to suffer data breaches, find it difficult to retain customer loyalty, and even lack employee trust[1].

Sensitive data, such as Personally Identifiable Information (PII), must be protected. But a wide range of threats, vulnerabilities, and rapidly evolving regulation have put network defenders in a difficult position. Eventually, most companies find that traditional information security strategies are fraught with challenges - and not worth the risk and cost of losing sensitive data.

There is a new and better approach to corporate information security called "Zero Data," based on the idea that it is possible to benefit from sensitive information without having to store or secure it. So when data thieves and hackers break into your house, there are simply no jewels to steal.

Recent Data Breach Statistics

80%

of breaches included customer PII

IBM

In 2020, 80% of breaches included customer PII, customer PII was the data type most often lost or stolen, the average cost per PII record was $150, and the average total cost of a data breach in the US was $8.64 million[2].

44%

of breaches compromised PII

Forrester

44% of breaches compromised PII, and the number of insider incidents is rising. Firms are adopting compliance-focused technology: 49% of businesses have recently purchased privacy management software to comply with data protection regulatory requirements[3].

147m

customers PII was exposed

Equifax

This 2017 data breach exposed the PII of 147 million people. The global settlement has risen to $425 million. Claims may be filed until 2024, and Equifax is offering free credit reports until 2026[4].

1. "The Future Of Data Security And Privacy: Growth And Competitive Differentiation," Forrester, January 19, 2021
2. "2020 Cost of a Data Breach Report," IBM
3. "The State Of Data Security And Privacy, 2021," Forrester, April 6, 2021
4. "Equifax Data Breach Settlement," Federal Trade Commission, January 2020

PII

used for synthetic identity fraud, and/or extortion

Accenture

Cybercriminals rapidly monetize stolen PII for synthetic identity fraud, and/or threaten to release PII as part of an extortion campaign. The remote nature of the pandemic workforce has made PII theft easier[5].

70%

say their PII is less secure over time

Pew Research Center

According to surveys, 70% of Americans say their PII is less secure over time, 81% say the risks of PII collection outweigh its benefits, 81% say they have little to no control over PII collection, and 75% say there should be more government regulation[6].

Current Approach: Is Failing

When it comes to PII, according to the National Institute of Standards and Technology (NIST), "If you collect it, you must protect it." PII data breaches are defined as inappropriate disclosures, whether lost, stolen, or compromised, and whether the breach was intentional or accidental. PII should never be kept any longer than needed[7].

There are so many facets to information security, however, that it is difficult to get them all right. At a minimum, you must properly manage firewalls, endpoint protection, access control, encryption, audit history, network monitoring, incident response, multi-factor authentication (MFA), and the principle of least privilege[8].

And even when information security is tight, your network could mistakenly expose a decryption key, an employee might fall for a social-engineering trick, or a trusted insider could simply walk out the door with your crown jewels.

New Approach: Zero Data

Given the increase in PII data theft, a new approach to information security has emerged: Zero Data. Zero Data allows your company to gather, store, and operate on sensitive information without being responsible for its security or liability. Sensitive data such as PII is converted to synthetic data, which if lost or stolen is meaningless to data thieves and hackers. With Zero Data, your company never even has to see the original PII, unless you specifically ask for it.

The Zero Data approach is very much in spirit with one of the hottest trends in information security: zero trust. This new paradigm is data-centric, in which the focus has shifted away from network perimeter security to application and data security[9]. Depending on information sensitivity, Zero Data strategies often involve de-identification, pseudonymization, or anonymization. Tactics include differential privacy (adding "noise" to data), synthetic data (swapping artificial data for the original), and tokenization (replacing data with nonsensitive symbols).

5. "2020 Cyber Threatscape Report," Accenture, October 19, 2020
6. "Americans and Privacy," Pew Research Center, November 15, 2019
7. "Privacy 101: Awareness and Best Practices," National Institute of Standards and Technology (NIST)
8. "2020 Cyber Threatscape Report," Accenture, October 19, 2020
9. "The Future Of Data Security And Privacy: Growth And Competitive Differentiation," Forrester, January 19, 2021

Zero Data Benefits

The Zero Data approach to information security offers many benefits, because PII is never captured, stored, or shared. Your developers do not have to become security or compliance experts. You retain control of your data. You achieve the same business outcomes, without the risk or liability of securing sensitive information.

Here are some of the primary benefits:

- Reduce compliance scope
- Reduce business risk
- Retain data value
- Transfer liability to a security partner
- Save money
- Go to market faster
- Operate on synthetic data just like original data
- Simplify application development
- Simplify compliance audits
- Avoid legal trouble
- Avoid a PR disaster

VGS Case Study: Gem

Gem

Gem offers companies an easy way to connect cryptocurrency to their applications. However, because hackers love to target sensitive financial and PII data, Gem wanted to add an extra layer of security. Gem partnered with VGS to create a proxy layer on top of their in-house security system, and created a defense-in-depth infrastructure to help keep its customers safe. Now, when data is entered into the Gem widget, it flows through VGS first, where sensitive information is redacted and replaced with an alias (an advanced form of token).

VGS successfully partnered with Gem despite a complex environment that encompasses various payment methods, more than 2000 cryptocurrencies, and over 20 exchanges in different legal jurisdictions.

Micah Winkelspecht
CEO & Founder
Gem

“We work in an industry that is a super-target,” and “I want to make sure we're doing everything we possibly can to secure our customers’ data.” Having VGS as a dedicated security proxy provides an “extra layer of protection I needed to actually sleep at night.”

Full Case Study >

Stay Ahead of the Game

One of the most important benefits of adopting a Zero Data strategy is that it is far easier for your company to keep up-to-date with a rapidly evolving regulatory environment. The US Federal Data Privacy Framework began with the Privacy Act of 1974, but shows no sign of slowing down. Here at VGS, we have recently written about Virginia's new data privacy law and Brazil's version of GDPR.

The risk of storing and securing PII is more significant than other types of sensitive data, because there are clear ramifications for physical security, human rights, political freedom, and personal reputation. Therefore, companies are required to protect PII from unauthorized use, access, modification, disclosure, and sharing. On paper, PII should be stored in locked cabinets, transported only to authorized locations, and destroyed with cross-cut shredding. In electronic format, it should be encrypted at rest, encrypted in transit, and available only to authorized users.

Conclusion

Businesses need to leverage their customers' PII for normal business operations. Internet users must provide their PII in order to obtain goods and services. However, most businesses are simply not equipped to store and secure PII, because there are too many security threats and vulnerabilities. Sensitive data breaches are common and have ruined many businesses.

The good news is that your company does not need to collect or retain PII in order to leverage its benefits. With a Zero Data approach to information security, you can still have the benefits of PII without being responsible for its costs and risks. In 2021, data security and privacy are hallmarks of a mature company, and they offer a distinguishing competitive advantage.

VGS is the pioneer of Zero Data. Partner with us to dramatically improve your scope of compliance. To learn more, please visit www.verygoodsecurity.com.

10. "Privacy 101: Awareness and Best Practices," National Institute of Standards and Technology (NIST)

VERY GOOD SECURITY

207 Powell Street, Suite 200
San Francisco, CA 94102

contact@verygoodsecurity.com
verygoodsecurity.com

About Us

Very Good Security (VGS) enables organizations to focus on their core business by offloading their data security and compliance burden to VGS. VGS customers unlock the value of sensitive data without the cost and liability of securing it themselves, and accelerate compliance with PCI, SOC 2, HIPAA, GDPR, and more.