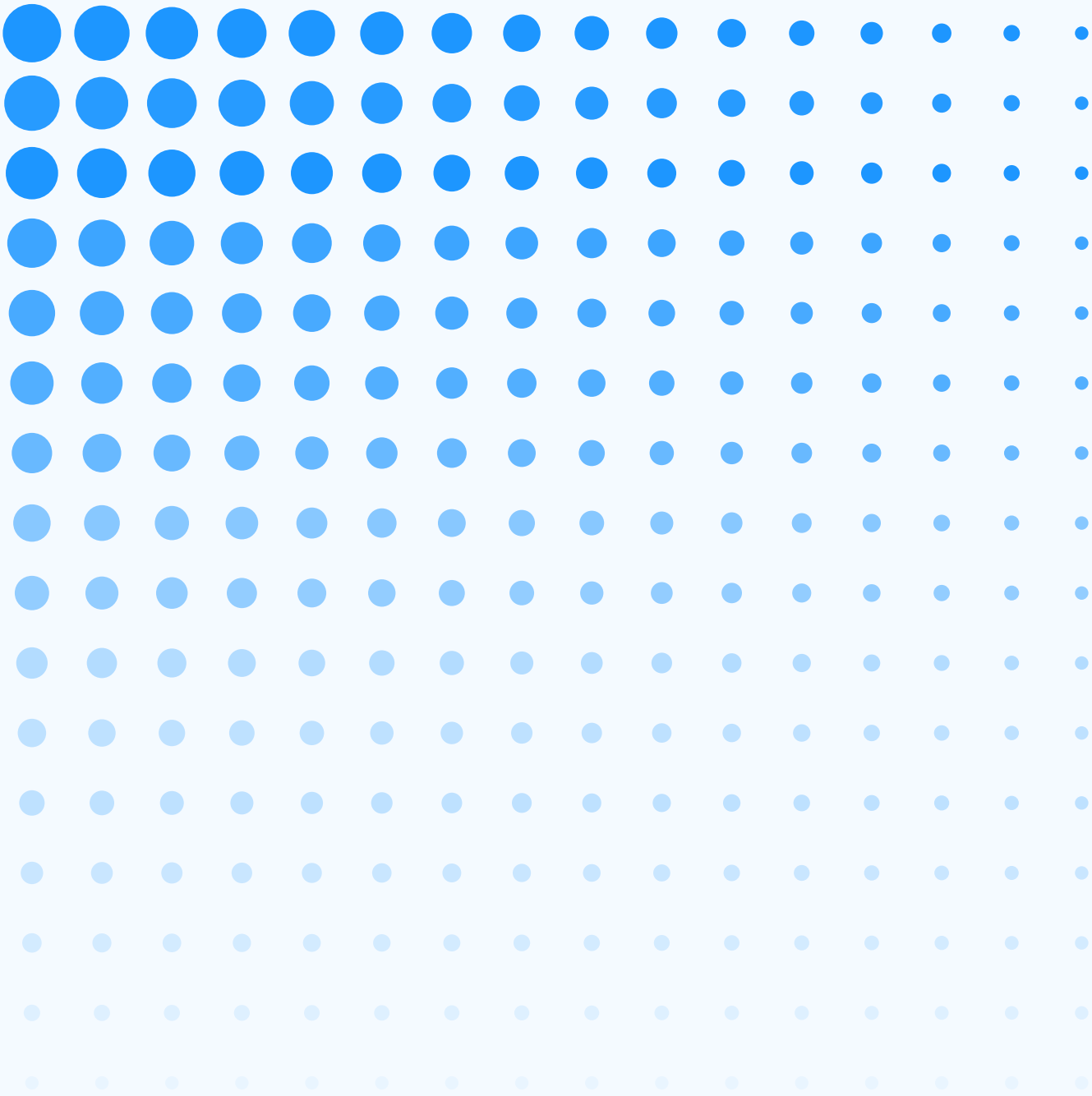
Data Security Solutions 101



integrate.io

Table Of Contents

01

INTRODUCTION

Cybercrime is becoming increasingly common.

According to one source, nearly 70 percent of CEOs believe their cybersecurity risks are increasing by the year. Over 60 percent of all successful breaches result from internal sources. This means that your greatest risk comes from within your own company or enterprise and within your own data management strategy. Are you taking all the necessary measures to protect your data and your clients' data? This white paper will tell you what you need to know about data security: what it is, why it is so important, top data security risks, methods for securing data and software solutions for ensuring data security.

02

DEFINING DATA SECURITY

A data breach or leak results from unauthorized access to data.

It is when information, often personal, ends up in the wrong hands. This usually occurs with disastrous results. The data is now compromised. It loses all value for your organization, but worse still, it can become an ongoing problem. A good example is the loss of passwords or encryption keys. Unless you immediately change all passwords and keys, this will affect future data transfers as well.

Data security is preventing this from happening. Companies have strategies in place to protect data from any unauthorized use. Data security involves many aspects, like preventative measures, identifying potential risks, monitoring performance to detect breaches and providing patches or updates to solve potential leaks. Unfortunately, almost 80 percent of companies lack a system for Cyber Security Incident Response (CSIR), and those companies that do respond often do so too late, no matter how serious the breach may be.

Many companies allow their employees total access to data instead of limiting access to necessary data. Those that limit access are considerably less likely to suffer a breach. Unfortunately, most enterprises simply do not have the right mindset for securing data.

03

WHY IS DATA SECURITY SO IMPORTANT?

A data breach means someone from the outside gets into your data.

A data leak means someone on the inside accidentally or deliberately makes confidential information available to unauthorized users. With fewer than half of companies fully committed to on-premise work for their employees, more and more data stays in the cloud, where it is vulnerable to attack. Also, more data is directly available for insiders to compromise. Your enterprise must take special care to prevent breaches or leaks. But why exactly is data security so essential?

1 COMPLIANCE

There are many standards that different industries have to comply with.

- HIPAA. Health Insurance Portability and Accountability Act. HIPAA is definitely the most well-known data security standard in the health insurance industry. It defines what protected health information (PHI) consists of, as well as how you must secure it and how companies must respond to a data breach that leaks any of this protected data.

- SOC 2. Service Organization Control. SOC 2 addresses third-party service providers and how they may access, store and use business and client data. In particular, it relates to data stored in the cloud.

- GDPR. General Data Protection Regulation. This standard is the product of the EU's decision to enhance data security through a regulation that targets any and all data belonging to or regarding anyone in the European Union. There are heavy fines in place to ensure compliance. The

standard is relatively specific and detailed, meaning it requires considerable effort for companies to comply adequately.

- PCI DSS. Payment Card Industry Data Security Standard. This standard controls how companies can process and store payment card information. There are different 'levels' depending on the number of transactions processed per year.

- CCPA. The California Consumer Privacy Act. This policy empowers consumers with higher levels of control over the information enterprises collect about them. It is the foundation for many privacy policies. Privacy policies operate on the principle that companies have to let consumers know what data is actually being collected about them, as well as how the business is going to use this information. CCPA also protects consumers' right to opt-out of data collection or sale as well as to delete the collected data under certain circumstances. If your company is not in California, you might think that this does not apply to you, but you would probably be wrong. If your website collects data from anyone in California, you also have to comply with the CCPA.

Lack of compliance with any of these standards can result in high fines, lawsuits and even criminal charges, especially with HIPAA. Integrate.io is compliant with HIPAA, SOC 2, GDPR and CCPA, enabling businesses to better ensure data security compliance throughout the ETL process.

2 COST MODEL

HIPAA violations alone can cost up to $1.5 million per year or $50,000 per record. GDPR violations can be up to €20 million. Those are just two examples. Companies may have to pay money to various governments, businesses or individuals as compensation for the consequences of leaking data.

Another aspect of the heavy cost of a breach comes from ransomware. Ransomware is a type of malware that targets data or systems and renders them inaccessible or unusable until a company or government entity pays a certain amount of money. While enterprises do not always publicly report ransomware payments, some have been up to tens of millions of dollars.

3 CLIENT TRUST

According to one terrifying statistic, as few as 30 percent of consumers may continue trusting your institution with their data after a breach. That means you risk losing 70 percent of your business to a data breach. Clientele grows when trust grows, and a data breach shatters it. These costs are sobering at the very least. What are some risks facing you that may result in one or all of these costs?

04

DATA SECURITY RISKS

There are many and varied cybersecurity risks facing enterprises now and in the future.

1 ACCIDENTAL LEAK

Over 90 percent of breaches are in some way a result of human error. Hackers take advantage of it all the time. While there are many ways that you may leak data accidentally, unsecured networks are notable. Any time your employees use public Wi-Fi to access your company's data or even sign in to an account, they risk a leak. An astonishing 60 percent of people believe there is no risk in using public Wi-Fi. One of the best things you can do is to educate them about the possibility of encountering malware or exposing sensitive data.

System errors are a much less prevalent cause of an accidental leak, but they do happen. That is why it is essential to ensure that your ETL (extract, transform and load) or BI (Business Intelligence) software has all the security measures and redundancy necessary to prevent such a leak.

2 PHISHING

Phishing is a more specific form of an accidental leak due to human error, and it usually occurs through email. On certain occasions, it may also happen through a phony website, online form or even a spam phone call. A small percentage of spam emails are actually phishing attacks. According to some sources, over 80 percent of companies face phishing scams in a year. Phishing scams always 'fish' for personal or confidential information under some guise. It is important to equip employees to recognize and respond appropriately, especially since it may not only be their data that is at risk. Password leakage can cause a serious breach.

3 INSIDER THREAT

An insider threat does not have to be deliberate. It can also be negligent. The distinction is that it comes purely from inside your business instead of from the outside. A relatively small percentage of breaches are completely the result of malicious intent on the part of someone inside your company.

4 MALWARE

Malware, a contraction of 'malicious software', is an unfortunately well-known threat. Just a few types of malware:

- Virus. A virus is a self-copying computer program that injures processes or systems, preventing them from working properly to, for example, protect data.
- Spyware. Spyware is specific to stealing data. It is a program that, far from interrupting normal processes, simply watches them. One form of spyware logs keystrokes to steal passwords and other sensitive information.
- Ransomware. As already mentioned, ransomware is a type of malware that takes data or parts of a system 'hostage' until the victim pays.

Any of these types of malware can come because of clicking on bad links in emails or on untrustworthy websites. They can also come through the use of unsecured Wi-Fi. These are only a few of the risks facing businesses today. Any time you transfer data, there is risk. The longer moving the data takes, the more danger there is of suffering a leak or breach. Integrate.io offers native support for a variety of common sources and destinations to enable secure and fast data transformation.

Thankfully, there are many other methods you can use as well to identify potential risks and prevent a data breach before it starts.

05

METHODS FOR IDENTIFYING DATA SECURITY RISKS

Security testing is a way to determine whether software or systems are secure.

Companies have many methods of ensuring this. They do not limit tests to the beginning of the software lifecycle prior to the release of a new product. Identifying risks is part of beta testing, and developers may continue it throughout the life of the product for the best safety.

One of the main standards for cybersecurity testing today is the WSTG (Web Security Testing Guide). The WSTG comes from OWASP, the Offensive Web Testing Framework. The OWASP Foundation is a nonprofit that provides guides and the Web Testing Environment (WTE). WTE consists of a variety of application security and security testing documentation and other resources. The WSTG is an excellent starting place. A few of the tests used to fulfill the principles laid out by OWASP are security and vulnerability scanning, penetration testing/ ethical hacking, risk assessment and security auditing.

1 VULNERABILITY AND SECURITY SCANNING

Vulnerability scanning targets potential problems in applications through the use of specialized, automated software. These scans can detect various types of vulnerabilities like any susceptibility to injection attacks or faulty configurations. Since injection attacks are in the OWASP Top 10 Security Risks, vulnerability scanning is absolutely necessary to ensure application security.

Security scanning can target applications, APIs and networks and may consist of scans that are automated or manual. You can then analyze potential threats more deeply and provide solutions.

2 PENETRATION TESTING/ETHICAL HACKING

This form of testing checks how applications or systems respond to an attack. It asks, is penetration possible? How could it happen? What systems are vulnerable, and how do you counter an attack? Penetration testing is a form of manual security testing, so it requires the help of what is commonly called a 'white hat hacker', also known as an ethical hacker. Ethical hackers only perform according to the law and work to assist rather than victimize enterprises.

3 RISK ASSESSMENT

An in-house team or a third-party expert may perform risk assessment in order to prioritize security budgeting to the most critical systems or assets as well as identify the greatest risks facing the enterprise.

4 SECURITY AUDITING

Security auditing reviews industry standards for cybersecurity, ensuring the software or system implements them correctly. It is a thorough and focused review of flaws, potential vulnerabilities and compliance.

Once you have performed a risk assessment and security audit, how can you best ensure the security of your data and solve potential problems before they become serious liabilities?

06

METHODS FOR SECURING DATA

Just a few of the top methods for DLP (Data Loss Prevention) include encryption, PII masking and IAM. Integrate.io provides each of these throughout your ETL process.

1 ENCRYPTION

There are various types of encryption, but all boil down to the same basic concept. Encryption is a cipher that encodes your information. Users cannot read it without a decryption key. Integrate.io offers Field-Level Encryption (FLE). FLE allows you to encrypt individual fields on the client's side before it even reaches the server.

Another type of encryption you are probably familiar with is SSL (Secure Socket Layer)/ TSL (Transport Layer Security) encryption and HTTPS (HyperText Transfer Protocol Secure). SSL and TSL are methods of encrypting and therefore securing internet connections. These protocols encrypt data in transit, ensuring that no unauthorized users access it between the sender and destination. HTTPS in a URL lets you know that one of these protocols is securing the website.

Two primary categories for any encryption method are symmetrical and asymmetrical encryption. Symmetrical encryption just means that the sender's encryption key is the same as the receiver's decryption key. In asymmetrical encryption, you require a key pair: one for the sender/owner of the data for encryption, called a private key, and an entirely different key for decryption. You can give the decryption key, called the public key, either to a select group of users or to the public at large.

2 PII MASKING

Integrate.io allows you to perform PII (Personally Identifiable Information) Masking. PII masking, also known as pseudonymization, is a method to conceal, replace or entirely remove anything in a dataset that makes the data identifiable to a particular person. This can be essential for compliance, especially in the healthcare industry or with certain types of surveys and studies.

PII could be an email address or an SSN, among many other things. The compliance policies mentioned above have very specific directions for protecting PII. The two main types of PII masking are static masking and dynamic masking. Static masking first replicates the database, then masks the data. Dynamic masking conceals the data on the fly so that any user accessing the database to prevent unauthorized users from seeing the PII.

3 IDENTITY AND ACCESS MANAGEMENT (IAM)

The Gartner glossary calls IAM "the discipline that enables the right individuals to access the right resources at the right times for the right reasons." Yet again, there are different methods that make this possible.

- Passwords and password management. Virtually any account you will create on the internet requires a password, so this is not an unfamiliar concept. However, companies have had to become much wiser with password management. Accounts can require a password of a specific length or passwords with a number or special character or both. This article shows some potential threats to passwords, as well as how to make them more secure. Any database where you store passwords has to be especially secure.

- Multi-factor/two-step authentication. Google is probably the most famous proponent of two-step verification, also known as two-factor authentication. Many other big companies are now following the trend, and for good reason. It prevents up to 99 percent of

automated attacks. Basically, it combines a PIN or password with another point of authentication. The second factor may be biometric or simply a code sent to your cellphone or email. Unfortunately, as of late 2019, only a little over a quarter of companies have implemented two-step authentication.

- OAuth (Open Authorization). Integrate.io allows you to implement OAuth with ease. This feature generates a security token that is delegated to users to whom you want to give access. It is separate from a password, so you can generate an authorization token without exposing any password information. OAuth is for authenticating API calls and is a feature of Integrate.io's REST API connector.

- SAML (Security Assertion Markup Language). Another common authentication standard is SAML, the open standard that provides the foundation for SSO (Single Sign-on). The most familiar form of SSO is probably your Google account. You can use one login to access many sites and services through the information you only share with one service provider, in that case, Google.

07

DATA SECURITY SOFTWARE SOLUTIONS

Some types of software solutions you may be interested in using to improve data security in your enterprise include Security Risk Assessment tools (SRA), high-level encryption software, EPP (Endpoint Protection), EDR (Endpoint Detection and Response), DLP (Data Loss Prevention), IDS (Intrusion Detection Systems), user management software and firewall software.

Security Risk Assessment

HIPAA actually requires certain businesses to perform risk assessments to determine potential vulnerabilities and risks to sensitive data. An SRA tool conducts automated risk assessment. Some open-source tools are available for this purpose. These solutions generate reports you can then study to decide how to prioritize security and systems as well as check compliance with different data security standards.

High-Level Encryption

While many ETL or data storage solutions provide encryption options, you can also find dedicated software to strengthen security further. These tools can provide public and private encryption keys for asymmetrical encryption or generate authorization tokens. You can use some solutions to encrypt particular files or folders before sharing. Integrate.io performs field-level encryption to help you keep information even safer.

EPP (Endpoint Protection)

Endpoint security software protects personal computers, servers and more. A good example is a typical anti-malware software on an employee's PC. However, many companies have to go much deeper and ensure that they have secured every individual endpoint. Any failure to do so is a data breach waiting to happen. Some software specifically protects or monitors mobile devices. This is especially important since as many as half of all organizations report having an employee who fell victim to mobile malware.

EDR (Endpoint Detection and Response)

EDR is a more focused version of EPP. It can detect even the most advanced vulnerabilities and threats, or even just irregular behavior/activity. This type of software gives you regular updates and presents analytics in a way that helps you properly identify all threats.

Data Loss Prevention

DLP software sorts data into classifications based on various factors like importance, whether it contains PII and how compliance policies regulate it. It then protects the data based on the classification. DLP performs many functions. For example, it can alert users to warn them against sharing some data. It can also function as EDR or EPP software, monitor activity, provide reports and encrypt data.

IDS (Intrusion Detection Systems)

IDS are primarily for incidence response. They monitor events, logs and activity of any kind in order to flag suspicious or dangerous violations and processes. They can detect hacking attempts or malware activity and alert you about them. These systems often require a very skilled person to configure and to analyze results.

User Management

Sometimes, IAM is as easy as installing software you can use to create and configure user accounts. You can manage permissions for users at different levels and roles (Role-based Access Control/RBAC). For example, you might have one level of access for admins, another for IT, etc. In this way, you can ensure that users only have access to the data they need to complete their job, significantly reducing the risk of leaking data.

Firewalls

A firewall blocks unauthorized users and filters traffic on a network level. It can flag suspicious or dangerous activity. Different solutions may have different levels of security or customizability, but each should allow you to choose what kind of traffic you want the software to block automatically or allow. There are open-source options for this as well, but open-source solutions can come with their own set of security risks and should be chosen carefully.

Software is not the whole solution, but it is a big part of it. What should you look for in ETL software to ensure the safety of your data?

08

INTEGRATE.IO ETL AND DATA SECURITY

Integrate.io provides many of the features mentioned above. You can protect PII with the PII masking feature. Additionally, Integrate.io partners with Amazon's KMS (Key Management Service) to provide FLE. You can expect SSL and TSL encryption as well. Integrate.io is GDPR, HIPAA, CCPA and SOC 2 compliant and helps you avoid fines and violations. The platform even provides two-factor authentication.

Members of the Integrate.io security team are CISSP (Certified Information Systems Security Professional) and cybersecurity-certified. Integrate.io also ensures your data is secure with regular penetration testing through a third-party security firm.

Finally, using Integrate.io ETL you can build data pipelines in minutes with no coding experience and limit the amount of time your data spend exposed.

Hopefully, this has given you a deeper understanding of and the ability for protecting data from leaks and breaches. Ensuring adequate data security becomes more important every day, and you can equip your enterprise to do just that.