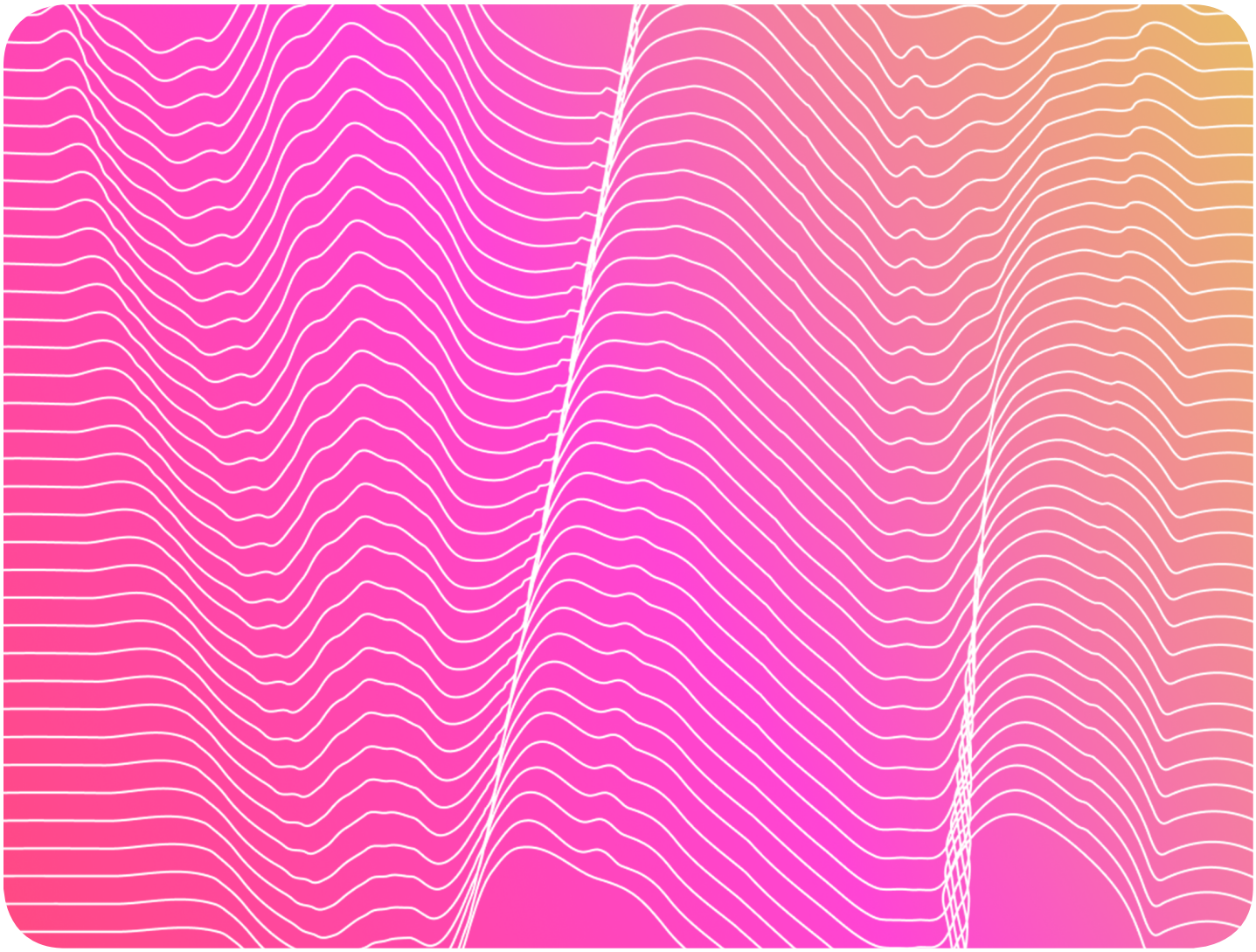
auth0 by Okta

Secured and Assured

Unit 3: Data Protection in-Use, in-Transit, and at-Rest

Author:
Anne Ellegood

Contributors:
Andrea Chiarelli & Annybell Villarroel



Contents

Introduction

Secured and Assured is an e-learning series of posts and downloads about the technology and tools securing and protecting important data and digital properties across an organization.

Secured and Assured Unit 3:

Data Protection in-Use, in-Transit, and at-Rest

People place a lot of trust in the organizations they choose to have a business relationship with. That trust can be shaken, if not irreparably damaged, with just one data breach. The aftermath for the entity (or entities) entrusted with their data where it was compromised can be felt for months, if not years.

Safeguarding data is the responsibility of everyone within the organization, not a select few, IT only, or just one vendor. And while the suggested best practices, systems, and component tools covered in Unit 2 can serve as a catalyst for protection, they should not be relied on alone.

To protect your organization's data, let's start by getting to know the 3 types of states your data can be in, where it resides in that state, and some best practices for protecting that data. Along with the best practices, (and where applicable) we've listed some tools used that can help support a business with its data protection needs.

The 3 States of Data:

Data Type #1 – Data in-Transit

What Data in-Transit is:
Data traveling from one point to another via the web, email, public or private communications channels, cloud-based software applications, file downloads and uploads, file sync apps, et al., is data in-transit. It is the digital processes we cannot see occurring rapidly between two endpoints. This type of data poses challenges for protection due to:

1) An almost infinite number of methods in which data can be transferred
2) The many regulations for data protection and control compliance needed

However, there are measures which can be taken to protect in-transit data. For example, the use of SSL/TSL (Secure Socket Layer/ Transport Security Layer), a process for establishing secure links between networked computers provides an endpoint encryption system to prevent unauthorized access.

Best Practices for Protecting Data in-Transit

- Current and clearly defined data access policy

  A strong data access policy is current, clearly defined, and establishes the types of data classifications users have access to, classification criteria, and levels of access. In addition, the policy should also provide information on the repercussions for any violations. As the average business handles millions of digital interactions a day by both humans and machines, the policy should reflect the breadth of users the organization exchanges data with. Individual contributors and leaders alike should know the access policies that impact them and the organization.

- Limited and actively monitored access

  Who has access for full-ownership of data? Who can access and modify or delete data? Access permissions and levels based on role, relationship, attribute, or a discretionary basis should be set and reviewed regularly with the designated responsible resource(s). Offering users the least amount of access needed to provide their intended purpose with the data will also help to protect data from unauthorized access.

- Up-to-date data transmission systems

  Most of the systems used today to transmit data require some form of hardware, software, or other systems and processes to function. These critical assets should be proactively updated. Doing so will help ensure that the transmission of data is both efficient and isn't subject to vulnerability risks stemming from out-of-date, or previously compromised and known-risk assets.

Tools Used to Protect Data in-Transit: Encryption & Tokenization

Encryption

Encryption prevents data from being manipulated or read between the source and its destination and can be implemented a number of ways, depending on the use case. To decrypt or decipher the data, a "key" is required.

There are 2 families of key-based encryption:

1. Asymmetric - Asymmetric Encryption uses two different keys to encrypt and decrypt (or decode) data. One key is a public key that *encrypts* the data which anyone can access. The second key is a private key that *decrypts* the data. Only an authenticated recipient has access to a private key. These two keys are separate, but equal– both are needed in order to decode.

2. Symmetric - Symmetric Encryption uses only one key to encrypt and decrypt which must be shared between the two parties desiring to share the encrypted and decrypted data.

Learn more: *Asymmetric Encryption: Definition, Architecture, & Usage* (web page)

Tokenization

Tokenization replaces sensitive data with a randomly generated, non-sensitive, placeholder (a "token") and unlike encryption, it does not provide a way for the data which is linked to the token to be deciphered. This process does not alter the length of the data and requires less storage space.

Learn more: *Tokenization Explained: What is Tokenization and Why Use it?* (web page)

Data Type #2 – Data in-Use

What Data in-Use is:
Just as the term implies, the data's state is in-use. Data in use is being accessed or consumed actively by users and the applications powering this data. The data resides in software applications, databases, the cloud, etc. The process of accessing the data is typically achieved through a login and though in-use data is vulnerable, with the right tools in place, it can be safeguarded.

Best Practices for Protecting Data in-Use

- Clearly define how data is to be used

  By now, we've all encountered a website or app where we were notified and informed how the information we provided at-will was going to be used (purpose). For data to be used, it must first be accessed. Having clear guidelines established for how all forms of data are to be used and for what purpose will help mitigate risk and liability often associated with, "not knowing."

- Actively monitor network and actions

  Most IT infrastructure today have mechanisms in place to detect if data has been compromised. Activity logs and network traffic reports are especially useful for protecting data; serving as means to identify when, where, what was done, and (usually) who was involved. These actions can report and provide notification of suspicious activity before it becomes a deeper security problem. Depending on the types of data an organization works with, audit reporting may need to be provided for compliance.

- Train and keep training

  Conducting or participating in regular training and making ongoing training as new systems, policies, procedures, and tech is introduced should be mandatory and cover foundational and advanced data protection measures. As inventor Ben Franklin once said, “An ounce of prevention is worth a pound of cure.”

Data Type #3 – Data at-Rest

What Data at Rest is:
Data in this state is not being accessed and is being stored. At rest, data can be scattered across a variety of media and equipment (on-site or off-site.) Like data in-transit, data at-rest is also subject to the same stringent data regulations regarding control and protection compliance.

Best Practices for Protecting Data at-Rest

- Know the answers to the what and where for your data

  Data comes in many different forms and classifications. If your organization hasn’t already, it’s time to figure out what data you have by type and classification, and where it resides.

- Take steps to safeguard data physically

  Something as simple as locking down your workstation or devices when not in use can go miles for helping to protect data and prevent unauthorized access. Additionally, login information for workstations and devices should never be shared.

Learn More: Cybersecurity Checklist: Workplace Edition & Cybersecurity Checklist: Home Edition (Checklists)

- Let go and destroy data

  Data hoarding can be a real problem. In addition to taking up storage space, data may contain sensitive information that could put your organization at risk. Just like you would wipe a personal computer or mobile devices which are no longer in use, letting go of and properly destroying data can free up room and aid in

meeting security and compliance requirements. As mentioned earlier, not everyone has permission to delete data, nor should they. It's best to work with a trusted IT resource to discuss the proper procedures for removing and destroying data, especially those that come from formalized consumer deletion requests.

- Use endpoint security systems

  Endpoints are the source or destination where your data comes to rest or permit access in order to transmit data, such as a computer. Establishing a security system to protect data not only helps to protect data, but also serves as evidence for adhering to compliance requirements.

Tools Used to Protect Data at-Rest: Encryption & Tokenization*

**see above provided information under Data in Transit*

Unit 3 Review

Go over the Key Takeaways for Unit 3: Data Protection in-Transit, in-Use, and at-Rest. Then, work through and answer the following Review Questions to test your understanding of the materials covered in this unit. Correct answers to the questions can be found beneath the full question list in the answer key.

Key Takeaways

There are 3 states of data:

- Data in-Transit
- Data in-Use
- Data at-Rest

Best practices for protecting data in-transit:

- Current and clearly defined data access policy
- Limited and actively monitored access
- Up-to-date data transmission systems

Best practices for protecting data in-use:

- Clearly define how data is to be used
- Actively monitor network and actions
- Train and keep training

Best practices for protecting data at-rest:

- Know the answers to the what and where for your data
- Take steps to safeguard data physically
- Let go and destroy data
- Use endpoint security systems

Encryption prevents data from being manipulated or read between the source and its destination and can be implemented a number of ways, depending on the use case. To decrypt or decipher the data, a “key” is required. There are two (2) families of key-based encryption: 1) Asymmetric encryption 2) Symmetric encryption

Asymmetric Encryption uses two different keys to encrypt and decrypt (or decode) data. One key is a public key that *encrypts* the data which anyone can access. The second key is a private key that *decrypts* the data. Only an authenticated recipient has access to a private key. These two keys are separate, but equal– both are needed in order to decode.

Symmetric Encryption uses only one key to encrypt and decrypt which must be shared between the two parties desiring to share the encrypted and decrypted data.

Tokenization replaces sensitive data with a randomly generated, non-sensitive, placeholder (a "token") and unlike encryption, it does not provide a way for the data which is linked to the token to be deciphered. This process does not alter the length of the data and requires less storage space.

Unit 3 Review

Work through and answer the following Review Questions to test your understanding of the materials covered in this unit. Correct answers to the questions can be found after the Additional Resources section below.

Review Questions

1. Data traveling from one point to another is called what?

2. Which of the following tools can be used to protect data in-transit?
    a. Encryption
    b. Tokenization
    c. None of the above
    d. Both a. and b.

3. Fill in the blank: _____ replaces sensitive data with a randomly generated, non-sensitive placeholder.

4. True or False – Both Asymmetric and and Symmetric Encryption require keys

5. Name two tools used to protect data in-transit

6. What is the source or destination where data is stored or permit access called?

7. Data being accessed and actively used is called:
    a. Data-in-Transit
    b. Data-in-Process
    c. Data-at-Large
    d. Data-in-Use

8. True or False – Asymmetric Encryption uses 1 key

Additional Resources

- *3 Fundamentals in Data Risk Mitigation for Nonprofit Staff* (Blog post)

Unit 3 Review Answer Key

1. Data in-Transit
2. d. - Both a. and b.
3. Tokenization
4. True
5. Encryption and Tokenization
6. Data-at-Rest
7. Data-in-Use
8. False

Auth0 provides a platform to authenticate, authorize, and secure access for applications, devices, and users. Security and development teams rely on Auth0's simplicity, extensibility, and expertise to make identity work for everyone. Safeguarding more than 4.5 billion login transactions each month, Auth0 secures identities so innovators can innovate, and empowers global enterprises to deliver trusted, superior digital experiences to their customers around the world.

For more information, visit **https://auth0.com** or follow **@auth0** on Twitter.