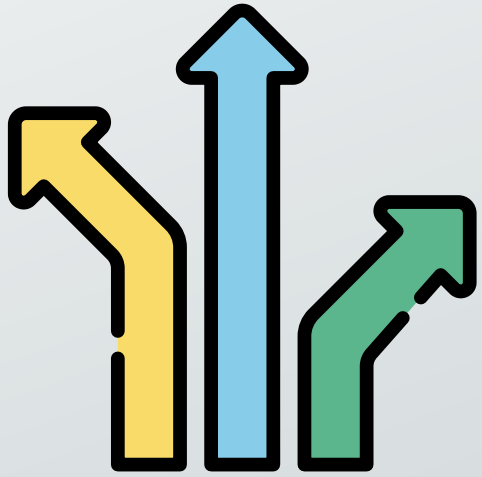
Designing a Zero Trust Architecture

No “Right” Way to Zero Trust

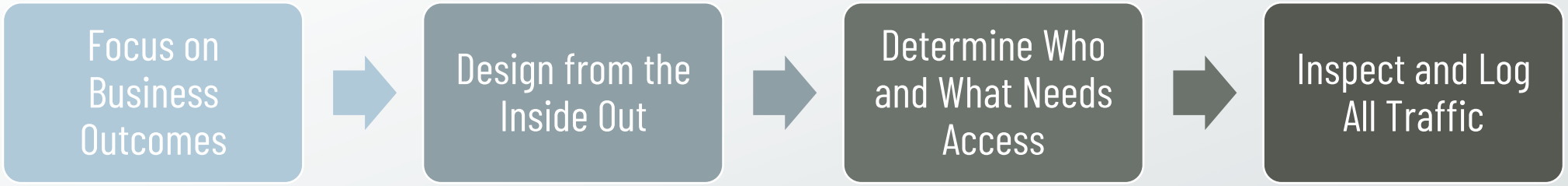
INSTRUCTOR ALTON

- Zero Trust is a strategy and framework where each organization’s journey will be unique.
- No two organizations are the same:
  - ✓ Size
  - ✓ Mission
  - ✓ Budget
  - ✓ Resources
  - ✓ Risk Environment
  - ✓ Regulatory Requirements
  - ✓ IT Architecture
  - ✓ Cyber Security Capabilities

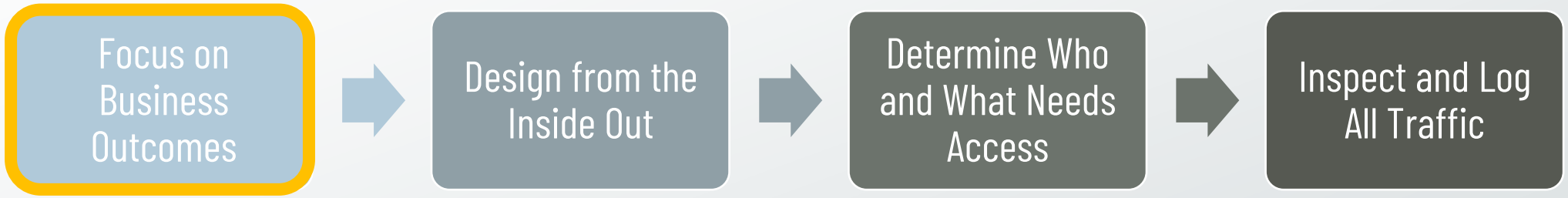


Key Takeaway: You should adopt aspects of Zero Trust that make the most sense for your organization.

Zero Trust Four Design Principles

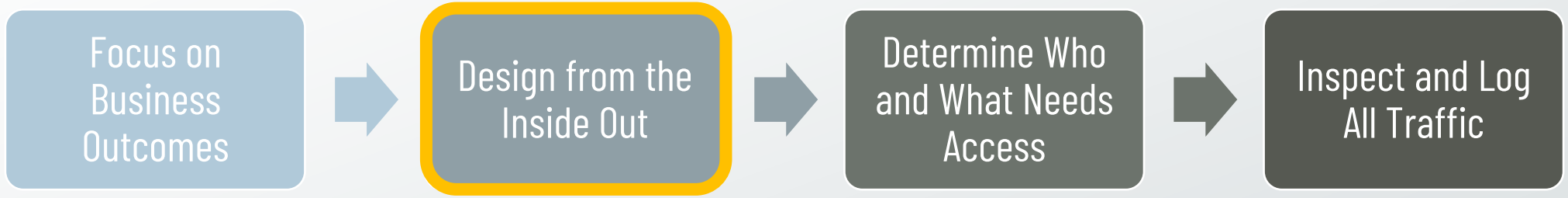


Zero Trust Four Design Principles



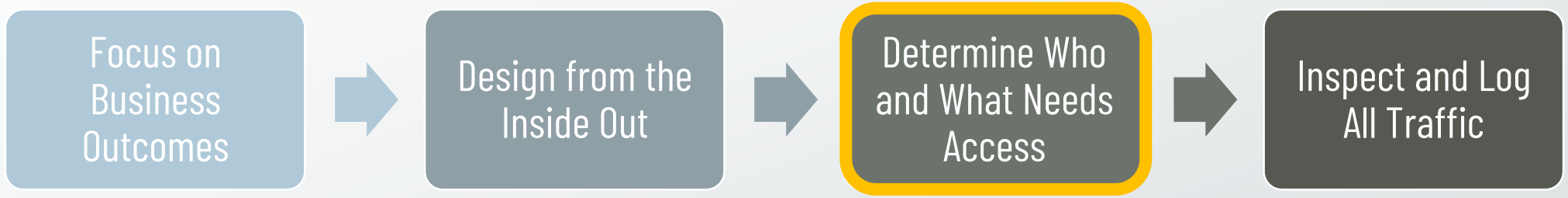
- Align your Zero Trust efforts with the organization's mission, goals, and strategies, where Zero Trust becomes a strategic business asset that differentiates the organization from its competitors.
- The end goal is for Zero Trust to act as a business enabler rather than an inhibitor.

Zero Trust Four Design Principles



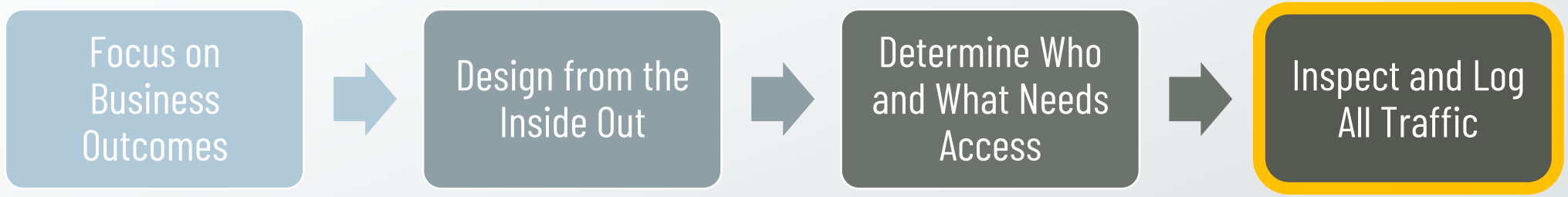
- Focus on protecting your trusted resources: data, assets, applications, and services (DAAS) rather than your entire attack surface.
- Your DAAS are considered your protect surfaces, which are trusted resources and assets that are essential to your organization.

Zero Trust Four Design Principles



- Once you know what your DAAS protect surfaces are, you then need to determine who and what needs access to them.
- The end goal is to apply just-in-time (JIT) and just-enough-access (JEA) to prevent giving too much access to sensitive resources and data.

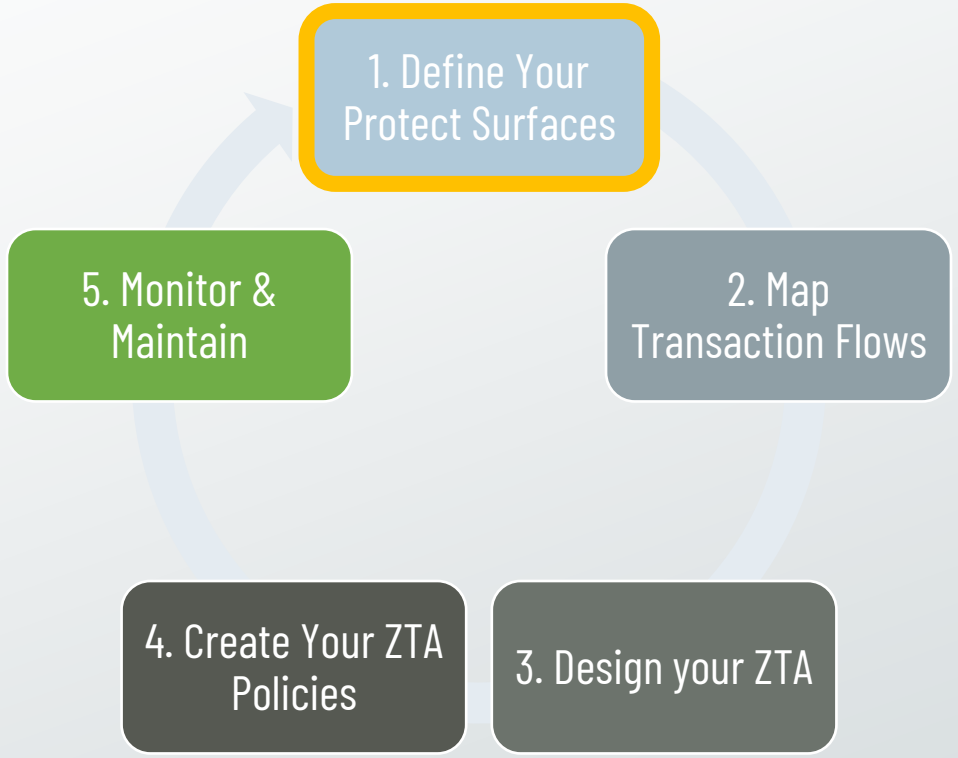
Zero Trust Four Design Principles



- The last principle is to inspect and log all inbound and outbound traffic, scanning for malicious and unauthorized activities.
- This should occur both on-premise and within your cloud environments.

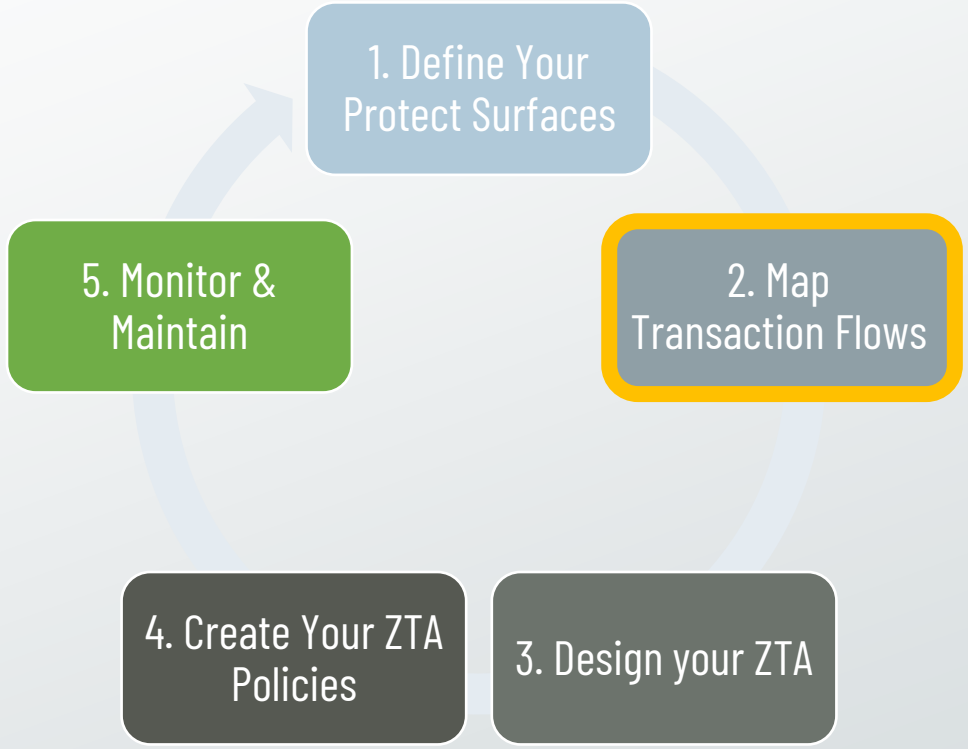
Five-Step Zero Trust Design Methodology

Five-Step Zero Trust Design Methodology



- The first step is to identify your most critical organizational data, assets, applications, and services (DAAS), which are your protect surfaces.
- You should prioritize your Zero Trust efforts based on each protect surface's criticality to the organization.

Five-Step Zero Trust Design Methodology



- The next step is to understand how data and various DAAS components interact with one another by mapping their network traffic transaction flows.

- This allows us to understand how they currently interact (**current state**) to help us design how they should interact in a Zero Trust environment (**target state**).

Five-Step Zero Trust Design Methodology

- Once we've defined our protect surfaces and mapped our transaction flows, we can then begin designing our ZTA.
- There's no singular universal approach to designing a ZTA, as each organization is uniquely different, so expect your Zero Trust journey to be unique to you.

Five-Step Zero Trust Design Methodology

- Once the ZTA is designed, the next step is to create your ZTA policies to determine who or what should have access to your protect surfaces.

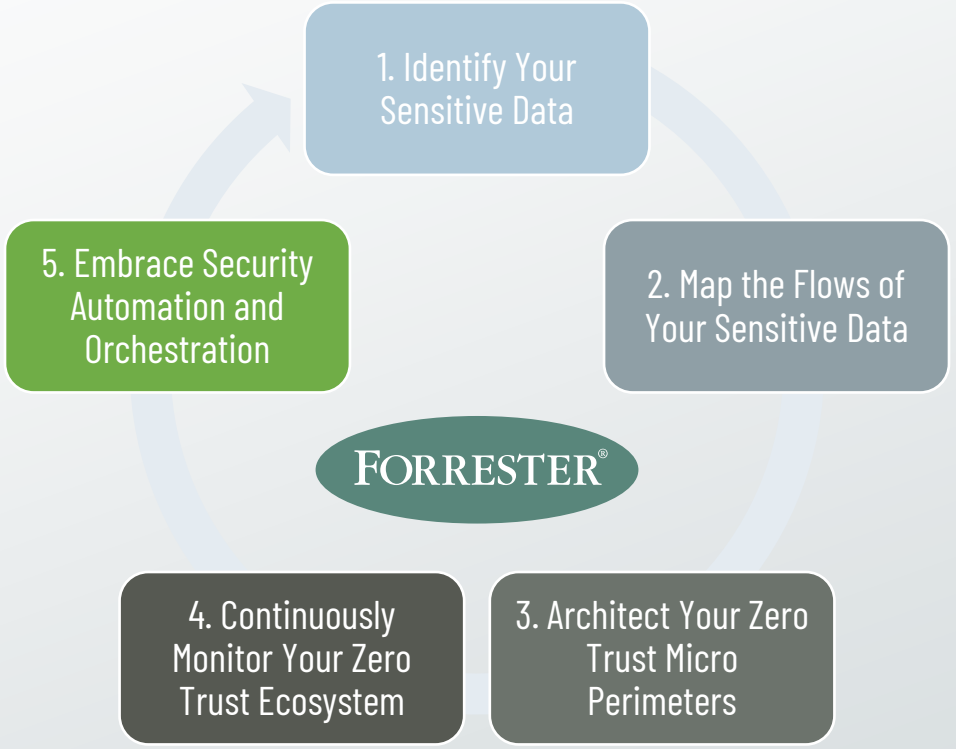
- A good way to begin drafting up ZTA policies is to follow Kipling's method, which covers who, what, when, where, why, and how to design contextual-based policies.

Five-Step Zero Trust Design Methodology

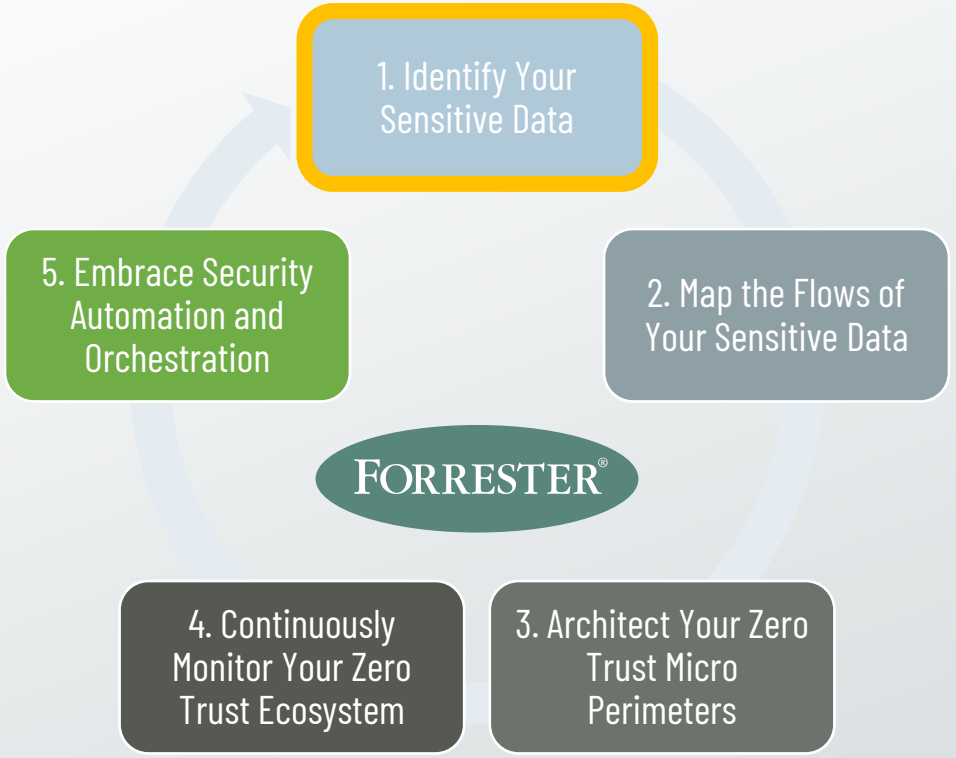
- Once everything is designed and in place, the next step is to monitor and maintain your ZTA to help you fine-tune and improve your ZTA over time.

- Zero Trust is an iterative process, so you should always be looking for ways to make improvements in your ZTA. Zero Trust is adaptive, so your ZTA should be as well.

Forrester's Five Steps to Zero Trust

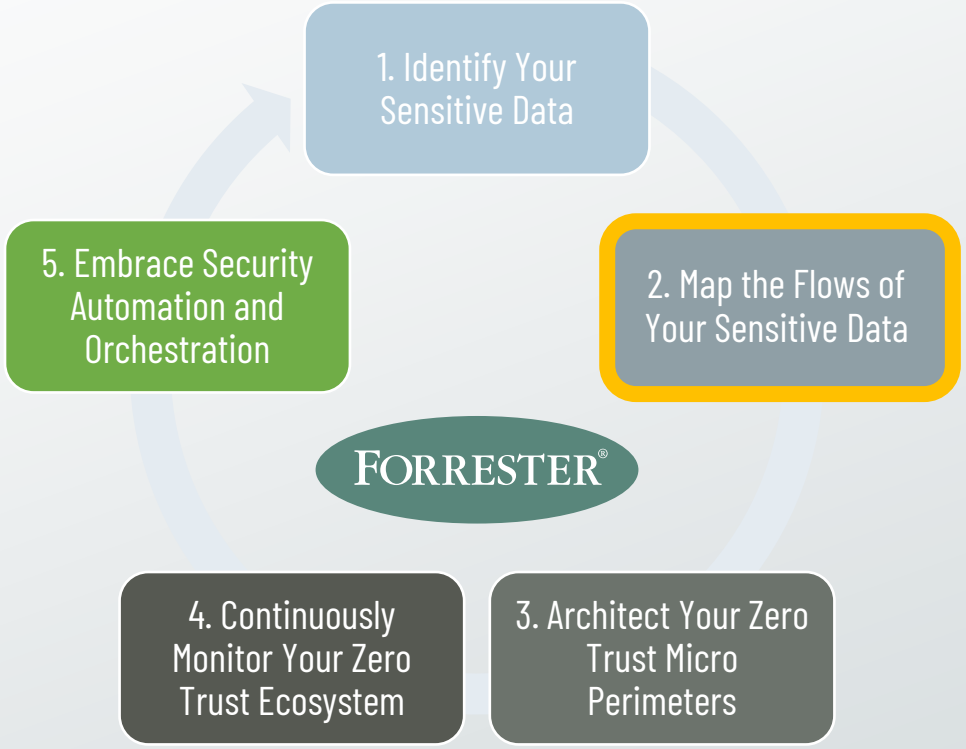


Forrester's Five Steps to Zero Trust



- Forrester recommends beginning your Zero Trust journey by identifying your most valuable data and focusing your efforts on protecting that first.
- This includes data identification, categorization, and classification.

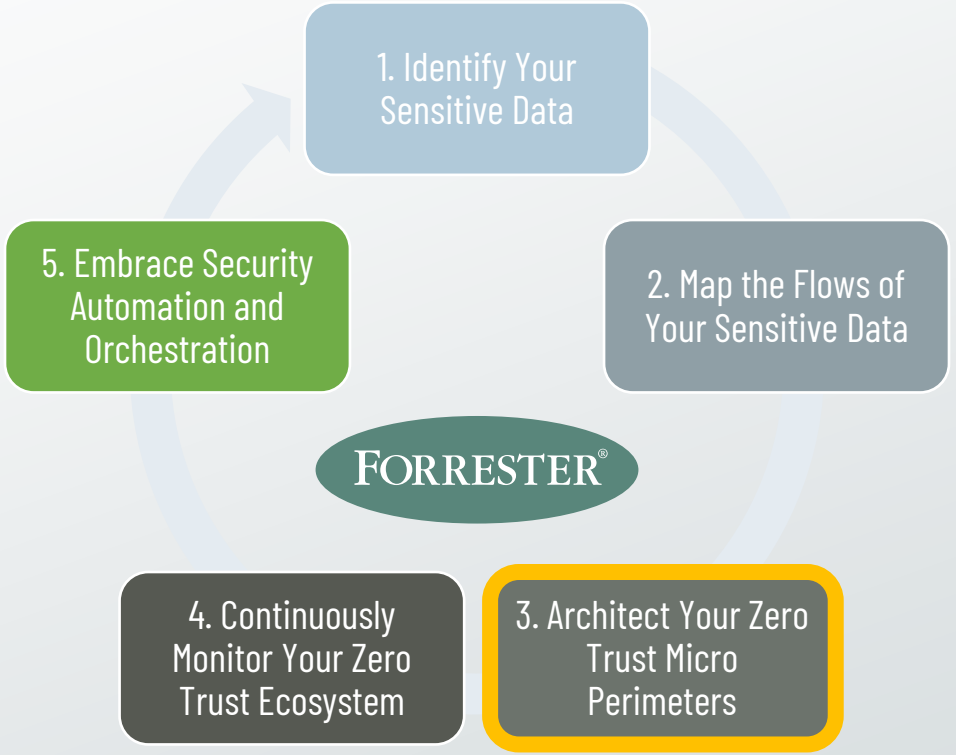
Forrester's Five Steps to Zero Trust



- The next step in Forrester's process is to map your data transaction flows, just like in our Five-Step Zero Trust Design Methodology.

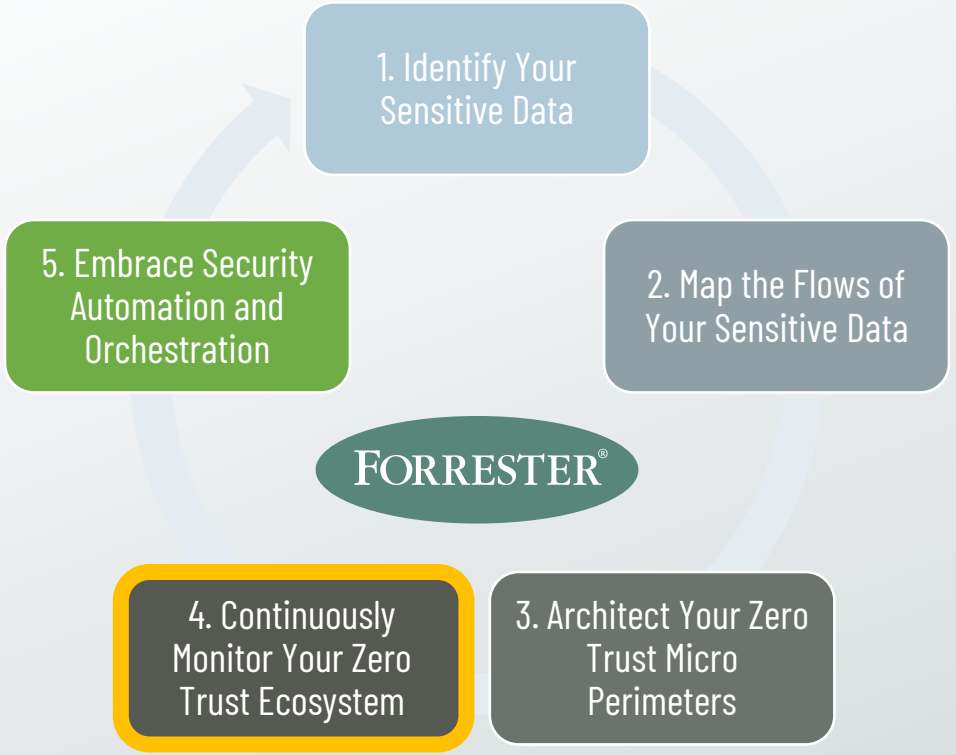
- This allows us to understand where our sensitive data is stored, what applications utilize it, and which users can access it, revealing potential vulnerabilities and inefficient processes.

Forrester's Five Steps to Zero Trust



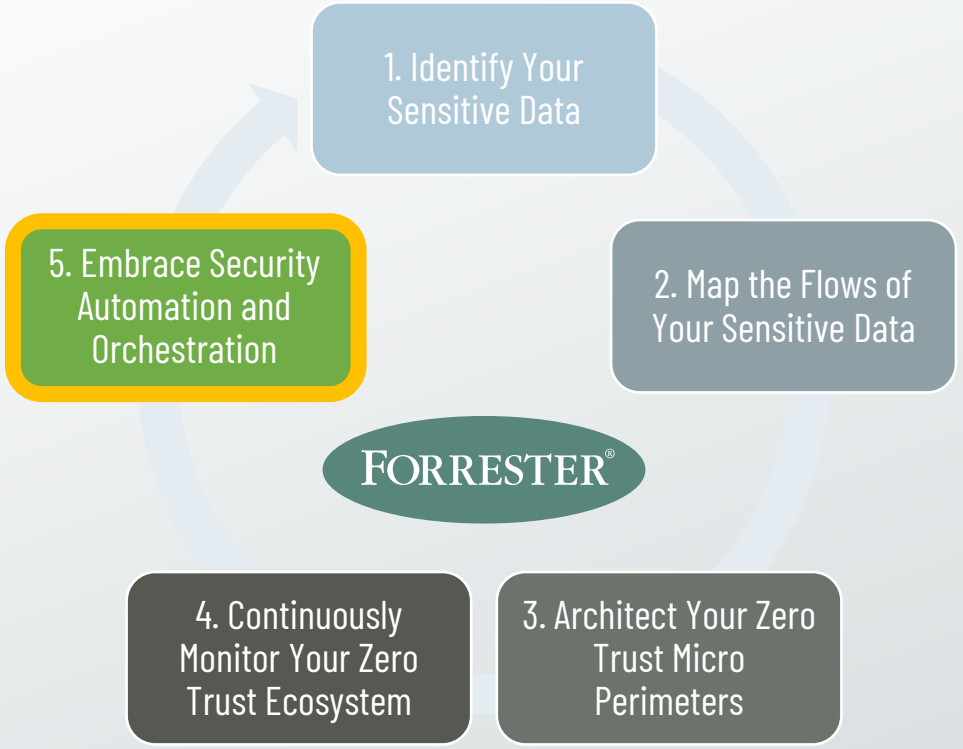
- Forrester is a proponent of Zero Trust micro perimeters, i.e., micro-segmentation as a primary aspect of a ZTA.
- Forrester recommends defining micro perimeters around your sensitive data, utilizing physical or virtual security controls.

Forrester's Five Steps to Zero Trust



- The next step in Forrester's methodology is to continually monitor your ZTA, with a focus on IT asset visibility and security analytics.
- Forrester recommends solutions that enable action rather than just analysis, with an end goal of security automation and orchestration.

Forrester's Five Steps to Zero Trust



- The last step in Forrester's approach is embracing security automation and orchestration to automate and orchestrate security processes and functions across the enterprise.
- This enables organizations to move from inefficient one-at-a-time manual processes to faster and more robust automated solutions.