"Zero trust" has gained a lot of attention, and for good reason. Information security architectures have struggled to keep pace with the threat landscape and have not supplied organizations with a successful mechanism to protect itself from external and internal threats. This assertion is well supported by the reports of organizations across industry sectors being breached on a regular basis. These reports tell us that what we have been doing is not working and we need a fresh approach to the problem of information security. Zero trust provides a new way to approach and handle these threats through a holistic approach that does not innately trust any part of the data flow from the end user to where the data resides on its host information system.

**Zero Trust Is A Strategy, Not A Technology**

It is important to understand that zero trust is an architectural approach and not a specific technology or product. This means you cannot simply procure zero trust. It is the responsibility of an organization to develop an architecture that implements the concepts of zero trust tailored to the needs of that specific organization. Once an architecture has been developed, the tools that support the architecture can be procured and implemented. There are a staggering number of tools that can be procured to achieve a zero trust goal. Understanding how to integrate the individual tools coupled with a solid understanding of your organization's business and data will result in a strong approach to zero trust.
Approach your organization's zero trust architecture and strategy from a roadmap/maturity perspective. Unless you are operating in a greenfield environment, successful zero trust implementation may take years. This reality exists due to the complex integration and interoperability needs that exist between on-premise and cloud technologies. Additionally, you will need to secure and maintain strong commitment and buy-in from your organization's business and mission units, which must be factored into your planning effort.

The good news is, you may have already done some of the work to achieve a zero trust architecture within your organization. Tools like multi-factor authentication, software-defined networking, device health monitoring, security information and event management (SIEM) and robotic process automation (RPA) are all part of an effective zero trust strategy. If you have these tools or are already planning for them, you have already begun to lay the bricks necessary to develop a zero trust architecture for your organization.

**Know Your Business And Data**

Zero trust is focused on data protection and is a strategy to protect organizational data assets. The information security program should be working with organizational leaders to determine where critical data assets reside and their value through information security categorization processes, resulting in a triaged, prioritized and risk-ranked data inventory. Prioritizing your data in this way allows you to focus on high-priority data first. This strategy will allow you to phase in the data that falls under zero trust protections, assisting with your overall ability to implement a zero trust strategy.

A dataset's true contextual usage can only be ascertained through the business user of the data and their leadership. Another reason to focus on your executive and mission relationships has to do with understanding the context in which data is used. Tools that are part of a zero trust architecture can apply algorithms to ascertain some level of contextual usage. However, this level of contextual analysis has a high false positive rate. Close interaction with your business is required to reduce this false positive rate and develop an environment where context around data usage is well-understood.

Let’s use the example of a user accessing a file externally. If your business unit has a requirement for consistent travel, then it may not be unusual to see certain users accessing files at off-peak hours from different geographically separated areas throughout a given day. Without business context, this type of
access could be blocked. If this behavior is expected by your business unit, the blocked access may result in business dissatisfaction. This business dissatisfaction could result in an unraveling of your hard-fought-for information security and zero trust protections.

Just like you will not be able to implement all zero trust capabilities at once, you will also not be able to get all data assets under zero trust management at once. Work with your business to build a roadmap for implementation based on their needs, the risk to the organization and the ability to build context around data usage.

**Practice Effective Cyber Hygiene**

Architecturally, zero trust provides a mechanism to address current information security architecture shortcomings, which have plagued organizations for decades. Zero trust requires a significant amount of rigor to implement and maintain. As a foundational concept for zero trust, your organization must already be practicing effective information security and resiliency practices for zero trust to be an effective and implementable strategy.

Some activities to focus on include:

- Perform a complete asset inventory of your entire environment, including endpoints (regardless of form factor and operating systems), network and systems components, applications and outsourced/cloud environments.
- Develop a standard within your organization to properly secure your asset inventory.
- Ensure that your asset inventory is fully patched against known threats.
- Conduct vulnerability and penetration testing against your asset inventory.
- Limit administrative access to IT assets using a least privileges approach.
- Establish strong security operations controls with effective centralized logging and alerting.
- Ensure that data and critical IT asset configurations are backed up.

Focusing on these capabilities in addition to others will help ensure your zero trust architecture is built on a solid foundation and your implementation
cannot be circumvented due to easily exploited vulnerabilities related to poor configuration and old, unpatched code and software.