protiviti®
Face the Future with Confidence

The shift to zero trust

The future of organizations will be built on the ability to work securely from anywhere, using any device at any time. This was made clear during the COVID-19 pandemic, which forced millions of workers to work from home using company-owned or personal devices. As the velocity and persistence of cybersecurity attacks increase daily and digital transformation continues to be a priority for businesses, the concept of "zero trust" has quickly shifted to the forefront. We view the shift to a zero-trust architecture as essential to continue enhancing the security posture of an organization's data, identity, network, workloads and endpoints.

What is zero trust?

Zero trust (ZT) is a cybersecurity paradigm shift from the traditional security architecture of perimeter-based security, where anything inside the network perimeter was considered trusted. While some traffic is segregated into a demilitarized zone (DMZ) or specialized network segment, it is still trusted once it passes the toll gate. This exposes any data or systems to compromise (i.e., lateral movement) once the attacker gets through the toll gate.

ZT is not a single product, but rather a set of architectural guidelines that focus on a risk-based, data-centric, workload-first and identity-aware approach to security. A zero-trust architecture (ZTA) assumes that nothing is trusted, and that all access is verified and continually monitored and evaluated for context that could change the access requirements or even remove previously granted access.

While each zero-trust vendor, from Microsoft to Palo Alto Networks, have their "special sauce," there are commonalities. These include:

- Data protection, driven by policy, is at the core.
- Identity governance, with risk-based conditional access controls, is the first line of defense.
- Identity management includes preventative controls like adaptive authentication and detective controls like identity governance.
- Micro-segmentation is used for containment.
- ZTA overtakes VPN as the method by which remote users access network resources.
- Endpoints and infrastructure leverage tools and are supported by processes to perpetually identify threats on an ongoing basis using machine learning.

- Device trust is leveraged to strengthen authentication.
- Continuous monitoring and analytics are used to identify threats, update risk scores and provide auditability.

Zero trust origin and growth

As discussed earlier, zero trust is rooted in the principle of "never trust, always verify." It was primarily designed to address the threats of lateral movement within the network by utilizing micro-segmentation and by redefining the perimeter based on user, data and location.

The use of micro-segmentation-controlled access points, identity verification, continuous authorization and continuous evaluation of security posture allows organizations to reduce their attack surface and the capability for lateral movement.

Over the past decade, zero trust has evolved alongside cloud computing concepts to incorporate the entire business ecosystem. Zero trust is now a set of cybersecurity principles and reference architecture elements which apply broadly across the organization's technology operating environment to increase protections for workloads and data regardless of where they reside.

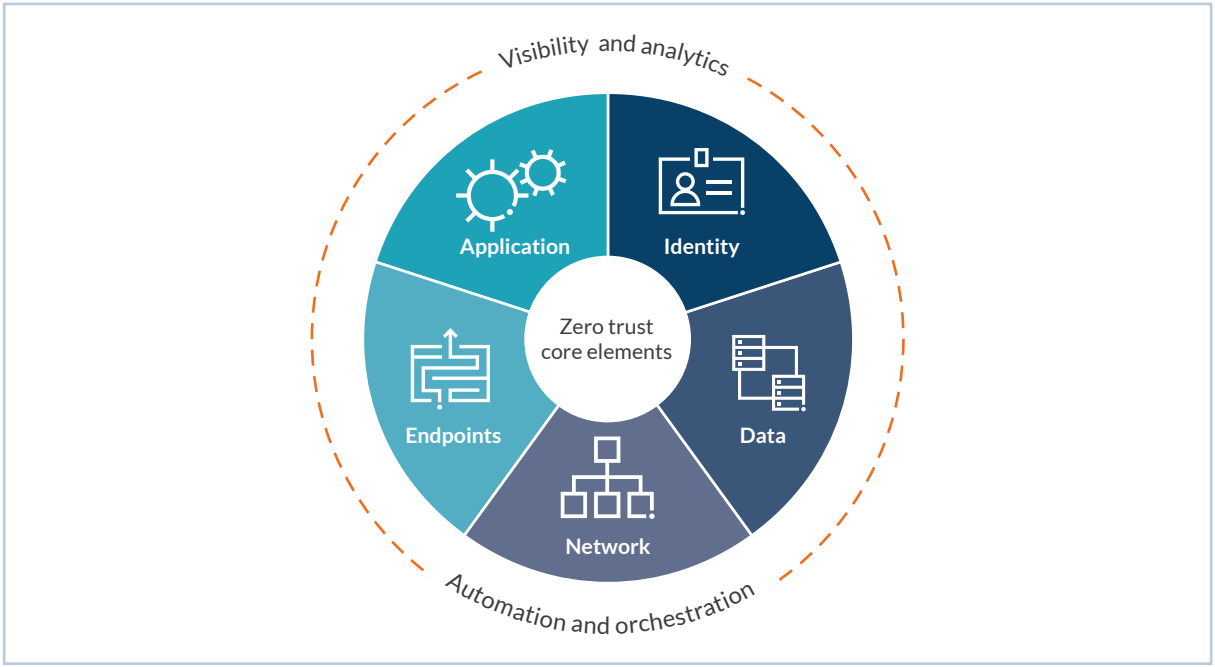
A variety of zero trust architecture models are now available from government agencies (e.g., NIST SP-800-207), commercial vendors (e.g., Microsoft, Palo Alto Networks, Netskope, Okta), and research institutions (e.g., Forrester). Most of the models are synergistic and enable an enterprise to choose a model that best aligns with their existing investments and risk profiles.

Zero trust is about policy and context — who, what, when, why and how — all being constantly evaluated to provide a current risk score to evaluate access. Protiviti views this diversity of frameworks and contextual approaches as key to the adoption of zero trust as it does not require organizations to completely reset their cybersecurity programs. At the same time, zero trust helps protect organizations from an ever-changing and complex set of privacy regulations, including GDPR and CCPA.

Core elements of zero trust

There are many trends in the marketplace for zero trust, with most focusing on point solutions that enable one architectural component or feature of zero trust. Many companies think that zero trust starts with Identity, primarily because IAM vendors are mature and have embraced ZTA principles such as Multi-Factor Authentication (MFA) and Conditional Access — and advertise them.

While IAM is a critical component and primary entry point, Protiviti views zero trust as a holistic strategy and program that consist of seven design elements. This viewpoint enables organizations to build on their current strengths in their adoption of zero trust.



The zero trust core elements used in a zero-trust architecture are:

- **Identity and access.** Every identity should be verified and secured with strong authentication practices, including multi-factor authentication, adaptive and conditional access, and role-based access controls, to validate the identity across the entire digital estate.
- **Data governance.** Data should be defined through classification and labels to ensure data discoverability of both structured and unstructured data. Organizations should enable differentiated data protections that are proportionate to the value of the data and not a one-size-fits-all proposition.
- **Networks.** Networks will continue to be the key point of control for most organizations. Micro-segmentation and micro-perimeters should be deployed to limit lateral movement across the environment and provide control points that can enable visibility into data flows.
- **Endpoints.** Endpoints must be identifiable, inventoried, isolated and secured on a network. Just like identities, the endpoint should be authenticated in the authentication process to ensure access is from an approved and secure system.
- **Application.** Applications and application programming interfaces (APIs) enable users to consume data. Safeguards are essential to discover shadow IT and control access with real-time analytics and monitoring for all applications (e.g., homegrown or third-party).

These core elements are encircled by two critical elements:

- **Security automation and orchestration.** Humans cannot operate at the speed that is required to secure modern workloads. Security automation introduces capabilities that enable automated actions when known events occur within an environment. Orchestration enables teams to modernize their processes for routine operations and incident handling to enable quicker response times and request fulfillment.
- **Visibility and analytics.** Zero trust depends upon an organization to have sufficient logging, visibility and signal from the various infrastructure and application components. Analytics moves beyond the basics of logging and introduces metrics and key performance indicators that reflect the zero-trust lens of actionable and meaningful interactions with the business.

Digital transformation and zero trust

Although COVID-19 undoubtedly accelerated the trend of "bring your own device" (BYOD) and the remote workforce, the Internet of Things (IoT) devices, cloud applications and other cloud services also contribute to the erosion of perimeter-based security. For example,

• • • Digital transformation and zero trust

Protiviti sees that most digital transformation projects are not internally aligned.

This results in delayed products launches, mediocre user experiences, and significantly **security risk**.

Zero Trust contributes to **security of digital transformation** deployments, pilots, products, platforms, and more!

an individual using their tablet to connect to a cloud application can be hundreds of miles from the corporate data center and would require security of corporate data across a multiplicity of systems. Ideally, ZTA will break down those barriers using identity, contextual data and device data, which are continuously validated and monitored. The goal of ZTA is to deliver data and access only to authenticated and authorized users and devices.

What should companies do?

- **Commit to a zero-trust strategy —** ZTA requires commitment at the highest levels of leadership across multiple lines of business to be successful.
- **Assess the current project roadmap —** Organizations should identify and understand the current and future security projects in the pipeline so they can potentially be aligned to achieve ZT principles.
- **Identify and map data —** It is critical to identify sensitive data and gain a deep understanding of where sensitive data is stored, processed and transmitted. Further, the flows of sensitive enterprise data should be mapped to effectively describe the boundaries of ZT core elements (e.g., workload, data, etc.).
- **Develop or update security policies and standards —** Security policies and standards should be updated to accommodate for changes made to enterprise resources based on ZT principles.
- **Design the future network —** Organizations should architect micro-segmentation by logically creating network segments that are used to control traffic within and between the segments. This method is used to restrict the spread of lateral threats and focuses on the development of granular policies based on a data-centric approach.
- **Implement identity governance and administration (IGA) —** A robust IGA program should be developed that emphasizes meaningful preventive and detective controls over who has access to what.
- **Strengthen access management approach —** Organizations should embrace multi-factor authentication and make adaptive and contingent decisions based on the right user having access to the right resources at the right time.
- **Implement monitoring and visualization tools —** It is important to continuously monitor the ZT ecosystem by expanding the use of existing technologies or implementing recent technologies to gain visibility into the security of ZT core elements.
- **Embrace security automation and orchestration —** Information from corporate resources should be gathered to enable development of visualizations and expand the use of automation and orchestration to create feedback loops and scoring models.
- **Be patient —** The zero-trust methodology represents a journey and will take a few years to expand across the entire network and associated components.

How can Protiviti help?

As the paradigm shift to zero trust occurs and companies continue their digital transformation journey, Protiviti can assist organizations at every stage, providing industry leading expertise to help achieve a more secure and robust security posture. Our services to help organizations implement a zero-trust methodology include:

- **Prepare a zero-trust strategy.** Our design thinking workshops can help organizations develop and communicate a ZTA strategy, including creation of the artifacts needed to socialize with staff, executives and the board of directors.
- **Assess an organization's readiness to move towards a zero-trust architecture** from existing governance artifacts to existing technology investments. Protiviti can help organizations determine capability gaps, then develop a roadmap for the deployment of zero trust architecture components over time. Zero trust is an evolution of existing architecture and does not have to occur in a "big bang" moment.
- **Perform an identity and access management (IAM) assessment** of the environment to assess gaps and build a roadmap to have an IAM program that aligns with a ZTA.

- **Perform a data assessment to discover** where the organization's most critical data is located and how it is used within the environment, using automated tooling to assist in data discovery efforts that span across structured and unstructured data.
- **Conduct readiness workshops** with an organization's infrastructure, operations, business and security teams to build buy-in and establish the foundation for implementing a zero-trust architecture.
- **Connect organizations with leading vendors** in identity, network and managed security services to speed up and simplify implementation.

Contacts

Chip Wolford
+1.937.541.1545
chip.wolford@protiviti.com

Jon Medina
+1.415.402.6421
jon.medina@protiviti.com

Nick Puetz
+1.314.656.1716
nick.puetz@protiviti.com

Terry Jost
+1.469.965.6564
terry.jost@protiviti.com

John Stevenson
+1.469.374.2410
john.stevenson@protiviti.com