Enterprise Strategy Group | Getting to the bigger truth.™

ESG SHOWCASE

Top Segmentation Attributes to Simplify Zero Trust

Date: July 2021 **Author:** John Grady, Senior Analyst

ABSTRACT: As the concept of zero trust has gained traction, confusion has increased with regard to what it entails, where to start, and what technologies best support the strategy. While zero trust touches on many security disciplines, segmentation must be a foundational element to ensure that resources are isolated and attackers that gain a foothold in the environment are not able to move laterally. Illumio Core delivers Zero Trust Segmentation that helps organizations more efficiently implement zero trust; consistently protect complex, hybrid environments; and improve security effectiveness by enabling collaboration across a diverse set of stakeholders.

The Zero Trust Dilemma

Most modern businesses rely on applications to keep employees productive, collaborate with partners and vendors, and ultimately drive revenue. In fact, ESG research has found that 88% of organizations support at least 100 business applications, with more than half of respondents (59%) indicating that at least 31% of those applications are internally developed.[1] The increasing use of cloud platforms, agile development methodologies, and modern application architectures has helped enable application scale, but also created complexity.

A significant reason for this is the volume of intra-application, or east/west, traffic. As workloads have become more distributed and applications more interdependent, the amount of east/west traffic in the enterprise has skyrocketed. Traditional controls have historically been location-based and more focused on north/south traffic, an approach that fails to address ephemeral workloads that reside across on-premises data centers and multiple public cloud platforms. Considering the sensitive data these applications often contain, maintaining granular visibility and control across all the applications the modern enterprise supports has become critical.

> **The increasing use of cloud platforms, agile development methodologies, and modern application architectures has helped enable application scale, but also created complexity.**

Zero Trust Can Help, But Many Are Overwhelmed and Don't Know Where to Start

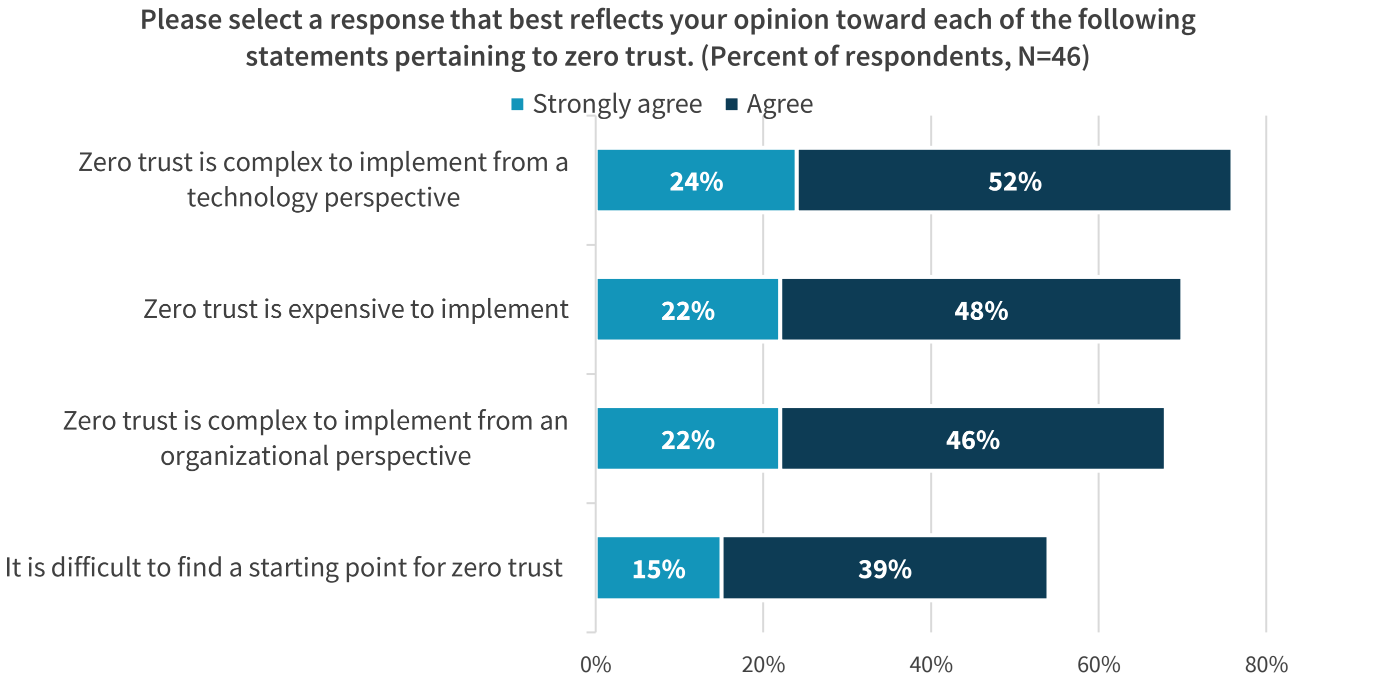
To address these and other issues, many organizations have begun to explore zero trust strategies. The concept of zero trust is not new but has taken on even more importance over the last few years, as enterprise environments have become more distributed. At a high level, zero trust removes the idea of implicitly trusting the user, resource, or device based on its

[1] Source: ESG Master Survey Results, *Trends in Modern Application Environments,* December 2019.

location. It assumes the network is compromised and seeks to broker specific access through a least-privileged approach by identifying what should be allowed and blocking everything else.

As the importance of zero trust has risen, a variety of industry voices have introduced differing views that may put emphasis on identity, data, remote access, or analytics. ESG research indicates that this has led to user confusion and contributed to some negative perceptions among organizations that have yet to implement the initiative. Specific concerns focus on cost, complexity, and finding a starting point (see Figure 1).[2]

Figure 1. Negative Perceptions of Zero Trust



Source: Enterprise Strategy Group

An additional difficulty with regard to zero trust is the cross-functional collaboration required for success. In fact, ESG research found that 40% of organizations have had to pause or abandon a zero trust project in the past. The most common reason, cited by 50% of those who had paused or abandoned a project, was that they had organizational issues in implementing the initiative.[3]

Segmentation Should be a Foundational Element of Zero Trust, But Must Be Simplified

While it is true that many tools can support zero trust principles to one extent or another, the prime focus of the strategy is to remove any implicit trust from the network. At its core, this requires that entities be isolated from one another and only allowed to communicate when allowed by corporate policy. This is often described as moving from an open network model to a highly segmented one. However, traditional, static methods of achieving segmentation, such as access control lists and VLANs, often lack the scalability modern environments require. Solutions focused on the workload level to abstract segmentation from the network can help ensure segmentation is as dynamic and scalable as the environment it protects, without rearchitecting the network itself.

[2] Source: ESG Master Survey Results, *The State of Zero Trust Strategies*, May 2021.
[3] Ibid.

Specifically with regard to zero trust, ESG research respondents cited five key attributes that tools supporting these strategies must include, all of which are directly applicable to segmentation.[4] Specifically, these tools should provide:

- Coverage for cloud and on-premises environments (31%). The distributed nature of enterprise applications means most organizations can no longer support different security tools for each part of the environment. Tools that unify control across different locations and focus on the application and workload rather than network or VPC they reside on are more important than ever.

- Risk assessment capabilities (29%). A core element to zero trust is understanding the risk a connection may pose. With regard to secure access, this may be predicated on whether the device is corporate-managed or employee-owned. When the focus is applications, understanding the relationships between workloads and any vulnerabilities contained within is essential in determining risk.

- Automation of policy creation and management (25%). As the rate with which new workloads are created increases, policy should be automatically generated based on the type of application, dependencies, platform, and other factors. Administrators can then quickly review and test the policy before turning it on to ensure the application will function properly.

- Ease of deployment (23%). Even before automating policy, solutions must be deployed across on-premises and cloud locations. Reducing the time to value by streamlining this process can help security teams generate quick wins to show the value of segmentation in support of zero trust and begin to build a business case for expansion.

- Support for legacy applications/systems (23%). As much as the market highlights modern applications, the reality is that most enterprises will continue to support a variety of architectures for the foreseeable future. Solutions that provide consistency across the entire application landscape can help streamline zero trust deployments.

Finally, both zero trust and segmentation often have a variety of stakeholders across security, network, IT, and application teams. To help drive collaboration, tools supporting zero trust should help break down organizational boundaries by supporting multiple personas and providing role-based visibility and reporting across all the different stakeholders involved in the initiative.

Illumio Zero Trust Segmentation

Illumio was founded in 2013 and currently has hundreds of global enterprise customers, including 6 of the 10 largest banks, the 3 largest enterprise SaaS companies, 5 of the largest insurance companies, as well as other large and mid-size organizations that use Illumio to protect anywhere from 100 to more than 100,000 workloads. The vendor's flagship workload segmentation product is Illumio Core. Core directly enforces rules using the built-in native firewall capability inside modern operating systems, network devices like switches and routers, load balancers, and even hardware firewalls. Illumio believes this holistic approach provides the most reliable way of delivering Zero Trust Segmentation.

Core is comprised of 2 components:

- A lightweight agent called the virtual enforcement node (VEN), which is deployed on workloads to collect data from, and push rules to, the native firewall.

[4] Source: ESG Master Survey Results, *The State of Zero Trust Strategies*, May 2021

- The policy control engine (PCE), which collects all the flow information from the VENs and builds an application dependency map, showing the relationships between workloads in real time. The PCE then generates application-centric policies and automatically distributes rules to the VEN to push to the native firewall for enforcement.

Illumio Core acts like a control plane for native firewalls and generates security policies based on the identity of the workloads in the environment. This is achieved by using a 4-dimensional labelling scheme, which allows the abstraction of policy generation away from the network and infrastructure. Additionally, Core provides role-based access control (RBAC) to allow application owners, DevOps teams, and other stakeholders visibility into segmentation policies to foster better communication and collaboration across silos.

Recent updates to Illumio Core help deliver on the core attributes organizations require from solutions supporting zero trust strategies. Automated security enforcement via a feature named Enforcement Boundaries provides customers the flexibility to deploy segmentation broadly or through a phased approach. Security teams can create and enforce a policy protecting high-value assets such as customer data or sensitive intellectual property across the entire organization at once or service by service over time. This reduces time to value while also providing customers flexibility for those who would prefer to work at their own pace.

Through integrations with Qualys, Rapid7, and Tenable, Intelligent Visibility flags vulnerability and exposure data, generating real-time application insights. This helps security teams identify at-risk workloads, recommends policy to mitigate the risk, and tests the policy to ensure application dependencies are not impacted. DevOps and applications teams benefit from this visibility across multi-cloud environments and can monitor workloads as they are generated in public clouds.

Finally, Illumio offers organizations flexibility through its expanding list of technology integration partners and SuperClusters capability. While Illumio is more than capable of supporting segmentation projects in environments with only a handful of workloads, SuperClusters expands the vendor's capabilities to environments with more than 100,000 workloads across cloud, hybrid, and on-premises locations. Additionally, integrations and interoperability across cloud and technology providers such as AWS, Microsoft Azure, Google Cloud, Palo Alto Networks, F5, IBM Cloud, and Oracle Exadata mean that customers can deploy Illumio broadly by leveraging a variety of existing investments to achieve segmentation quickly.

The Bigger Truth

Segmentation projects have often been viewed with some level of skepticism. Many initiatives stall due to complexity, cost, timing, or any number of other reasons. Yet segmenting resources is critical to zero trust and, when implemented correctly, a zero trust strategy focused on segmentation can improve security, enhance efficiency, and increase business resiliency. This leaves many organizations struggling with how to bridge this gap and what to look for in segmentation technologies. To simplify this process, users should seek out solutions that provide consistent coverage across different locations and application architectures, offer ease of deployment and management powered by automation, have a strong focus on risk to help teams prioritize resources and planning, and foster cross-functional collaboration.

Illumio Core supports Zero Trust Segmentation by delivering on each of these requirements. By abstracting segmentation from the network and leveraging existing control points, Illumio Core can help simplify deployment, while providing consistent protection across complex, hybrid environments. The broad visibility into application relationships, coupled with integrations across threat, configuration, and vulnerability scanners, provides security teams with proactive, risk-based policy recommendations to improve efficiency. Finally, role-based management and reporting ensure all stakeholders have the visibility they require to do their jobs.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com ☎ 508.482.0188