illumio

SOLUTION BRIEF

Achieving Zero Trust with Illumio

Enterprises struggling with increasingly complex infrastructure are turning to Zero Trust as a common security model for controlling and ensuring consistent security across environments. This paper lays out how Illumio Core™ maps to a Zero Trust framework.

What's Driving This?

The growing complexity of cloud, multi-cloud, and hybrid compute, combined with a rapidly evolving adversary threat landscape, has exposed the inadequacy of traditional network security. Increasingly complex applications and a lack of visibility creates the perfect storm of blind spots, poor detection, and limited enforcement options for hybrid and multi-cloud deployments.

Yet cloud adoption is projected to grow to nearly 80 percent over the next two years[1]. By 2020, almost 50 percent of businesses will store the majority of their data in the public cloud[2]. Enterprises are adopting cloud to accelerate business; however, traditional security can slow this down – or worse, sabotage it.

What Is the Threat?

One of the biggest blind spots in current network defenses is the lack of visibility and control of East-West traffic (also known as the lateral movement of traffic). Because network security has been focused on North-South traffic through the perimeter, attackers who successfully breach the external firewall often have no further restrictions once inside the network. In other words, hackers are free to move laterally through the network until they reach their targets. This is often referred to as the "flat network" problem.

The same challenges of network security extend to the cloud since most organizations' public cloud environments are logical extensions of their existing data centers.

Illumio Core solves the problem of invisible or obscured East-West communications within network environments, enforcing default-deny security through granular microperimeters around data and applications behind the firewall.

What Is Zero Trust?

"Zero Trust" is all in the name. Instead of assuming internal traffic within the network is trusted and "safe" for permitted access, Zero Trust eliminates automatic access for any source – internal or external. Forrester's Zero Trust eXtended (ZTX) framework is comprised of seven components of an enterprise ecosystem where Zero Trust principles should be applied. See figure 2 below for how Illumio Core maps to the framework.

> "Forrester recently concluded that Zero Trust can reduce an organization's risk exposure by 37% or more. But it also found that organizations deploying Zero Trust can reduce security costs by 31% and realize millions of dollars in savings in their overall IT security budgets."[3]

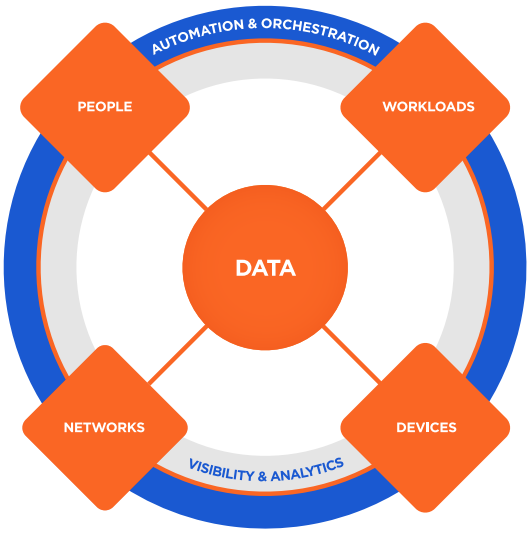

Figure 1. The Zero Trust eXtended (ZTX) Ecosystem, Forrester Research, Inc., January 19, 2018

[1] https://resources.idg.com/download/executive-summary/
[2] https://www.oracle.com/cloud/cloud-threat-report/
[3] https://www.darkreading.com/cloud/debunking-5-myths-about-zero-trust-security/a/d-id/1334064

illumio

Framework Components	Illumio Core Capabilities
Network	• Default-deny micro-segmentation • Informed, granular policy design and testing • Infrastructure-agnostic enforcement • Violation alerts
Data	• Secure data and application with microperimeters • Security follows the data – anywhere • Protection for data-in-transit
Workloads	• Granular policy control at massive scale • Process-level enforcement • Security follows the workload – anywhere • Simplified deployment
People	• User-based segmentation • Remote access control • Lateral movement prevention
Devices	• Device-level segmentation • Unknown device detection • Device quarantine
Visibility and Analytics	• Live visibility across environments • Painless discovery and classification • Thorough auditing
Automation and Orchestration	• Orchestration tool integration • REST API • CMDB integration • CMDB hygiene • SIEM integration

Figure 2: How Illumio Core maps to Forrester's Zero Trust eXtended framework.

Illumio Core's host-based micro-segmentation effectively limits lateral or East-West movement behind the firewall by requiring affirmative permissions to access anything on the network. This is done through allowlisting.

An allowlist approach is consistent with a Zero Trust model because it denies everything and only permits what you explicitly allow. Allowlisting is a better choice in today's data centers because the list of what you do want to connect in your data center is much smaller than what you do not want to connect, effectively eliminating false positives.

How Does It Work?

How can you enforce Zero Trust across all of your data and applications behind the firewall?

Zero Trust requires coordinating rules and policies governing perimeter and internal defenses. Architecturally, it demands that you segment and secure networks across locations (public and private cloud) in order to isolate threats at a "microperimeter" level.

Micro-segmenting your network transforms security from an "outside-in," perimeter-based model of protection to an "inside-out" framework where everything is locked down unless it is approved. Organizations who want to achieve Zero Trust data can also optionally secure data in transit within or across microperimeters.

Zero Trust is:	**Zero Trust is not:**
• Default-deny access also known as "allowlisting."	• Allowing access unless it is specifically forbidden.
• Full visibility of your environment across on-premise, cloud, bare-metal, virtual machines, and containers.	• Lack of visibility across external environments to inform policy decisions and enforcement.
• Consistent security across workloads – wherever they run.	• Managing disparate policies across different environments with security that can't follow the workload.
• Granular segmentation with microperimeters to isolate data and applications by Role, Application, Environment, or Location.	• Perimeter-only firewall defense.
• Successful deployment at scale and ease of use to operate effectively.	• Heroic efforts with bad outcomes.

What Solutions Are Available?

Can Zero Trust be deployed leveraging existing investments?

If an organization has upgraded their switches and hypervisors with software-defined networking capabilities, it theoretically sounds straightforward to use these solutions for micro-segmentation as well. But these approaches can't offer Zero Trust consistency within and across environments outside of the network, much less give you visibility or control.

Traditional perimeter-based defenses were made and architected for the network you own – not for the public cloud you are renting. They simply don't cut it. In practice, they compound complexity and limit visibility in an environment demanding greater speed and agility.

So, what's the secret to segmenting your data down to a microperimeter level and applying granular policy consistently across any environment? The key to understanding micro-segmentation to create microperimeters is understanding that it is not network segmentation. The network should not matter.

Zero Trust with Illumio

How can you adopt a Zero Trust architecture without re-architecting your network?

Use the native enforcement points that already exist in your applications, with orchestration to coordinate them as they follow the workload wherever it goes.

How does Illumio's host-based micro-segmentation work?

- Illumio Core uses an extremely lightweight agent called a Virtual Enforcement Node (VEN) to activate the operating system firewall on every server in a network, enabling clear definition of the workload's identity, role, group membership, and resident applications.
- The VEN programs the Windows Filtering Platform (WFP) for Windows and Linux kernel firewalls to enforce policy. Granular policy definition sets explicit permissions on who may communicate and the permitted workload. Unauthorized application uses are blocked from accessing workload applications and access attempts are logged and generate alerts. Unneeded and unauthorized communications between workloads and communications not allowed by policy are blocked. The resulting operational picture is intuitive and manageable, combining visibility, understanding, and control.
- VEN rules and policies are coordinated through a central Policy Compute Engine that serves as the orchestrating "brain" to provide the holistic and easily understandable views of network traffic and relationships.
- Insights from the VENs are combined to visualize workflows in a real-time application dependency map, Illumination. This map gives you visibility into traffic across environments, including feedback on unauthorized flows. The visibility is also key to initially designing and testing micro-segmentation policy – you can't protect what you can't see.

Illumio Core's architecture enables Zero Trust without the need to layer new, complicated, and unproven technologies to address cloud security challenges. The infrastructure-agnostic approach has other key benefits: visibility across all environments, a single source of control, adaptive policy as a workload moves, and the ability to measure your results. Deploying it is also less risky to applications running on your network.

What Does Successful Deployment Look Like?

Zero Trust principles are designed to be bulletproof in theory – but they must also scale in practice. How does an organization roll out their Zero Trust micro-segmentation solution, and what does success look like in a deployment and beyond?

A successful micro-segmentation deployment requires a solution with the following elements:

- **Full visibility** – Do you have visibility across all environments to make informed decisions when designing policies?
- **Policy modeling** – Can you model and test policies within their environment prior to enforcement, and without affecting network communications and data flows or breaking applications?
- **Granularity** – Can you enforce policies from entire environments down to processes running on individual hosts?
- **Dynamic adaptation** – Do policies adapt to changes in your environment?
- **Quantifiable risk mitigation** – Can you measure your "before and after" risk mitigation?
- **Reporting** – Can you generate on-demand documentation of policy provisions?

The diagram below maps out the common path in many organizations' journey to Zero Trust with Illumio.

Conclusion

Rapid adoption of cloud computing and unprecedented connectivity of enterprise IT has exposed the inadequacies of existing network security. Zero Trust has become a dominating framework because of its aggressive restrictions on access both from outside and inside the firewall. Zero Trust security requires:

1. Default-deny access permissions.
2. Locking down data and applications by segmenting them with microperimeters.

These actions limit the spread of breaches in data centers and cloud environments.

Host-based approaches offer full visibility and granularity required to design segmentation across your environments and enforce microperimeters at scale wherever workloads are running – serving many of the tenets of Forrester's Zero Trust framework. What's more, host-based micro-segmentation is faster and simpler to deploy and operate than traditional infrastructure or hypervisor-dependent methods, as well as more agile in its approach to environments outside the network.

Learn more:

- Read the Illumio Core datasheet.
- Visit our Zero Trust page.

illumio

Illumio enables organizations to realize a future without high-profile breaches by preventing the lateral movement of attackers across any organization. Founded on the principle of least privilege in 2013, Illumio provides visibility and segmentation for endpoints, data centers or clouds. The world's leading organizations, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit www.illumio.com/what-we-do.

Gartner peerinsights™

See what customers have to say about Illumio.