The business benefits of Application-Centric Zero Trust

An AlgoSec eBook

Table of content

Introduction

The frequency and cost of cyberattacks are staggering. SentinelOne research disclosed 30,000 vulnerabilities last year, a 17% increase from previous figures, reflecting the steady rise in cyber risks. Other statistics indicate that there are 2,200 cyber attacks per day, with one happening every 39 seconds on average. Experts have found that increases in ransomware attacks, nation-state cyber warfare, and financial fraud have led to a projected total global cost of cybercrime reaching $1.2 trillion annually by the end of 2025.

Cyber threats are also becoming increasingly complex and sophisticated, escalating security risks. Prevailing wisdom is that breaches are inevitable, which makes containment just as critical as detection and prevention.

As a result, businesses must adopt a proactive approach to cybersecurity that can contain attacks, thereby protecting higher-value, sensitive assets. This is where Zero Trust security comes in.

Zero Trust is not a technology, but a philosophy that suggests a fundamental cybersecurity problem lies in a flawed trust model, where everything outside the network cannot be trusted, while everything inside the network is trusted by default. Zero Trust posits that perimeter-based security is no longer viable. Instead, we need an approach to designing and implementing a security program based on the idea that no user, device, or agent should have implicit trust, either externally or internally.

The three foundational principles of Zero Trust

Verify explicitly

Every access request is authenticated and authorized based on all available data, such as user identity, location, device health, and workload context

Use least privilege access

Access is granted with the minimum permissions necessary for users or applications to perform their tasks, reducing exposure to attacks

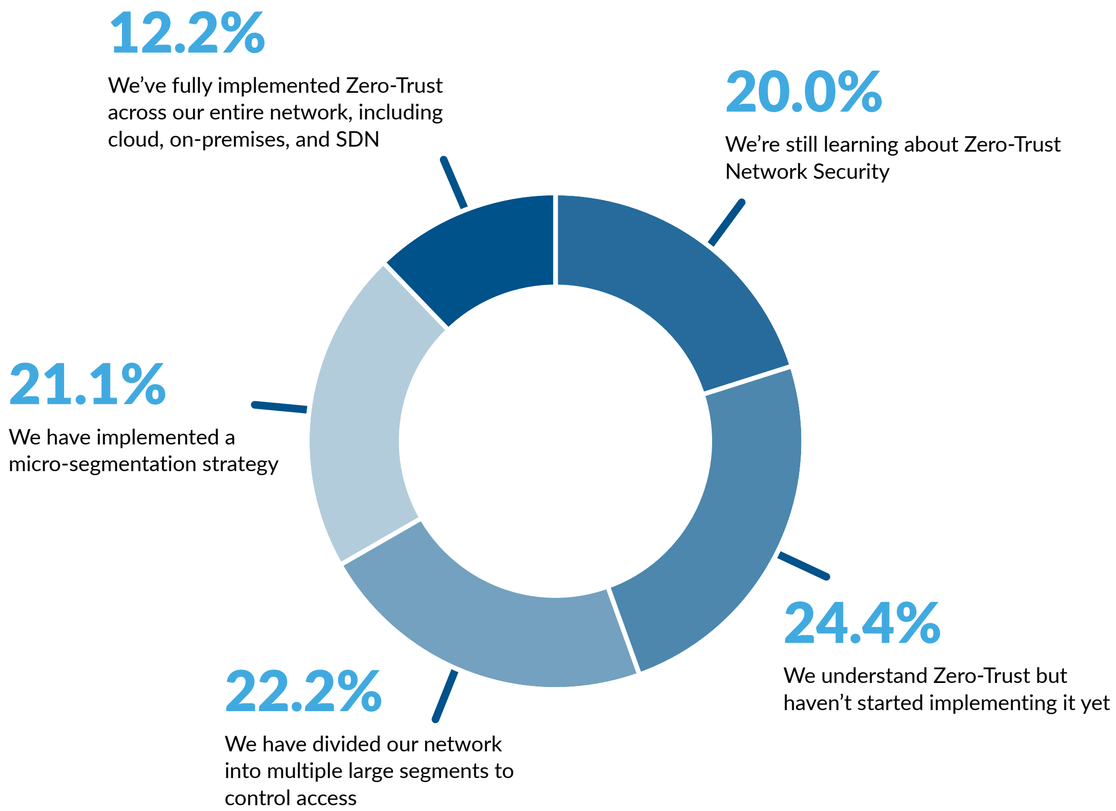
Assume breach

The network is treated as compromised by default, and segmentation is used to contain threats, limiting lateral movement within the network

The case for expediting Zero Trust at the network level

The primary goal of Zero Trust is to mitigate breaches, which is far more cost-effective than recovering from a breach, including paying regulatory fines and restoring customer and employee confidence. IBM's 2025 Cost of a Data Breach Report found that the global average price tag for a breach was USD 4.44 million, with 76% of organizations saying the recovery took longer than 100 days, and 26% reporting it took more than 150 days.

AlgoSec found that while awareness of Zero Trust continues to gain traction, with 56% of businesses fully or partially implementing it, 20% are still in the learning phase and lack a clear implementation strategy. The hesitation to pursue Zero Trust can be rooted in misconceptions, including the impression that it's a rigid, complex, and expensive approach to cybersecurity, and even the belief that it's just another passing buzzword or fad.



Enterprises are grappling with integration challenges, legacy infrastructure limitations, and the need for greater security awareness

Another barrier that impedes the progress of Zero Trust is rooted in past challenges associated with standard and virtual firewalls, which required tedious, time-consuming actions such as:

- Reassigning IP addresses
- Making routing changes
- Defining new VLANs
- Connecting new cables

According to Gartner, software-defined data centers mitigate these challenges by embedding filtering and policy enforcement directly into the network fabric. For instance, on-premise virtualized data centers, such as Cisco ACI and VMware NSX, can automatically filter and apply policies, while public clouds like Amazon AWS and Microsoft Azure come with built-in filtering capabilities.

One of the biggest hurdles for organizations looking to implement a Zero Trust framework is how to configure and write policies that help them achieve their goals, especially as businesses adopt cloud and on-premise systems. This makes managing interconnected applications, meeting compliance requirements, and securing hybrid environments even more complex. With the rapid expansion of application deployment and increased network complexity, organizations need to simplify Zero Trust adoption through application-based segmentation.

Application-based segmentation is central to Zero Trust

Segmentation is a fundamental element of Zero Trust, helping to isolate different parts of the network and limit the potential spread of attacks. Despite its importance, organizations often face difficulties in its implementation. According to a recent survey by AlgoSec, only 5% of companies have fully deployed network segmentation, while 75% struggle with enforcement for a variety of reasons, such as:

- **Unclear objectives**
  Organizations may lack clarity on how segmentation aligns with broader business goals, leading to misaligned priorities.
- **Limited visibility**
  Without comprehensive insight into traffic flows, devices, and applications, identifying the correct segmentation boundaries is challenging.
- **Complex infrastructure**
  Hybrid networks incorporating firewalls, cloud security, and micro-segmentation solutions complicate segmentation efforts.
- **Lack of automation**
  Manually configuring segmentation policies is time-consuming and prone to errors, especially across large, hybrid networks.

AlgoSec prioritizes application-based micro-segmentation for its clients, finding it to be a more effective approach that overcomes these challenges by focusing on securing application connectivity rather than just the infrastructure. This critical shift provides deeper visibility into application traffic patterns, enabling more precise and automated security controls. A few best practices for this approach include:

- **Conduct a comprehensive discovery exercise** that provides a view of all application traffic flows. This will define how each application communicates across the network and provide east-west traffic visibility, enabling the identification of optimal segmentation points. The process includes annotating all network flows with the application name (intent), the reason they exist, and the application they serve. It also requires optimizing the network by aggregating the thousands of "thin" flows into a lower number of "fat" flows that describe the traffic at a larger granularity.
- **Write policies and activate filters** that restrict unauthorized traffic from moving between segments. This requires defining the type of traffic authorized to travel between segments and writing policies that enable it to flow freely within each segment. It also involves understanding the intent of all legitimate traffic in the data center and which application each connection serves.
- **Automate the change management process** by creating and enforcing security policies based on discovered application flows, ensuring consistent and reliable security controls across hybrid environments. It can also minimize the risk of misconfigurations and ensure segmentation policies are maintained over time.

AlgoSec's application-based approach to Zero Trust segmentation offers significant advantages.

- **Limit breach impact:** Micro-segmentation's ability to confine breaches and reduce damage is making it a growing priority for industries and government institutions around the world. Gartner found 60% percent of enterprises working toward a Zero Trust architecture are planning more than one deployment form of micro-segmentation, which is up from less than 5% in 2023.
- **Strengthen security posture:** Smaller, well-defined segments with specific security controls offer stronger protection for critical assets. IBM's Cost of a Data Breach also found a 9% decrease in the global average breach costs due to faster identification and containment—much of it from organizations' own security and security service teams, with help from AI and automation.
- **Reduce lateral movement:** An analysis conducted by VMware showed that 45% of intrusions contain a lateral movement event. By utilizing segmented networks, organizations present attackers with greater barriers to moving laterally, helping to contain potential threats.
- **Enhance operational efficiency:** AlgoSec has found that proper segmentation also reduces network congestion, optimizes resource usage, and simplifies troubleshooting, ensuring continuous protection for business-critical applications.

Algosec's methodology for implementing Zero Trust practices

AlgoSec's philosophy is that each organization is on a unique journey toward automation, and consequently will have a different approach and timetable for implementing Zero Trust. Our goal is to customize the process so that it centers on your company's unique operational capabilities and philosophical perspectives.

While implementing Zero Trust is not a one-size-fits-all strategy, it does contain a standard set of principles based on John Kindervag's model that centers on automation and orchestration. It includes the following five steps:

1. Define the protect surface

The first step is to break down your environment into smaller pieces that need to be protected. These elements, known as the "crown jewels," include critical data, applications, assets, and services. Doing so helps concentrate resources, simplify security controls, and limit access. It also identifies patterns between elements that will ultimately help with the segmentation in step two.

2. Map the transaction flows

Next, it's crucial to analyze traffic flows across the hybrid network environment. This requires digesting multiple streams of traffic metadata, including the application it serves, to visualize transaction flows clearly. After these are discovered and optimized, the system must continue tracking changes and updating new flows as changes are made to the application.

3. Architect a Zero Trust environment

In this step, security measures are designed to thoroughly inspect every packet for malicious content before granting access to Layer 7, or the application layer, which is critical for network communication. This is done by using the Kipling method of asking who, what, when, where, why, and how to determine the validity of all access attempts, identify red flags, and block entry as warranted.

4. Create Zero Trust policies

Step four builds on step three by developing and implementing policies that ensure all access is continuously authenticated and verified before being granted. AlgoSec helps organizations automatically analyze and validate traffic changes before they are implemented in all firewalls, cloud, and software-defined network solutions. By automating the security policy change process, AlgoSec helps reduce risk, vulnerability, and compliance violations.

5. Monitor and maintain

The final step is a continuous and detailed analysis of all firewall policies, rules, traffic logs, and change configurations, which offers critical network intelligence about security breaches and attempted attacks, such as viruses, trojans, and denial of service. AlgoSec allows users to monitor behaviors on the network and enables network firewall administrators to identify which firewall rules to create and implement that allow only necessary access.

Zero Trust in the real world

NCR Corporation is a leading global point-of-sale (POS) provider for restaurants, retailers, and banks, and a provider of multi-vendor ATM software. Headquartered in Atlanta, Georgia, NCR has over 36,000 employees in 160 countries, and its solutions are distributed in 141 countries.

NCR Case Study #1: Accelerating Towards Zero Trust

Challenge

NCR needed to connect its DevOps pipeline with its network security. With over 4,500 policy changes made annually, it was difficult to securely manage their entire networking and security environment while being responsive to application owners, but still achieve Zero Trust.

Solution

Automate and orchestrate security policy changes across the entire hybrid network to securely accelerate application delivery and manage application connectivity end-to-end—including public cloud, Cisco ACI, and physical firewalls.

Results:

- Achieved complete visibility of their global security posture from a single dashboard
- Automated risk analysis, achieving visibility and insights into the risks that changes introduce
- Streamlined auditing process with automatic logging and audit-ready compliance reports
- Cleaned up and reduced firewall policies with rule cleanup, object cleanup, and policy tuning

"As we aspire to achieve Zero Trust, when moving into the cloud, micro-segmentation and container security come into play. Therefore, we need tools like AlgoSec to assist us in the journey because most application owners don't know what access is needed."

Scott Theriault
Global Manager Network Perimeter Security
NCR Corporation

NCR Case Study #2: Network Security Transformation

Challenge

Automate security policy changes, improve visibility, streamline auditing, and achieve a Zero Trust framework.

Solution

Create a policy management solution that provides a seamless pipeline. In this case, NCR needed the pipeline to allow the end-user to interact with ServiceNow, which then has to interact with AlgoSec. The next step required AlgoSec to interact with NCR's firewall infrastructure, conduct a validity check, and send the results back to ServiceNow.

Results:

- Decreased the security policy change timeframe from three to five days, to hours or even minutes
- Reduced by 50% the number of hours it took to prepare for auditors
- Enabled rule clean-up, object in-group clean-up, rule recording, and policy tuning
- Provided a metric to measure continuous improvement for policies that were allowed but didn't need to be implemented

"AlgoSec allows us to achieve security at the speed of business. It provides an end-to-end solution that covers application, infrastructure, and even container security, which is a new frontier for us."

Scott Theriault
Global Manager Network Perimeter Security
NCR Corporation

NCR

The long-term business benefits of segmentation and Zero Trust

AlgoSec research found that 43% of organizations had experienced an attack on their public cloud infrastructure in the last 24 months. One of the most common occurrences was malware moving laterally from other parts of the environment (44%), proving that attackers do not think in silos. They find the easiest point of entry and work their way to something of value. Weakness in any part of the environment can lead to a compromise elsewhere.

Zero Trust, with its focus on continuous verification and network segmentation – both micro and macro – offers a robust framework for reducing security risks while ensuring protection for business-critical applications. Ultimately, Zero Trust brings value beyond security in that it supports a wide range of business objectives that resonate with the C-Suite and board, including maintaining continuous operations, elevating customer service, improving the employee experience, supporting growth, and minimizing liabilities.

While implementing Zero Trust may seem overwhelming, AlgoSec's application-centric approach simplifies the process by providing automation, visibility, and the ability to manage both micro and macro-segmentation effectively. This allows organizations to execute and maintain an efficient, secure, and resilient Zero Trust architecture tailored to their unique business needs and capabilities.

Ultimately, every business will need to implement a Zero Trust framework not only to mitigate the impacts of cyberattacks, but to gain a competitive advantage now and in the future. Long-term, Forrester anticipates Zero Trust will go well beyond a security model and be integral for evolving business paradigms and the rapid integration of emerging technologies. Its analysts predict that because Zero Trust's core principles can easily adapt to future scenarios, it will be essential for any organization that wants to mature to a future-fit technology strategy, which is a customer-centric approach that enables adaptivity, creativity, and resilience.

About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to securely accelerate application delivery up to 10 times faster by automating application connectivity and security policy across the hybrid network environment.

With two decades of expertise securing hybrid networks, over 2200 of the world's most complex organizations trust AlgoSec to help secure their most critical workloads. AlgoSec Horizon platform utilizes advanced AI capabilities, enabling users to automatically discover and identify their business applications across multi-clouds, and remediate risks more effectively. It serves as a single source for visibility into security and compliance issues across the hybrid network environment, to ensure ongoing adherence to internet security standards, industry, and internal regulations.

Additionally, organizations can leverage intelligent change automation to streamline security change processes, thus improving security and agility. Learn how AlgoSec enables application owners, information security experts, SecOps and cloud security teams to deploy business applications faster while maintaining security at www.algosec.com.

For more information, visit www.AlgoSec.com

algosec