vArmour

ZERO TRUST SOLUTION BRIEF

Accelerate Your Zero Trust Journey

Gain Enterprise-Wide Visibility in Just Days with vArmour

Background

Zero Trust has been a well-defined security model for over a decade, and now, many regulatory bodies such as NIST, have specified Zero Trust principles as part of the published control guidelines. Furthermore, due to the rapid decline of network perimeters, the explosion in identity sprawl and remote work, growth in threat landscape including ransomware, and new compliance requirements, enterprises need to realize the time is now to deploy Zero Trust Architecture (ZTA).

Zero Trust Principles

There is no single product, solution, or vendor that provides a silver bullet to implement Zero Trust. Rather, Zero Trust is an architecture with a set of guiding principles for workflow, system design, and operations. A ZTA assumes attackers are always present, and trusted relationships must be explicitly declared and lifecycle for every enterprise resource.

Seasoned security leaders recognize that before defining trust policies or deploying anything, they need the visibility to know what they need to protect and how. Many existing systems of record such as CMDBs are out of date and inaccurate. Firewall or log management solutions cannot provide this type of visibility easily because they rely on event-based or log-based architectures, are limited to certain technology stacks, and cannot easily scale to protect the entire application infrastructure.

Legacy firewall solutions are not built for Zero Trust

Organizations face a number of challenges as they begin their Zero Trust journey:

- Dynamic development lifecycles introduce constant change into the production environment.
- Critical applications are increasingly deployed across multiple clouds and highly diverse technologies, from mainframes to container platforms, resulting in security leaders being blind to unknown applications, assets and workloads, as well as the complex interdependencies and relationships they have with one another.
- Poor visibility inside the enterprise perimeter means there is no way to know what to trust to minimize the attack surface area and protect applications.

vArmour Business Value for Zero Trust Architecture

Reduce Cyber Risk

- Establish trust perimeters and establish micro-perimeters to isolate applications from lateral movements

Secure Cloud Applications

- Implement consistent policies across multi-cloud to accelerate adoption
- Shrink attack surface to protect critical cloud-based applications

Empower App Teams

- Ensure developers integrate security controls into DevOps processes

Automate / Meet Compliance & Audits

- Prove policy controls efficacy easily with real-time and historical views
- Meet NIST 800-207 and NIST 800-53 ZTA requirements

- The threat landscape has grown dramatically, including ransomware attacks that are numerous, damaging, and costly. In most cases, these attacks use breaches from malware and lateral movements inside a flat enterprise network without trust boundaries to disrupt the most critical business services and functions.
- Solutions that require new agents can be too costly or time-consuming to provide value, and legacy firewall solutions already in use are clearly not designed or built for today's modern security problems.

Modern enterprises need a new approach that focuses on ensuring granular trust levels can be enforced continuously for applications.

vArmour simplifies your journey to Zero Trust

vArmour lets enterprises quickly resolve one of the biggest roadblocks to starting their Zero Trust journey: the ability to discover and visualize every application, every identity, and every relationship across the enterprise environment. You can't protect what you can't see, and you can't trust that which is unknown.

With vArmour, enterprises can:

- Quickly gain full and continuous observability across their hybrid cloud environments using the infrastructure already in place.
- Integrate with existing investments, ingesting, correlating, and synthesizing data telemetry using advanced ML-based methodologies. There are no agents or additional infrastructure needed.
- Gain industry-leading observability that provides quick and continuous insights from enterprise-wide to application-level views.
- Create infrastructure- and vendor-agnostic policies that will persist as workloads migrate or transform over their life cycle — resulting in the separation of control and data planes to meet NIST 800-207 and NIST 800-53 ZTA requirements.

With this deep visibility into the enterprise, vArmour helps organizations validate the accuracy of their systems of record and reconcile errors and omissions in applications, workloads, and identities.

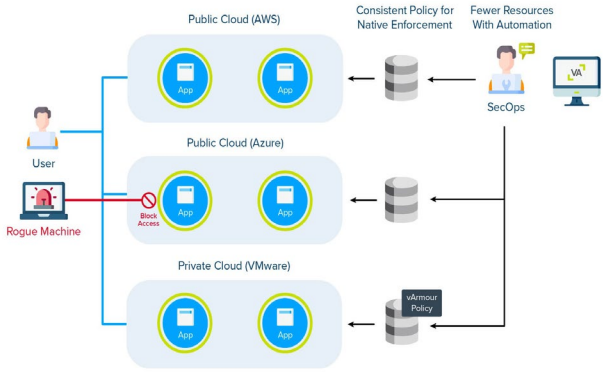

Figure 1. vArmour provides automated discovery and visibility that makes Zero Trust projects successful.

As a result, security teams can begin defining Zero Trust priorities and policies from a solid foundation. With vArmour, enterprises can:

- Compute intent-based Zero Trust security policies for critical applications or enterprise-wide
- Simulate those policies before deployment to understand and mitigate any impacts to services
- Implement in detective mode to baseline and analyze behavior using DVR-like playback capabilities, and report any violations without blocking initially.
- Automatically orchestrate the Zero Trust policies to the existing policy enforcement platforms that are already deployed.

This journey ensures that access to applications is based on least-privilege principles and prevents unauthorized lateral movements from applications to applications inside the perimeter, accelerating your cyber defenses while reducing your risk.

To learn more about how vArmour can accelerate your Zero Trust journey, please visit varmour.com.

Find out more about vArmour