vArmour Relationships Matter

Five Reasons Why Zero Trust Projects (That Failed Before) Will Succeed Today

Special eBook prepared by vArmour

Zero Trust has been a well-defined security model for over a decade now. The least-privilege concept has been around for even longer. Many regulatory bodies, such as NIST, have specified Zero Trust principles as part of the published control guidelines. But adoption of Zero Trust within organizations has been slow and uneven, despite the appeal of the principles. Why? Many organizations initiated projects to implement Zero Trust, but significant technical and operational pitfalls prevented enterprise adoption from meeting the initial promise.

Past Challenges

Previously, technical solutions for Zero Trust were too complex, resulting in projects that were less than hoped for. This was felt acutely in larger enterprises that needed to sustain many legacy applications and environments while also moving quickly to digitally-defined, modern architectures. Organizations were forced to rely on proprietary or walled-garden technology stacks from their major vendors. At the same time, they began to deploy workloads and assets in multiple clouds, resulting in environments with too many siloes and enclaves. These solutions required new agents or SDN controllers that proved too costly and complex to deploy throughout the enterprise. Poor asset inventory data quality, which impeded accuracy and effectiveness in policy creation and enforcement, exacerbated the problem.

Why Zero Trust Will Succeed Today

During the past year, enterprises have been getting more familiar with the Zero Trust security model as part of their pandemic response. Given that many organizations became fully remote almost overnight,

traditional VPN access solutions to corporate applications became unsustainable, either due to VPN license or capacity constraints, or internal bandwidth capacity limitations for network traffic. Businesses sought alternatives like Zero Trust Network Access, deployed the technology quickly, and aligned on processes, policies, and governance. Budgets for Zero Trust were prioritized as maintaining productivity across the enterprise was paramount.

Organizations are now learning that they can now realize the benefits of Zero Trust across the enterprise for five key reasons.

1

Technology Maturity:

Previous technology could not scale or perform as needed to implement Zero Trust visibility and policy computation across the entire enterprise. But recent advancements, notably in graph database technology, now make it possible to discover, model, and persist relationships between every compute node, VM, service, microservice, and function across the enterprise. From social media to financial services, graph databases and analytic capabilities have exploded. These solutions can layer in the latest AI and ML technologies to apply valuable analytics functions for more insights and better outcomes.

2

Standardized Platforms With Data Telemetry:

The adoption of standardized cloud platforms (public and private) and related advancements in agents and SDNs, have fundamentally transformed the telemetry and data equation. Enterprises no longer need to deploy and manage dedicated telemetry generation points. In fact, the challenge now is making sense of all the data generated by all these sources. Ubiquitous platforms with APIs can more easily provide the data such that upstream solutions can visualize real-time behavior and create dynamic policy controls.

3

Consistent "Evergreen" Distributed Enforcement Points:

Distributed policy enforcement points are now everywhere, from security groups in public clouds to host-controls embedded in endpoint agents. Due to the nature of these platforms, the controls are also "evergreen," meaning unlike classic perimeter firewalls, these controls do not degrade over time as their technology platforms age, thus requiring them to be periodically lifecycled. This eliminates the need to deploy and manage distributed controls as they're already there. Given modern heterogeneous environments, leveraging a single security management plane to program Zero Trust enforcement agents can be achieved without increasing complexity or requiring more segmentation-specific endpoint agents.

4

Control Plane and Data Plane Separation:

The consistent availability of distributed controls enables the separation of control plane (e.g. policy creation, governance, and assurance) from data plane (e.g. policy enforcement and instrumentation). This separation enables a scalable model that is resilient to uncontrollable changes in the underlying enterprise compute platforms, agents, and technologies. Now policies can be created in an infrastructure- and vendor-agnostic fashion, and thus, can persist as workloads migrate or transform over their lifecycle. The separation of control and data planes is a fundamental element of the NIST Zero Trust Architecture model.

5

Automation and Operations Maturity:

Infrastructure-as-code operational models, whether applied to a DevOps or a classic IT Ops model, enable a level of scalability, repeatability, and consistency to deploy distributed controls at scale. As enterprises continue on their hybrid-cloud migration journey, these tools and operational models are becoming more familiar across the enterprises. Zero Trust projects benefit from this larger organizational transformation; this enables scalable policy management without the classic overhead of legacy firewall rule changes.

Technology constraints alone were not the sole cause for failed Zero Trust projects. Operational hurdles also posed challenges. Diverse organizational roles and functions complicated the creation of end-to-end solutions, and impeded alignment on prioritization, budget, and approach. In other cases, having to refactor organizational processes, workflows, and governance was too difficult. Finally, creating and approving new security policies, especially for mature regulated organizations that relied on existing firewall rulesets, proved too challenging to overcome. These operational considerations also need to be addressed in nascent Zero Trust projects to ensure successful outcomes.

Accelerate your Zero Trust Journey with vArmour

Organizations now recognize the need to deploy new software solutions that identify, visualize and map applications, users, and relationships across all enterprise environments to begin their Zero Trust journey. They can subsequently build, deploy and enforce new Zero Trust policies to protect their applications and assets with more confidence. vArmour is a leader in an emerging category, Application Relationship Management, that provides these application visibility and security solutions to organizations around the globe. To learn more about how vArmour can accelerate your Zero Trust journey, please visit varmour.com.

Find out more about vArmour

vArmour

 | 650.564.5100 | info@varmour.com | 270 3rd Street, Los Altos, CA 94022