vARMOUR

VARMOUR TECHNICAL WHITE PAPER

DISTRIBUTED SECURITY

Executive Summary: With the shift to cloud and mobile computing, security architectures have not kept pace with modern data center architectures. In a world where perimeters have largely disappeared, organizations must embrace security models designed for cloud: distributed systems. Taking a cue from cloud architectures, distributed systems allow security to scale horizontally, adding capacity dynamically based on need. Distributed systems offer a superior architecture for security by providing simplified operations, more effective threat analysis, and better economics.

Background

Innovations in digital business, mobile, big data, social collaboration, and Internet of Things have pushed the limits on existing computing systems. As a result, organizations are transitioning to cloud architectures that are better geared to handle the new requirements for agility, scalability and flexibility.

Cloud computing architectures (whether public, private, or hybrid) offer numerous benefits over traditional client/server models: on-demand service instantiation and reconfiguration; elastic scaling of capacity; and arbitrary placement of workloads to keep physical asset utilization high, to name a few. The business value created by these benefits is transforming entire industries.

Yet security architectures have not evolved and remain dominated by legacy client/server models, monolithic proprietary hardware platforms, and workload-based software agents. These legacy security systems fall into two broad categories: perimeter-based, and host-based.

Perimeter-Based Security

Perimeter-based security systems (often referred to as network-based systems) intercept the communications between clients and servers, and interrogate that traffic for compliance with established security policies. Firewalls and IPSs are common examples of perimeter-based security.

One of the primary benefits of perimeter-based approaches is coverage. All kinds of computing systems can be protected by a firewall – whether it's a web server, a mainframe, or a piece of infrastructure. Next generation firewalls emerged to include application awareness and deep packet inspection to give companies more control over applications ingressing or egressing the perimeter while detecting malicious threats.

Historically, a challenge with perimeter models has been gaining sufficient context on the endpoint. Perimeters are far from the endpoints they seek to protect, and the traffic can be transformed or obscured in transit. This creates challenges in inspection (i.e. ensuring high fidelity in the policy evaluation to avoid false positives or negatives), and in attribution (i.e. once an issue has been identified, the ability to connect that issue back to a specific originating host).

Another common challenge with perimeter-based approaches is the requirement to modify physical network topology to ensure traffic is processed by the physical appliances providing the security services. This constraint results in inefficient network designs where functions are duplicated and computing resources are fragmented. It also results in "choke points," which creates risks of network performance, impacting congestion and resource exhaustion.

However, in a cloud world, perimeter-based approaches face even more fundamental problems. The concept of a clearly defined perimeter is rapidly eroding. When workloads are dynamically created, moved, and decommissioned, all on demand, it becomes impossible to define a perimeter in the traditional sense. This challenge is independent of whether the perimeter-based system is a physical or virtual appliance. A security model in which policy enforcement is dependent on driving all communications through a single instance is incompatible with cloud architectures. While perimeter-based approaches will continue to have a role in defense-in-depth approaches at the Internet edge, they will be challenged to meet the needs of cloud computing.

Host-Based Security

Host-based security systems typically involve running a piece of security software (commonly referred to as an agent) on the same OS running the client or server application. Anti-virus software or host-based IDS are classic examples of host-based security.

Host-based security systems have the benefit of residing on the endpoint they're protecting and, in doing so, gain additional context when compared with perimeter-based approaches. Host-based approaches also simplify workload mobility challenges created by virtualization. If a virtual machine is migrated from one hypervisor to another, all of the agents sharing that same OS will migrate with it.

Host-based approaches have some significant security design challenges, and as such have historically seen limited roll out inside data centers. While host-based approaches can be an important part of a defense-in-depth strategy, they suffer from a separation-of-duty problem. A security best practice is to maintain independence between security controls and trust boundaries. If a workload is compromised by an attacker, an independent set of security controls are required to alert on and react to that compromise. When the security controls are within the workload's 'trust boundary' (as they are with host-based approaches) that independence is lost, which limits a security administrator's ability to respond to an attack.

Another practical challenge for host-based approaches is compatibility between the security agent and the business application or workload. Because agents share the same OS as the workload, ensuring compatibility and support for the broad diversity of operating systems and compute platforms in a modern data center is nearly impossible. Whether it is legacy platforms like mainframes, vendor-specific hardware appliances, or new applications or OS versions not yet supported by the security software problem, there are inevitably critical systems that are

incompatible with a particular agent technology, thus exposing significant gaps in protection. In a cloud world, the complexity of this approach only multiplies. Variability in hypervisors, orchestration stacks, container models, and public cloud platforms add new permutations to the compatibility matrix that must be managed and maintained by not only the security vendor but also the security organization.

Finally, host-based security models are challenging for security and infrastructure teams to roll out in a consistent fashion in multi-tenant "infrastructure as a service" (IaaS) models. In both public and private IaaS clouds, the infrastructure (including security) is typically provided by the cloud infrastructure provider, while the workloads are created and operated by individual tenants (whether they be subscribers or business units). The cloud infrastructure provider has a responsibility to deliver secure infrastructure to all tenants. A host-based model that relies on all tenants maintaining the agents within their workloads is incompatible with that responsibility. A better model is for cloud infrastructure providers to implement a distinct 'security plane" which maintains an independent trust boundary, which can be called, dependent upon permissions, by either the infrastructure provider or the tenants themselves.

The Value of Distributed Systems

While the drive to cloud computing is a relatively recent phenomenon, the benefits of distributed systems have been well understood in computer science for decades. A distributed system is a single logical system, composed of multiple autonomous elements, connected through a network, that send messages to one and other. It is a very different architecture than a single-instance system, in which a single monolithic application operates independently of other components.

Distributed systems provide many advantages over a single-instanced application. Distributed systems are highly scalable and performant. They are the only way to scale capacity past a certain limit, which is why this architecture is the basis of web-scale service providers such as Amazon, Google or Facebook. Elements in a distributed system share information with each other, enabling each element to have a broader view than that provided by its specific local visibility. Moreover, distributed systems are elastic and resilient. System capacity can be expanded or reduced by adding and removing individual elements, matching capacity and availability with service demand.

Transforming Security Through Distributed Systems

While distributed computing concepts lie at the heart of cloud computing, they have not been applied until recently to information security. A distributed security system overcomes many of

the challenges posed by both perimeter-based and host-based security approaches. By distributing hundreds or thousands of security detection and enforcement elements deep down in the network to the hypervisor, top of rack, or individual VPC layer, controls can be placed directly adjacent to the individual workload for greater application context and greater security.

This model provides the independence of control and completeness of coverage benefits of perimeter-based approaches, while matching the additional endpoint context provided by host-based approaches. In a distributed system, the individual elements share information with each other over well-defined APIs, enabling aggregated threat correlation and seamless support for workload mobility and migration. In this fashion, a distributed system provides a single, logical layer of protection across physical, virtual, and cloud-based workloads. A distributed security architecture provides numerous benefits over traditional security architectures including: simplified ongoing operations, more accurate threat identification, and better economics.

Simplified Operations

Single-instance architectures impose significant capacity constraints, which can impact system availability. In a single instance system, the system capacity is directly coupled to the hardware resources available to that instance. If that system comes under attack, those underlying hardware resources will become taxed, and ultimately overwhelmed. In a single-instance model, the system has effectively been DoS'ed at that point, and the security system has been rendered inoperable (along with any workloads behind that system). With a distributed system, operating as a single logical entity, any security element in the system can take over processing responsibilities for any other. In this manner, security capacity will scale elastically based on need, making it extremely difficult to overwhelm the entire system.

In addition, a distributed security system removes much of the complexity of managing and troubleshooting traditional single-instance models. As a single logical entity, it provides a single point of manageability and control for the entire system. Policy management is simplified, as there is a global policy for the entire infrastructure. That policy is intelligently published throughout the system as required, and policy updates are automatically and instantaneously distributed to the elements. Troubleshooting is also significantly easier, as there is a single logical state table for the entire system. Responding to help desk tickets or troubleshooting policy or connectivity issues involves significantly fewer steps, as there is one authoritative point of control for the entire distributed system.

Distributed systems also allow for more flexible maintenance. Individual components can be removed for maintenance purposes, utilizing the same mechanisms employed to scale, and without impacting the functionality of the system. This capability is particularly critical in 'continuous operations' cloud environments. Likewise, the frequent needs for 'fork lift upgrades' associated with 'scale up' monolithic architectures after capacity is reached, along with the associated operational disruption, are avoided within the distributed model.

Accurate Threat Detection

A distributed system intrinsically correlates information from multiple elements across the data center, increasing the effectiveness of threat detection. With a single logical view of real-time communications across the entire data center and cloud, patterns of abuse and misuse can be readily detected that simply would go overlooked by single-instance architectures. The ability to detect such patterns is critical to the accurate identification of advanced attackers moving laterally across physical, virtual, and cloud assets across the data center.

By placing controls directly adjacent to the workload, the individual elements of a distributed system also gain better context and control over the assets under protection. Communications can be inspected before any network element transforms or obfuscates the traffic. This increases detection accuracy, as well as solves the attribution problem – that is, any incidents can directly be tied to an offending host, workload, or container. Additionally, the set of host-centric security data that require a heavy-weight agent in the workload to access is shrinking rapidly, as more workload context and business metadata is available through orchestration or configuration management databases, and as hypervisors expose more information about the state of workloads via API-based introspection.

Better Economics

The move to cloud architectures brings with it significant economic advantages not possible in traditional single-instance models. Consumption economics aligns cost to usage, which typically results in considerable reductions in the overall cost of ownership. With a software-based distributed system, service capacity is no longer held captive by the hardware that houses it.

Traditional hardware models lock capacity in a particular topological and physical location. This imposes both under- and over-capacity risks. With capacity tied to hardware, unanticipated growth in capacity requirements over the multi-year lifecycle of the hardware can result in a single appliance being overwhelmed (under-capacity risk). The natural response to

this is to over-spec a box, spending scarce budget on capacity that may never be used (over-capacity risk).

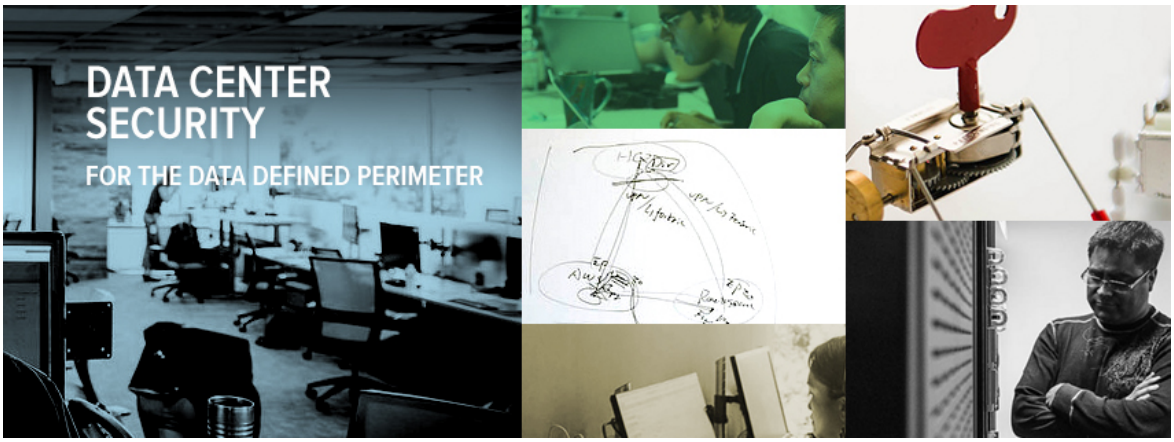
With a software-based distributed system, capacity can directly be tied to demand, lowering overall cost of ownership. These 'scale out' systems allow costs to be managed linearly and predictably based on usage and growth. Also, the economic dis-incentives to protect all assets caused by typical cost/benefit trade-offs for hardware solutions are eliminated – security can be pervasive. Security professionals are free to construct a security architecture based on the needs of the business, not the topological constraints imposed by hardware.

Conclusion

It is time for security to embrace the architectures fueling the transition to cloud computing: distributed systems. A distributed security system is a new model for security in today's modern data center that takes the best of both perimeter-based and host-based security, while adding many new architectural benefits: easier to operate, superior at detecting advanced attackers, and a better economic model for the business.

About vArmour

vArmour is transforming the next generation data center by revolutionizing how enterprises protect their data defined perimeter in the new reality of constant threats and advanced security breaches. To learn more, visit www.vArmour.com.



vArmour
800 W. El Camino Real, Suite 300
Mountain View, CA 94040
www.varmour.com