writeANGLE
Distinguishing Content

http://www.datacenterjournal.com/secure-public-cloud-oxymoron/

Why “Secure Public Clouds” Is *Not* an Oxymoron

Author: Vinay Wagh, Senior Product Manager, Bracket Computing

It’s safe to say the biggest barrier to more widespread adoption of public clouds by F500 enterprises is security—and with good reason. Concerns about unauthorized access, hijacking of accounts, data exfiltration, and the security of personal cloud storage services abound. The recent breaches at Target, Home Depot, and JP Morgan serve as grim reminders.

Aside from those headline-grabbing breaches, F500 enterprises have a fundamental lack of trust and fear of losing control when it comes to hosting sensitive data on public clouds. That’s because the long-standing paradigm for security in on-premise data centers is all about physical control that has historically functioned as the proxy for trust. But this trust model is breaking down as security best practices become logically embedded within software, which is the only way to successfully deploy ironclad protection schemes in the cloud.

Security and IT organizations need to come to terms with the fact that they no longer have direct control over the physical infrastructure of their cloud operators when it comes to securing their assets, apps, and—most important—*data* that is now distributed among private cloud, public cloud, SaaS, PaaS, IaaS, and MSP environments accessed by millions of endpoints.

Today’s new reality is that data resides everywhere. And this fact begs the question: “How do you secure highly distributed data assets in the cloud when physical boundaries are giving way to logical boundaries?”

The Need for “Data-Centric” Security Controls

CSPs have taken significant steps to successfully implement traditional data center layers of control for their cloud operations. Commonly deployed network and host-based security controls, along with visibility tools and logging mechanisms, are now built logically into software.

In spite of these best practices, however, a significant security gap remains. Conspicuously missing are *data-centric security controls* that protect data wherever it lives. Security measures must move with the data itself while providing enterprises with full independence from the underlying infrastructure provided by CSPs. In addition, these security measures must provide cloud customers with a root of trust under their direct control, as well as consistent security policies regardless of where data resides. It is no longer viable to rely on “trusted” network boundaries and perimeters, given the mushrooming volume and ubiquity of distributed data that creates growing attack-surface vulnerabilities.

Consequently, enterprises are now demanding security measures that can minimize and compartmentalize attack-surface risk down to the smallest possible target—the memory of the VM running in the hypervisor.

The Shared-Responsibility Burden

To compound matters, CSPs operate within a shared-responsibility model, which means they are accountable for the physical infrastructure they provide to customers, up to the hypervisor level. This model holds tenants accountable for properly securing their VMs, operating systems, the application layer, and associated workloads.

A real-world example that underscores the rigors of tenant accountability is the recent debacle involving Code Spaces, a code-hosting and collaboration platform, whose root credentials to their AWS account were compromised. What started out as a distributed denial of service (DDoS) attack quickly escalated to an extortion scheme. Hackers successfully penetrated Code Spaces' AWS control panel, and when the company attempted to recover access by changing EC2 passwords, the majority of data, backups, machine configurations, and offsite backups were deleted. This inability to secure root credentials resulted in the company going out of business in roughly 12 hours.

New Best Practices Are Mandatory

What this situation calls for is an entirely new data-centric security approach that offloads enterprise customers from the complexity and risk of protecting their CSP-hosted data/apps/workloads operating in a shared-responsibility cloud environment.

As a new best practice, the data-centric security model (DCSM) must deliver the following capabilities in order to make public clouds even more secure than on-premise data centers for F500 enterprises:

1. **Independence from CSP infrastructures:** Cloud customers require an independent virtualization layer that logically isolates and separates applications and data from CSPs and other tenants.

2. **Consistent security policy enforcement:** Encryption must be established as the new trust boundary. Security policies and controls travel with data wherever it goes, freeing cloud customers from the need to conform to CSP security postures.

3. **Programmability:** Essential security services—such as automated network configuration policies to ensure that no resources can ever be launched in an Internet-facing mode—must be "baked in" logically within software. Doing so ensures that all data is opaque and inaccessible, even to the underlying public cloud provider, while still allowing enterprises to fully leverage the capacity offered by cloud operators.

4. **Transparency:** Use of increasingly sophisticated key management and cryptographic segmentation that goes well beyond current offerings, without degrading application performance, is essential. In addition, end users want to focus on building applications rather than having to install, configure, and manage agent-based security solutions. Solutions that are agentless are needed to ensure that security doesn't get in the way of rapid deployment and provisioning. The best security is the kind that users never see, is always on, and is properly enforced.

5. **Customer control:** The establishment of trust anchors ensures that security enforcement remains under the absolute and direct control of the enterprise while integrating encryption and authentication with that organization's HSMs and key appliances, directory services, and certificate authorities.

The Takeaway

By applying a data-centric security model, the concept of a "secure public cloud" is now within reach. Given the shared-responsibility model demanded by CSPs, cloud customers want to achieve full sovereignty when it comes to sequestering their data—not only from the CSP, but from other tenants as well. At the same time, they don't want to be locked into a single cloud operator.

That's why a DCSM's ability to transparently enforce consistent security policies across multiple providers—without being at the mercy of the security measures of individual CSPs—is so attractive.

Finally, enterprises want to retain an authoritative grip over the control of their security destiny. And that's why a DCSM that enables enterprises to maintain ownership of trust anchors—such as key appliances, directory services, and certificate authorities—is essential.

About the Author: Vinay Wagh is Senior Product Manager at Bracket Computing. A veteran manager and engineer from Cisco and Netapp, he has extensive experience in virtualization and storage technologies as part of development teams for industry-leading products including Netapp Data ONTAP. Prior to joining Bracket Computing, Vinay architected the software and virtualization platform for the 4G LTE gateways at Wichorus, and remained through the Tellabs acquisition to lead and grow the 4G LTE team.