GuardiCore

Security Gaps Across Hybrid Cloud Environments

A Pivotal Opportunity for MSSPs

83% of enterprise workloads will be in the cloud by 2020. Conventional security measures cannot scale to this expanding environment.

Overview

Whether your customers are small businesses or vast enterprises, chances are that they will be expanding their data centers into the cloud in the very near future—if they haven't already. Cisco predicts that cloud data center traffic will represent 95% of total data center traffic by 2021.[1] The number of "hyperscale" data centers, which leverage distributed architecture and tens of thousands of servers for rapid, massive scaling, will increase from roughly 400 at the end of 2017 to 628 globally by 2021. LogicMonitor states that 83% of enterprise workloads will be in the cloud by the year 2020.[2]

This represents a huge security challenge, but also a pivotal opportunity for MSSPs. Are you prepared to take advantage of it? Do you have the right mix of security tools and expertise? More importantly, do you have the right partner to support you through this journey?

This paper explores the new security challenges created by the movement to dynamic, multi-cloud hybrid data centers—and why most conventional security measures fall short of meeting them. It outlines the evolving needs of enterprise customers in this changing environment, and how the GuardiCore solution can help MSSPs respond to those needs. Finally, it tells the story of an MSSP that has developed a groundbreaking Managed Detection and Response (MDR) program using the GuardiCore platform.

Security Challenges in a Cloud-Driven World

When a business decides to break out of the traditional on-premise data center to public and private clouds and hybrid infrastructures, its business applications will also break out from monolithic to distributed, scalable models. This trend is rapidly accelerating, due in large part to the wholesale change toward a DevOps model that requires IT and security to align to meet business objectives and drive a company's competitive differentiation. This results in an increasing number of processes running in the data center. Workloads will span physical servers, virtual machines and containers, delivering whole new levels of flexibility and scalability. With this, the complexity of IT infrastructures will also increase, with multiple tools, API's and internal protocols to support.

Perhaps the most sobering effect of this migration is a dramatically expanded attack surface. The perimeter as we've known it is no longer relevant. Conventional security measures cannot scale to this expanding environment. Data center operators are bound to lose visibility into their assets and the traffic flowing among them. With a lack of consistent security policies, any of those unmonitored servers, containers or VMs becomes a potential attack launching pad. Attackers can target blind spots in east-west traffic to land, expand laterally and dwell indefinitely. Thus, the attack surface keeps expanding every day.

[1] 2018. "Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper." Cisco. February 1. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf

[2] 2017. "Cloud Vision 2020: The Future of the Cloud." LogicMonitor. December. https://www.logicmonitor.com/wp-content/uploads/2017/12/LogicMonitor-Cloud-2020-The-Future-of-the-Cloud.pdf

Equifax Breach: Preventable

Inconsistent security controls were a major factor in the highly publicized Equifax breach in 2017 that resulted in the compromise of personally identifiable information (PII) records of about 147 million consumers. According to a US Government Accountability Office (GAO) report, the lack of segmentation and breach detection allowed the attackers to gain access to databases and to successfully remove large amounts of PII without triggering an alarm.

Source: 2018. "Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach." GAO. August. https://www.gao.gov/assets/700/694158.pdf

Securing increasingly dynamic data centers will require complete visibility into applications, workloads and underlying communications processes, combined with consistent security policies and continuous monitoring for compliance and breach detection.

The challenges don't end there. Security Operations Centers (SOCs) will need the ability to detect and stop lateral movement of attacks inside the hybrid infrastructure. They will be challenged to find the right mix of skills and tools to achieve this extra layer of protection and monitoring, particularly in view of the shortage of security skills on the market. Meanwhile, hundreds of security vendors with widely disparate offerings claim to deliver complete security solutions. If even fully staffed, large enterprises are daunted by this challenge, imagine the impact on small and medium-sized businesses lacking the in-house skills and resources to undertake such an effort.

So what does all this mean to Managed Security Services Providers? The MSSP market is growing, projected to surpass $45 billion by 2022, according to Market Research Engine.[3] At the same time, the market is saturated. It's become harder for many players to differentiate their offerings and maximize their value to clients. Companies often switch vendors quickly when their satisfaction level drops. MSSPs need to be able to demonstrate to clients and prospects that they understand this changing environment, and that they have the right technologies to help enterprises confidently and securely migrate to the cloud. MSSPs who are able to successfully deliver will gain a critical and strategic competitive advantage.

Evolving Customer Needs: What Companies Are Looking For

In light of these trends, the security needs of enterprise customers are changing. So are their expectations of managed security providers. Increasingly, customers expect their MSSPs to have:

1. **The ability to deliver deeper and broader security coverage, beyond traditional SIEM as a service, patch management and host-based security.** Clients are looking to consolidate the number of single-product vendors they work with in favor of a platform approach.

2. **Consistent visibility and security controls across hybrid cloud environments.** Enterprise customers often rely on their cloud providers' native security controls. However, as workloads and applications migrate among different cloud instances, security measures that work in one cloud provider's environment will not work in another.

[3] 2017. "Global Managed Security Services Market By Verticals Analysis (BFSI, Telecom & IT, Government, Retail, Energy and Power, Healthcare, Industrial Manufacturing); By Service Analysis (Threat Management, Incident Management, Vulnerability Management, Compliance Management); By Deployment Analysis (On-premises, On-demand) and By Regional Analysis—Global Forecast by 2016–2022." Market Research Engine. April. https://www.marketresearchengine.com/Managed-Security-Services-Market

3. **The ability to reduce false positives, accelerate response time and increase SOC efficiency.** A study by ATA Analytics, reported in InfoSecurity magazine, found that MSSPs are spending as much as five hours or more a day investigating security alerts, most of which turn out to be false.[4] This enormous waste of time and resources affects security effectiveness—many incident responders cope with this problem by either reducing the sensitivity of threat detection tools or simply ignoring alerts.

4. **The ability to address compliance as a part of the security-as-a-service offering.** In particular, Payment Card Industry (PCI) and SWIFT regulations include requirements to isolate transactional environments and applications from the general IT environment. This becomes increasingly difficult as those applications move into the cloud and out of the defined compliance framework. To achieve compliance, MSSPs and their enterprise customers must be able to apply compliant security controls consistently and seamlessly, regardless of the environment in which the applications are actually deployed. This is a major challenge, especially when security teams find themselves running behind application DevOps teams that are continuously launching containerized applications into the cloud without proper compliance measures in place.

Dwell Time = Millions Lost

SOC inefficiency played a role in the success of attacks on Mexico's SPEI system (the country's equivalent of the SWIFT interbank payment system). These attacks, reported in May 2018, resulted in losses of $18 to $20 million. Experts concluded that the attackers penetrated the network and dwelled within it for an extended period of time, long enough to collect authentications and observe the member banks' transaction and approval processes. Reliance on perimeter firewalls and the inability to distinguish between authorized and unauthorized activity inside the network allowed the attackers to maximize dwell time, move laterally and access network resources at will.

Source: Seals, Tara. 2018. "Mexico's Banking System Sees $18M Siphoned Off in Phantom Transactions." *Threatpost*. May 15. https://threatpost.com/mexicos-banking-system-sees-18m-siphoned-off-in-phantom-transactions/132004/

The GuardiCore Solution: Mastering Security in the Dynamic Data Center with Network Visibility, Micro-Segmentation and Automated Breach Detection and Response

GuardiCore is uniquely positioned to equip MSSPs with the tools to overcome these challenges and deliver on evolving customer demands. The GuardiCore Centra™ Security Platform is a comprehensive security solution for today's dynamic, hybrid cloud data centers. It provides advanced micro-segmentation capabilities for securing assets across heterogeneous data center environments, supported by deep visibility into traffic flows down to the process level. It also provides multiple methods of automated breach detection and incident response, including dynamic threat deception, that dramatically reduce an attacker's dwell time. With real-time, high TP (true positive) alerts on breach attempts, policy violations and known or unknown zero-day attacks, teams can swiftly detect, confirm, respond to and mitigate any live breach and internal threat directed at data center assets.

With built-in visualization, GuardiCore Centra provides graphic visibility into all data flows between data center assets, be they bare metal, virtual machines or containers, as well as the processes responsible for them. Security teams can see both successful flows and failed connections, along with attacks directed at the platform's deception servers—both in real time and in historical views. This enables analysts to review all flows down to the process level on every protected asset in real time and compare traffic against historical time frames.

[4] Seals, Tara. 2018. "MSSPs Waste Hours of Time on False Alerts." *Infosecurity Magazine*. February 12. https://www.infosecurity-magazine.com/news/mssps-waste-hours-of-time-on-false/

The comprehensive visibility provided with GuardiCore Centra enables a flexible and accelerated approach to micro-segmentation. The largest, most complex carrier grade environments can be easily navigated, reviewed and analyzed. Application dependencies are easily defined, labeled and micro-segmented in an intuitive process that dramatically reduces the attack surface and risk profile for each discrete client environment. This same set of capabilities can also be applied to meet compliance, and to more easily manage the ongoing security posture, as teams are able to assess and document real-time and historical application workflows.

With advanced filtering and time-based drill down capabilities, teams can quickly research and investigate connections and actions that occurred around the time of an incident, and trace events all the way back to the first step of an attack. This enables security professionals to more readily understand attacks, their origins and lateral movements, and to quickly detect the assets infected. The same filtering capabilities enable searching for specific indicators of compromise (IoCs) across the whole data center to detect infections.

GuardiCore Centra is the only security platform that provides integrated security controls for dynamic data centers and hybrid clouds. In doing so, it multiplies the effectiveness of security teams, enabling them to respond more quickly to incidents, armed with more thorough knowledge and information about the attack.

Case Study: Revolutionizing Security-as-a-Service Delivery

Blue Bastion, the cybersecurity division of Pittsburgh-based Ideal Integrations, delivers Managed Detection and Response (MDR) services that help its customers defend their most critical business assets around the clock. The MDR program is built on a unique approach that combines a diverse arsenal of security measures with a highly trained and talented team of security professionals that monitor high-fidelity alerts and vulnerabilities continuously.

Blue Bastion has revolutionized the delivery of security-as-a-service by introducing foundational security controls for the protection of assets within dynamic data center environments. Using the GuardiCore platform, Blue Bastion deploys micro-segmentation controls that enable its own security analysts as well as its customers to:

- Create and monitor a comprehensive visual map of all applications and activity inside the data center, allowing visibility into all workloads and a full understanding of application-layer communications
- Filter and organize applications into groups and label them for the purpose of setting common security policies—for example, all applications related to a particular workflow or business function
- Define and create rules governing authorized communications between applications
- Test and refine those rules to ensure they are not disrupting normal, authorized traffic

"We knew we needed additional controls and tooling that we could use to shrink the risk surface, monitor for unauthorized lateral movement, add an element of deception and increase the fidelity of alerts. GuardiCore was the only platform we tested that gave us everything we needed to fill those gaps."

—Corey Bussard,
Manager of the Blue Bastion SOC

The GuardiCore solution makes it possible to create strong micro-segmentation policies in a matter of minutes per application. Alerts triggered by these policies are focused only on non-compliant traffic, thereby reducing the volume of alerts and limiting them to cases in which a policy has been violated, indicating a likely threat. Policy-based detection helps the Blue Bastion team detect, confirm and contain threats quickly to prevent damage and minimize losses. These granular security controls do double duty, preventing an intruder from gaining malicious access to an application or process while simultaneously alerting administrators to the intruder's presence. GuardiCore automatically blocks unauthorized communications and directs threats to a quarantine sandbox for investigation, enabling a swift, real-time response that prevents attackers from reaching their goals.

In contrast, using only a SIEM, it is difficult to ascertain quickly whether an anomaly represents a true threat, and, if so, the level of the threat in question. "Our team routinely receives alerts related to reconnaissance traffic, testing perimeter security controls, and even attempts to brute force systems," says Corey Bussard, Manager of the Blue Bastion SOC. "While we monitor all of these very closely, asking our team to chase all of them to a final end-state is not realistic. We knew we needed additional controls and tooling that we could use to shrink the risk surface, monitor for unauthorized lateral movement, add an element of deception and increase the fidelity of alerts. GuardiCore was the only platform we tested that gave us everything we needed to fill those gaps."

According to Bussard, leveraging GuardiCore in conjunction with a SIEM has been so effective that it has allowed his team to boil 100 alerts down to one. "We make it a point not to knee-jerk react to every alert coming from the SIEM, especially those associated with typical perimeter recon and surface attacks. Instead, we keep an eye on those while also watching for unauthorized lateral movement via GuardiCore. We know if we see an attack followed closely by lateral movement, we have something we need to jump on directly."

The high fidelity of incident alerts from GuardiCore has also helped reduce the burden of "alert fatigue" that often affects cyber analysts working in 24x7 SOCs. The increased efficiency allows Blue Bastion to support more customers with a smaller team, making its MDR program economical and cost-effective for a substantial segment of the marketplace.

Dynamic Deception Strengthens Breach Detection

GuardiCore employs a dynamic deception technology in which attackers are redirected automatically to a decoy based on suspicious failed network traffic. An automated analysis tool analyzes every redirection and distinguishes between low severity events and real incidents. GuardiCore monitors the attacker's activity inside the deception server, registering every operation and system call in a transparent fashion so that the attacker is unaware that they are being monitored.

GuardiCore Fulfills the "Must Have" List

In selecting the technology to bolster its MDR offering, Blue Bastion set forth a list of "must-haves" that included:

- Maximum visibility (preferably up to Layer 7) for data centers and public clouds
- Real-time detection of lateral movement
- Threat intelligence and reputation feeds
- Micro-segmentation capabilities to shrink the attack surface and prevent compromise of assets
- Support for multi-customer deployments, allowing end customers to control some of the functions within the platform

Blue Bastion discloses the attacker's TTPs and performs complete IoC collection, turning the data collected into actionable alerts and intelligence. This ensures that every alert is real, with a very low rate of false positives. The alerts generated include detailed analysis and forensic information, explained in natural language, while providing forensic evidence and artifacts. These easy-to-read alerts simplify detection and threat hunting.

By combining highly interactive deception, analysis of every failed connection, and automatic redirection with complete monitoring of the attacker's actions, Blue Bastion is able to leverage highly accurate intelligence and reduce the rate of false positives without missing attacks. This allows more efficient and effective deployment of highly skilled security analysts across multiple sites, which translates to maximum value for customers.

Increasing SOC Efficiency with Built-In Reputation Analysis

GuardiCore's reputation analysis capability is aimed at identifying threats based on suspicious domain names, IP addresses and file hashes associated with known malicious activity. Non-conforming or unauthorized communications are indicators of compromise—for example, malware installed on a server and attempting to communicate with a known bad IP address or domain name. The Blue Bastion service leverages GuardiCore's vast network of attack sensors and deception engines, combined with regular threat intelligence feeds and the insights of GuardiCore security analysts to identify "good" and "bad" IoCs, indicating the presence of untrusted activity that warrants investigation. In combination with dynamic deception, reputation services provide real-time alerts with an extremely low false-positive rate, leveraging insights that include detailed information about the attack.

Why Blue Bastion Chose GuardiCore

The GuardiCore Centra platform with GuardiCore Reveal™ visibility serves as the centerpiece of Blue Bastion's technology tool set. The firm uses GuardiCore to bring visibility to customer data centers and cloud assets that had been previously lacking, and to implement micro-segmentation to protect against unauthorized lateral movement.

In selecting the technology to bolster its MDR offering, Blue Bastion set forth a list of "must-haves" to drive its comparison of vendors (see sidebar.)

GuardiCore was the only vendor with a platform that delivered on all of Blue Bastion's requirements, with the added benefit of dynamic deception. "It was either GuardiCore or a stack of technologies from two or three different manufacturers," says Bussard. "That wasn't going to work for us."

The Right Partner Makes the Difference

The marketplace for managed security services is changing quickly. The movement of traditional data centers to hybrid cloud infrastructures poses new and more complex challenges for enterprise customers who need to secure their valuable assets. Conventional perimeter defenses won't protect workloads and applications as they migrate among multiple cloud environments. Those assets become ripe targets for attackers who have become adept at exploiting a critical blind spot in data center defenses, namely lateral traffic movement. Security professionals need to shift their attention to protecting the assets themselves within the data center.

MSSPs with the agility to pivot toward these challenges stand to gain a significant competitive advantage. The trick is having the right answers, the right tools and the right partner. GuardiCore has spent years honing a solution set uniquely designed to address changing data center security requirements—the industry's only integrated platform encompassing micro-segmentation, threat detection and incident response. As the Blue Bastion experience demonstrates, partnering with GuardiCore is a way for an MSSP to quickly add significant value to its offering, and deliver the combination of deep visibility, process-level protection, SOC efficiency and compliance readiness that enterprises demand today.

About GuardiCore

GuardiCore is an innovator in data center and cloud security focused on delivering more accurate and effective ways to stop advanced threats through real-time breach detection and response. Developed by the top cyber security experts in their field, GuardiCore is changing the way organizations are fighting cyber attacks in their data centers and clouds.

More information is available at **www.guardicore.com**