GuardiCore

White Paper

New Strategies for Breach Detection and Security in the Software-Defined Data Center

In today's fast-expanding, dynamic data centers, the problem of malicious intrusion is growing apace.

The list of security vulnerabilities is long and worrisome: rising rates of cyberespionage; increasingly sophisticated malware; infiltration of industrial systems and other sensitive targets; relentless campaigns of spear-phishing, watering-hole, perimeter reconnaissance, and zero-day exploits; rising success of breaches and data theft.

New generations of ingenious worms, viruses and trojans burst into the headlines every month. Times elapsed from exposure to patch are lengthening as well, allowing damage and losses to accrue.

The virtualized software-defined data center (SDDC) is now a prime target for infiltration and attack, opening up a whole new front in this endless cyberwar. Explosive server workloads and VM sprawl have resulted in a massive upward scaling of the security coverage challenge.

Data center security has come under increasing pressure as hackers, both private and state-sponsored, try to engineer, force, or deceive their way past the perimeter's defenses and into the heart of an organization's information technology.

Responding to the urgent need for a fresh approach to security, the GuardiCore team developed a solution that actually uses the very strategies of the attackers against them. The GuardiCore solution enables a new dimension of instant, deep visibility and insight for detection, exposure, and identification of an attacker. Real-time, insightful analysis leads to quick remediation and minimizing of damage.

"Over 70% of data centers are attacked each year [and] up to 80% of inter-VM traffic never reaches the physical network for monitoring."

- Corvil, "Monitoring in a Virtualized Data Center"

Data Center Virtualization Opens Up New Horizons and New Security Challenges

The unfolding story of virtualization is exciting and open-ended in terms of cost-efficiency, performance, and revenue potential. But the bright story loses some of its shine when it comes to security. Virtualization and SDN, along with data center consolidation and ever-increasing speeds—all make the data center a challenge to protect. Because it is a treasure trove of proprietary, sensitive information and represents major capital value for a company, the data center becomes "big game." It's a tempting target for attack, whatever the arena: financial, manufacturing, healthcare, utilities, governmental, education, service provider, or others.

The distributed structure of the data center, with its interconnected applications, make security gateways ineffective. The vast numbers of vulnerabilities are exacerbated by a persistent lack of visibility, which has always trailed virtualization advances. Thus, applications running on virtual servers are subject to the same manner of threats as those running on dedicated servers, but decreased visibility in the virtualized environment raises the risk of intrusion substantially. Any visibility "blind spot" is a welcome mat for attackers.

The exploding volume of "east-west" [server-to-server) traffic, with hundreds and even thousands of sprawling virtual machines (VMs) migrating in a data center, plus cloud computing itself, makes the scale of the challenge enormous. With the high density of virtual servers on a single hypervisor, even identifying which virtual servers are running on a given hypervisor becomes difficult. It's clear that for administrators to respond effectively to attacks they need the resources to automate the security lifecycle. Add to this the fact that network and data center breaches can take months and even years to detect; and that even after the breach is identified, it can go on accruing damage—and the consequences of an attack grow severe.

Defending the Data Center from Attack: "Catch Me If You Can"

Frequent headlines keep the dismaying outcomes of security failures in the public eye, although many failures are not reported. Even a smaller-scale failure drains funds and damages efficiency and productivity. Today's software-defined data center (SDDC) is agile, dynamic, elastic and flexible. This fast-moving environment is proving unsuited by its very nature to many detection solutions. That means the structure and behavior of the SDDC itself works against the anomaly-detection model used by traditional security solutions.

While firewalls and ACLs may be scalable enough to support soaring traffic rates, highly compute-intensive resources such as IDSs, IPSs, and sandboxing can be expensive and consume large amounts of resources and personnel, making them impractical to implement.

Perimeters are the first line of defense, but over 80 percent of traffic passes into the data center. Endpoint security cannot defend against intentional or unintentional malicious actions once inside. The data center needs the Intelligence to understand and thwart illicit activity within that perimeter.

Attackers thrive on secrecy. As long as an attack goes undetected by security resources, the attacker can not only invade and steal data, but also learn the

SNAPSHOT

How Vulnerable Are Today's Data Centers?

37% have adopted Data Loss Prevention and whitelisting technology

35% monitor traffic between key servers and their clients in the data center

53% have dedicated compliance and security staff for their data center operations

>60% have even partially automated key database security and compliance functions

49% can investigate and remediate incidents within eight hours

90% use cloud-based data center technology for their operations

Top methods for detecting incidents:

Manual log review (43%)

Administrator hunch (42%)

Perimeter firewall / IDS/IPS (41%)

SIEM alerts (41%)

SANS 2014 Data Center Security Survey

systems, architecture and defense strategy of the data center for future attacks. Attackers also behave differently inside the data center, constantly seeking ways to penetrate and bypass perimeter security. Therefore, the ability to identify and gain insights on the attacker and source of the attack is vital for defenders to gain the leverage for protection.

Needed: A Comprehensive Solution to Identify and Mitigate Data Center Security Breaches

As more enterprises rely on data centers and virtualized environments, the need is urgent for effective security within the enterprise perimeter. This need has driven and informed GuardiCore's mission to defend the data center interior. The solution that GuardiCore developed is now changing the way enterprises identify and secure that 80 percent of traffic inside the data center. GuardiCore technology picks up where traditional firewalls leave off, to detect malicious activity, decoy attacks and deliver ironclad security.

"Acknowledge that not all threats can be prevented, and therefore, the speed to detect and respond to incidents is also critical."

- Gartner, *Best Practices for Detecting and Mitigating Advanced Persistent Threats*

The GuardiCore Data Center Security Suite Transforms Security Within the Perimeter

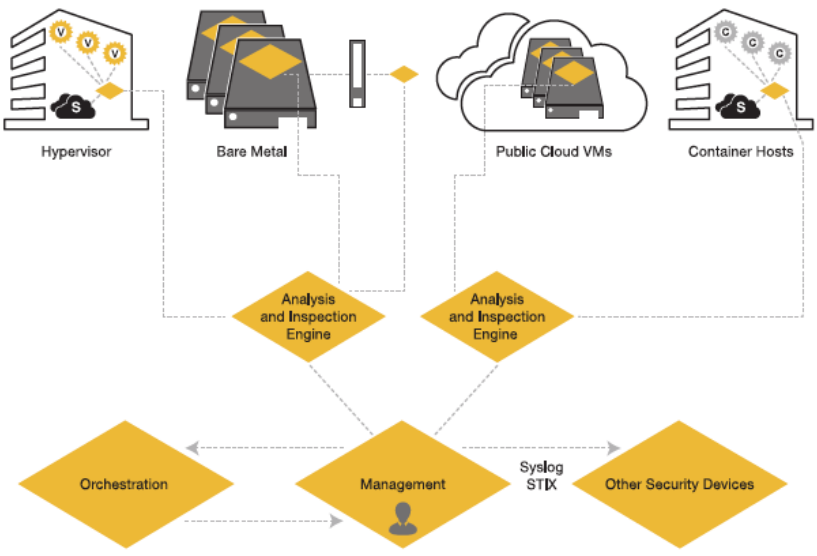
In developing its new data center security approach, GuardiCore's team of top security experts focused on the fact that data centers were the first to adopt Software-Defined Networking (SDN) and are already virtualized—therefore, they need an SDN-driven security infrastructure.

GuardiCore's unique ability to protect multiple environments in one solution

The innovative **GuardiCore Data Center Security Suite** utilizes distributed detection complemented with multiple types of sophisticated investigation capabilities, providing the high scalability for large networks and high traffic rates. The Suite is built in an open fashion and integrates with third-party solutions using Syslog, STIX and REST API.

Supports most data center architectures and networking topologies, including:

- Virtualized environments: ESX, NSX, OpenStack, CloudStack
- Physical/bare metal data centers
- Hybrid data centers
- Public clouds: Azure and AWS
- Internet facing threat deception honeypots
- Internal networks via direct routing, sinkhole gateways



Distributed Detection, Centralized Analysis, and Fast Response

GuardiCore's technology sits on the hypervisor—ideally positioned for monitoring what is happening within workloads. This ability to monitor process-level communication patterns closes the loop between the process application and network activity.

GuardiCore's inner breach detection technology embodies advanced techniques to discover and scope illicit activity and identify security breaches within the data center. It spots anomalies, irregular patterns and suspicious, ongoing, spreading attack processes. Then, it sends suspicious traffic for centralized analysis in order to quickly identify the attacker and grasp the nature of the attack.

The GuardiCore technology is able to:

- **Detect high risk usage,** illicit activity, including backdoor installations, password harvesting, running exploits, policy violation, multiple connection attempts throughout the data center, manipulation of log files and attack tools.
- **Identify behavioral breaches** via hypervisor introspection, which monitors connections between any process, network flow, or virtual machine. It actually manages behavioral baselines of approved activity, and quickly identifies deviations.
- **Scope the impact and footprint** of breaches across ALL data center environments— virtualized and hybrid servers, all hypervisors, containers, bare metal environments and public clouds.
- **Scalably detect breaches** across servers, virtual environments and traffic volumes.

Distributed, Automated Deception Snares the Attacker–Identity, Tactics, Footprint, and Source.

The GuardiCore solution uses significantly deepened deception technology to lure and capture an attacker in the context of workload traffic. Data center security personnel can then examine and understand the exact nature of the attack—where it originates, who is behind it, and which strategy it is using.

Gartner recently listed GuardiCore as the only vendor covering the entire deception stack, noting that GuardiCore's "distributed decoy solutions offer enhanced detection and stronger fidelity than other traditional security solutions."

> *" Deception as an automated responsive mechanism represents a sea change in the capabilities of the future of IT security that product managers or security programs should not take lightly."*
>
> - Gartner, *Emerging Technology Analysis*, July 2015

Hackers Study Their Failures–while GuardiCore Studies the Hackers

A data center often lets a blocked attempt end right there—complacent that the attack has failed and they are safe. Unfortunately, the hackers send rapid fusillades of new attacks to gain a "picture" of the network's defenses. So, by not pursuing the blocked attempt, the data center's defenders lose a prime opportunity to gain deep information about the attacker and type of attack.

Blocked Attack Triggers Investigation, Analysis and Exposure

A failed attack is just the starting point for GuardiCore to capture the attacker's identity. Since GuardiCore's proprietary technology connects to physical switches and sits on virtual switches, it is ideally positioned to watch for these attempts and take immediate action. The hackers are quickly under surveillance, and the GuardiCore technology begins analyzing and reporting on their tactics, who they are, and where they come from.

Block-and-Investigate Process: a Next-Generation Honeypot Approach

When an attacker is blocked by a firewall inside the data center, for example, GuardiCore is then able to answer seamlessly on behalf of the server—using a "fake" virtual machine. As the attacker tries to connect, GuardiCore automatically and transparently redirects suspect traffic to a highly monitored decoy environment to isolate and investigate. Active Honeypot instance isolation provides full visibility into the attacker's activity and prevents the attacker from using the honeypot as a launchpad to further attack the network assets. All this is achieved by automated creation of virtual IPs distributed across the host network. No active sessions are disrupted as the solution captures and isolates suspect activity in place.

> *" High interaction honeypots interact with the attacker, enticing him to do things that will lead to profiling the attack or the malware. If you are looking at deception technology be sure that you see high interaction."*
>
> - SC Magazine, *Emerging Products: Active Breach Detection*, February 2016

How Do Hackers Invade?

It's been said that defenders must succeed 100 percent of the time, while attackers need to be successful only once.

The law of large numbers is on the side of the hackers: out of hundreds or thousands of attempts, it's just a matter of time until even the best defended data center will be breached. One or two spear-phishing emails are sufficient to begin a costly,even catastrophic attack.

Once the hackers are inside, they look for opportunities to use tools they've created in advance. They probe for vulnerabilities to break through the data center's protocols. They may try to move laterally within the data center to identify the next target, and more subsequent targets.

When hackers try to connect to a server and are blocked, they re-use credentials in a constant trial-and-error attack to learn the patterns of blocked connections and create a map of the network.

This is why a security solution must be even more deceptive and sensitive than the hackers themselves to optimize visibility and capture the hackers' identities and information.

Identification of Compromise

With its state of the art semantic analysis capabilities, the Data Center Security Suite executes state-of-the-art detection methods on all traffic targeting the Honeypot to detect further malicious activity—even before the attacker can penetrate the Honeypot instance.

GuardiCore's Identification of Compromise (IOC) process collects the attack footprint; the files and tools being used and uploaded; and the arsenal of weapons that the intruder activates. The attackers still believe they have succeeded—even as GuardiCore is automatically gaining their complete attack footprint. The solution semantically analyzes and records information, including screen captures. It gathers attack characteristics using deep forensics to expose user credentials, tools, methods, propagation tactics, and more. In fact, GuardiCore takes over the attacker's entire process, including their uploaded files, backdoors and registry keys. This information lets GuardiCore search for any additional areas attacked or breached within the data center. The attackers are completely revealed and under scrutiny all this time not being suspicious of anything.

The security administrator can now take action and identify where within the data center the attack was attempted. Since most administrators are not forensics experts, this automatic process reduces detection time. Now the administrator can understand very quickly what has happened, how the attack works, and what to look out for. The Suite extracts the attacking process during interaction with the Active Honeypot, using it as part of the IOC that should be searched out. The GuardiCore solution, from where it sits on the hypervisor with access to the servers, will instantly and automatically quarantine the attack and block it from further spreading. Meanwhile, the attackers remain deceived and execute all further commands harmlessly from the shell that they connected to, still with no idea that they are being tracked.

GuardiCore Revolutionizes Data Center Security

To date, security has been a battle with few clear-cut victories over proliferating, persistent, globally situated attackers. Now, GuardiCore technology enables security administrators to catch and disable attackers before they wreak their damage.

GuardiCore's solution fully covers and supports all data center infrastructures, automating attack detection in real time in their earliest phases. GuardiCore interrupts hackers' lateral movement, using ingenuity, deception, and deep analysis to capture a complete, detailed footprint and stop the attack in its tracks. Cost-effective and non-disruptive, the GuardiCore Data Center Security Suite enables long-sought visibility into the virtualized data center, so that security teams quickly receive the critical information they need to thwart attacks.

DID YOU KNOW?

"False Positives" versus True Attacks

Built into the GuardiCore solution is the intelligence to safeguard against "false positives" such as configuration errors.

If an anomaly is simply a configuration error, i.e., one machine or a person trying to connect to another that does not exist, the result of the semantic analysis will not generate a security incident.

If the event is indeed a worm or other cyber weapon, it will try to propagate and infect the machine. Real attackers will also try to perform additional tasks such as log tampering.

The GuardiCore solution has the capability to analyze and differentiate between a true attack and a non-issue. (Of course, any anomaly or abnormal function is worth investigating.)

The GuardiCore solution is always in control, and the security of the data center is.

About GuardiCore

GuardiCore is a leader in Internal Data Center Security and Breach Detection. Developed by the top cyber security experts in their field, GuardiCore is changing the way organizations are fighting cyber attacks in their data centers.

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