Guardicore

PROTECTING WORKLOADS IN HYBRID AND MULTI-CLOUD ENVIRONMENTS

White Paper

PROTECTING WORKLOADS IN HYBRID AND MULTI-CLOUD ENVIRONMENTS

In seeking innovation, competitive advantages and efficiencies, enterprises have moved into a DevOps based Cloud infrastructure model. As such, they have increased enterprise IT speed and agility in ways we've never seen before. Many organizations now use public cloud infrastructure and new deployment approaches like containers and serverless. By embracing this new model, the latest cloud computing technology is dramatically accelerating the pace of change. These practices allow workloads, applications, and even environments to be automated, auto-scaled, migrated, and more. The resulting competitive advantages are powerful.

At the same time, some legacy services and systems, like traditional data center infrastructure, remain in use. Companies might be in the process of removing or modernizing them, but the systems inherently still exist because they hold business-critical applications and workflows.

Traditional security techniques are not effective in hybrid and multi-cloud environments

Furthermore, traditional security techniques have not been able to keep up with the pace of change that opens up the question of how to protect cloud workloads in these new hybrid cloud and multi-cloud environments. Beyond speed, perimeter-based security is no longer effective when the vast majority of traffic is taking place inside the cloud or data center (east-west) as opposed to from outside (north-south). This transformation also forces IT executives to rethink their security playbook.

In fact, no traditional cybersecurity models were built with Infrastructure as a Service (IaaS) in mind. The public cloud needs new strategies based around its own unique challenges.

Enterprise security must evolve to support the new business environment. Organizations have made dramatic changes already to satisfy business requirements and agile working methodology. Security has been left behind despite massive investment made.

The reality is that spending money on solutions that were developed without the cloud in mind is a mistake. It does not help detect and prevent today's - or future - breaches. So how can you consume public-cloud services and enjoy the benefits of speed and agility, without compromising the protection of critical data?

THE MODERN, HYBRID CLOUD DATA CENTER

On-premises data centers aren't going anywhere any time soon - **98% of enterprises run on-premise servers**

The makeup of the modern data center, granularity of workloads, and speed of development are changing rapidly. A typical modern hybrid data center is composed of workloads running both on-premises and in public cloud / IaaS, using multiple vendors and utilizing Platform as a Service (PaaS) either on-premises or in the cloud. The amount of workloads running in the public cloud continues to grow. Simultaneously, on-premises data centers aren't going anywhere any time soon. Case in point - a recent survey of CIOs by Spiceworks found that 98% of enterprises run on-premise servers.[1]

Enterprises are increasingly adopting DevOps practices and improving agility. Native-cloud services and serverless technology are becoming easier than ever before to implement. Using a combination of containers, VMs and serverless in the cloud can be cost-effective and transformational from a strategic point of view.

Security needs to fit into this hybrid cloud paradigm. Businesses need to address security at every stage of the DevOps process, from testing, building, and planning, to monitoring, operating, deploying, and releasing new features. Hybrid cloud data centers cannot be stumbling blocks that prevent success.

Distributed workloads are not well secured, limiting new cloud technology usage

Most enterprises have to protect workloads that are distributed across on-premises, co-location and multiple public cloud / IaaS platforms. They are struggling to keep these workloads secure with traditional on-premises network security models.

Matters are made more challenging when you attempt to deploy new cloud based tools and techniques to secure the new cloud technologies. The levels of complexity multiply, as businesses attempt to enforce different security controls in different environments and introduce risk by deploying these controls without adequate visibility.

In other words, the cloud, which is meant to make enterprises more dynamic, agile, fast and innovative, is now putting many organizations at risk. With a lack of relevant cloud-focused security tools, enterprises are limited in their ability to embrace this new technology without causing blind spots and more challenges.

That's where adaptive workload protection comes in.

[1] https://community.spiceworks.com/blog/3182-the-2019-state-of-servers

THE SHIFT TO IAAS DRIVES THE NEED FOR ADAPTIVE WORKLOAD PROTECTION

Cloud Workload Protection Platforms (CWPPs) support platform-agnostic workload-centric security solutions

The best way to secure granular workloads with short lifespans is with dynamic application of protection as soon as the workload is in use. Workload-centric solutions are far simpler for enforcing security policy than traditional network security models when it comes to public cloud infrastructure.

As a policy follows the workload - independent of the underlying infrastructure - the model can be applied to all workloads across the entire hybrid cloud data center environment. The result is a consistent, platform-agnostic approach to security controls.

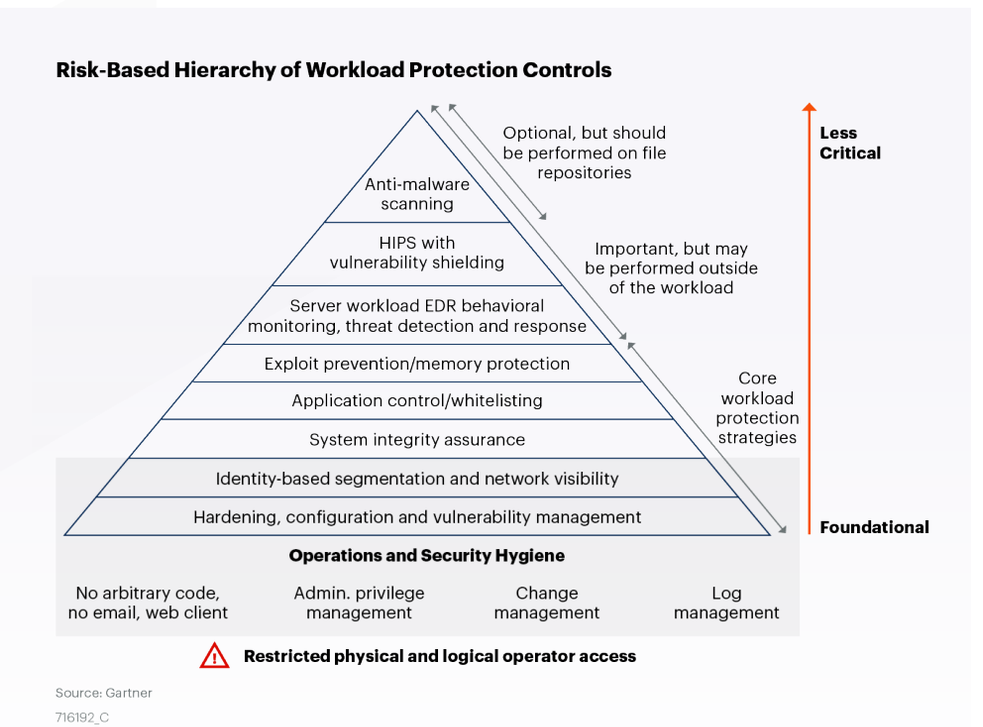
While there are native-cloud security tools, adaptive Cloud Workload Protection Platforms (CWPPs) provide more comprehensive, granular control at the process, user, and fully qualified domain name levels. They also work across multiple cloud providers and on-premises, supplying stronger and more comprehensive protection for virtual machines, containers, and serverless workloads.

ACTIONABLE CORE WORKLOAD PROTECTION STRATEGIES: MAPPING CONTROLS TO GARTNER'S CLOUD WORKLOAD PROTECTION GUIDELINES

Gartner's Cloud Workload Protection guidelines provide a clear hierarchy of security controls for enterprises

One of the most widely followed guidelines for Cloud Workload Protection is written by the industry experts at Gartner. According to Gartner, there is a clear hierarchy of controls when protecting cloud workloads.

The pyramid below moves from foundational to less critical, showing the strategies Gartner considers to be core, as well as those that are important but optional. Ideally, these steps should be included in each workload, ensuring that security is built in for each action on the cloud.



Risk-based Hierarchy of Workload Protection Controls - Source: Gartner[2]

Here's an expanded explanation of the points in the graphic above, to help you figure out how best to incorporate these strategies into your hybrid cloud or multi-cloud data center protection program.

[2] Market Guide for Cloud Workload Protection Platforms; written by Gartner analysts Neil MacDonald and Tom Crow; published 14 April 2020; ID G00716192; https://www.gartner.com/en/documents/3983483

1. Hardening, Configuration, and Vulnerability Management

According to the Gartner, the most foundational workload protection strategy is to configure your systems and settings appropriately to reduce risk. Vulnerability management tools take the manual removal of attack vectors a lot further and automate this process. You can then find and solve software issues that could open doors for malicious intent.

2. Identity-based Segmentation and Network Visibility

Gartner highlights network segmentation and visibility as core strategies for cloud protection. Most organizations are using next-gen firewalls on-premises, yet many accept a less secure solution when they move to the cloud.

Security teams understand that next-gen firewalls are insufficient for cloud protection, but don't know how to achieve heterogeneous insight or control in a dynamic, hybrid data center environment. So let's take a moment to go over how to do it right.

First, establish visibility. Quick visibility results in faster time to value, as all stakeholders are immediately and automatically on the same page.

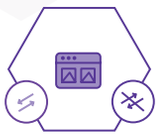
Native cloud tools may provide snapshot maps or textual logs, but these are generally dense, incomplete, or insufficient. The best micro-segmentation technology automatically discovers all applications, traffic, and dependencies in your network. That way, you can see at a glance your whole IT ecosystem, even when your enterprise works in a hybrid way.

Your micro-segmentation solution should include powerful context, with strong insight into the true picture of what's happening in your data center. For any enterprise looking to manage security operations and inquiry at scale, every flow needs to have this context. That enables data-driven decision making that bolsters policy creation.

After you establish visibility and context, create segmentation rules that fit best practices for your business. For example, you may want to separate Production and Development environments or isolate customer data to prove compliance. You can also develop other policies that suit your specific business context.

3. System Integrity Assurance

To ensure system integrity, look for a solution that includes File Integrity Monitoring and automatically alerts you to file changes that are unusual or against policy. A defined list of all systems, software, and configurations in your environment allows you to establish relevant alerts procedures, including when to flag an incident and to whom to escalate an issue.

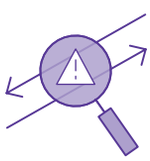


4. Application Control / Whitelisting

When your security team can set policy and be confident that it will run everywhere, your transition to the cloud will be simpler and more secure at every stage.

Relying on ports/IPs alone won't get you the level of visibility you need for full Cloud Workload Protection. Tightly controlling traffic between application components is a core part of a strong micro-segmentation solution. The best technologies have granular visibility and control, down to the application process, user, and fully qualified domain name, using details such as hash values, checksum, full path, resolutions and identity store authentications.
Some additional features that can augment application control include:

- Micro-segmentation that can limit lateral movement on the cloud even within the same application cluster.
- A single pane of glass approach, which translates to better security.
- The ability to create both whitelist and blacklist models, both of which can prevent unauthorized applications or traffic, and make sure that important connections run unimpeded.



5. Exploit Prevention/memory protection

The last core server protection strategy on the Gartner's Guide to CWPP is exploit prevention. Look for a micro-segmentation security tool that provides breach detection and response. That way you can replace redundant tools and reduce complexity in your data center.

Moreover, as mentioned previously, visibility and mapping are foundational. Once you have a thorough map of your whole network, it's easy to see unpatched vulnerabilities or malicious communications that are acting out of the norm. When your enterprise has established a baseline for legitimate traffic, unsanctioned movement stands out.

OTHER IMPORTANT PROTECTION STRATEGIES

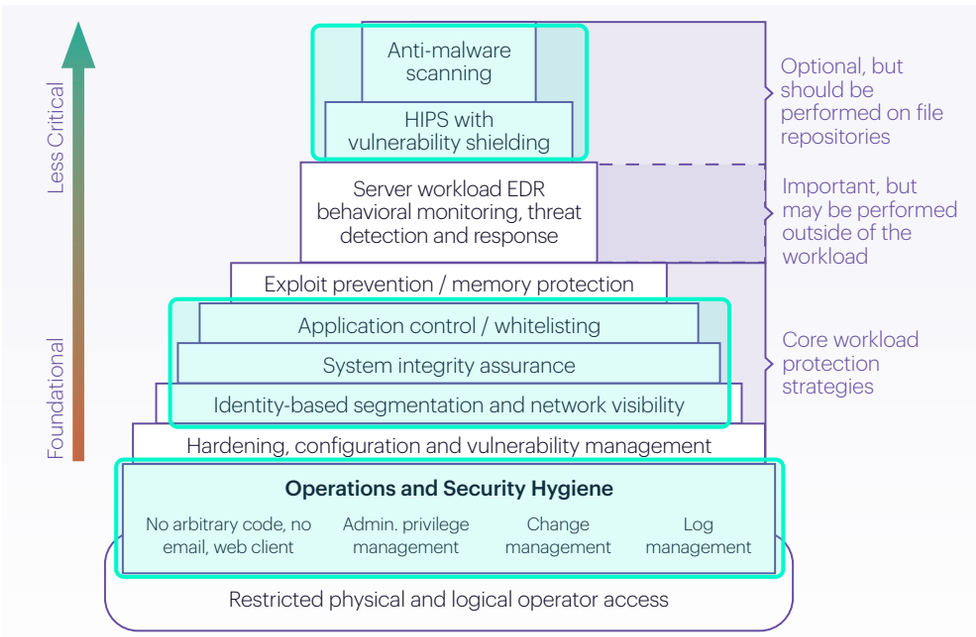
For a stronger security process, include server workload EDR behavioral monitoring, and TD/R in your strategy

The core server strategies mentioned above are foundational for security in the cloud. At the same time, Gartner identifies several other strategies that can strengthen your hybrid or multi-cloud environment, including server workload Endpoint Detection Response (EDR) behavioral monitoring, and Threat Detection and Response (TD/R).

EDR, behavioral monitoring, and TD/R are important parts of breach detection and incident response. In order to cover these aspects of security, look for a solution that includes reputation analysis. This will let you identify more information about an attack, as well as provide you with advanced deception capabilities to trick attackers into giving away their methods. In this way, you can harden your policy and security procedure moving forward.

Visibility data may be needed to establish information about a past event. The best providers store your data for months, allowing users to focus on specific applications, processes, and time periods. Security teams can also use this data for forensic investigation and improved incident response.

GUARDICORE CENTRA: PROTECTING HYBRID CLOUD WORKLOADS UNDER THE CWPP HIERARCHY



The Highlighted Areas Show Where Guardicore Fulfills CWPP Requirements

Guardicore Centra addresses the gaps of native-cloud security, meeting many of the foundational controls laid out in the CWPP. Moreover, the solution intelligently supports visibility, policy creation, and enforcement across hybrid and multi-cloud data centers.

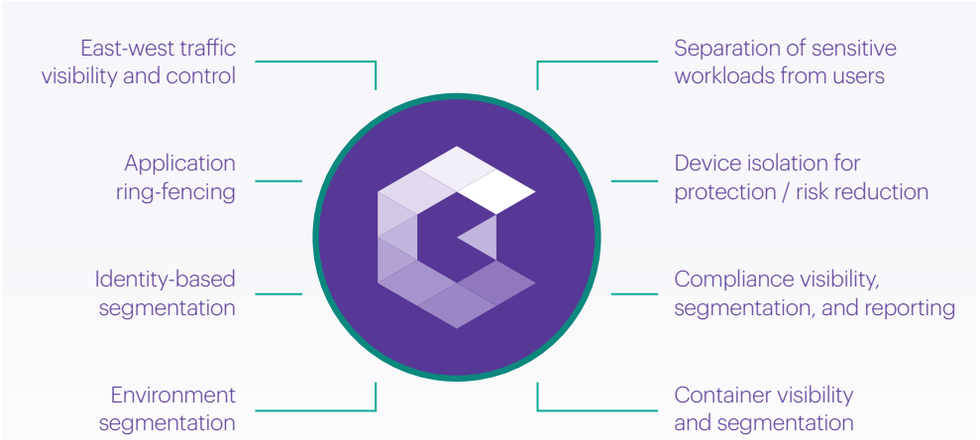
Centra provides in-depth visibility - one single pane of glass that gives a view of the entire data center. Visualizing your hybrid data center as a whole, you can thoroughly understand application dependencies and the effect that any policy will have on your network. This has a powerful effect on cloud migration, getting customers to the cloud significantly faster than native visualization tools.

Guardicore Centra's in-depth and context-based visibility results in a swift and thorough understanding of your environments

This in-depth visibility from Centra enables you to:

- Create a to-do list for networking in the cloud.
- Quickly detect applications across any infrastructure and application dependencies - a critical capability for successful migration.
- Understand your infrastructure and opeartional costs ahead of time.
- Gain insight into the best policy creation for lowering risk from migration planning stages.
- Take advantage of the shortest, simplest, and most secure path to your business goals for the cloud.

Guardicore visibility also comes with context for each communication and flow. This enables you to reduce errors and complexity. You can group and filter information to support any stakeholder reading the map, providing them with the exact information they need. This context-driven data reduces the need for third-party vendors and policy creators, resulting in swift understanding of your environments so you can create, refine, or amend applicable policies.



Examples of Guardicore Centra Micro-Segmentation Use Cases

Other critical features Guardicore provides include:

- Process-level policies, which enable simpler and stronger security when dealing with dynamic protocols such as FTP or Spark.
- Identity-based micro-segmentation policies, which enforce connections based on the user creating the connection.
- Fully qualified name-based policies allowing you to reach autoscaling resources whose IP addresses are dynamic.
- The use of existing public cloud tags as labels, simplifying the visualization of your hybrid or multi-cloud data-center.
- Automatic building of policies from observed traffic, so you get quick and expert guidance as you start your micro-segmentation journey.

Guardicore is platform- and infrastructure-agnostic, managing visibility and enforcement across the entire infrastructure

Reducing complexity is the ultimate goal when looking to secure a hybrid data center. In response to this need, Guardicore is platform- and infrastructure-agnostic, giving you one view of the whole application and policy that follows the workload, regardless of where it resides. Each rule is applied on all workloads, from vCenter and public clouds (AWS, Azure, GCP) to bare-metal and containers.

Not only does reducing complexity result in a stronger security posture, it also lightens the IT and security workload. With cloud-based security groups, you need native-cloud experts for each vendor. In contrast, with one security solution that manages visibility and enforcement across the entire infrastructure, you only need certified users for a single technology.

A FUTURE-PROOF CLOUD WORKLOAD PROTECTION PLATFORM

Guardicore provides the fundamentals of a trusted **Cloud Workload Protection Platform** so you can keep your hybrid cloud or multi-cloud data center secure across any environment

One of the cornerstones of Agile methodology and DevOps is the ability to fail fast and quickly and easily move to the Next Big Thing. Unfortunately, and somewhat ironically, migrating your workloads between different cloud providers can slow you down tremendously. It also can be difficult to do with security kept in place.

You need to be able to keep your options open. If you want to move to a multi-cloud infrastructure, or even migrate workloads to a new cloud provider altogether, it should not have a negative effect on security - nor should security stop you from making the move.

Guardicore allows you to remain flexible and move at the pace of business, migrating your workloads with security policies intact. It does not hinder the DevOps process or agility or require reconfiguration at every stage. Instead, Guardicore provides the fundamentals of a trusted Cloud Workload Protection Platform so you can keep your hybrid cloud or multi-cloud data center secure across any environment.

Guardicore enables migration to the cloud and between clouds, and provides unparalleled visibility with context. With Guardicore, you can enforce policy down to process and user level and follow your workloads wherever they go.

Now, you can make security a feature of every stage of the DevOps process, enabling agility and supporting your business. Your organization will be able to embrace cutting-edge cloud abilities while keeping security at its core.

Want to learn more about Guardicore Centra?
Visit www.guardicore.com today.

About Guardicore

Guardicore is an innovator in data center and cloud security that protects your organization's core assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security for any application, in any IT environment. www.guardicore.com

Guardicore