CITRIX®

White Paper

How Micro-Segmentation Solves Key Security Challenges in Virtual Environments

CITRIX Ready | Guardicore

Executive Summary

Virtual desktop infrastructure has long been used to make life easier for businesses the world over. Through the use of VDI, users can access data from anywhere in the world securely and instantly. VDI and virtual apps have made the modern workforce — comprised of telecommuting and remote employees — possible and practical.

But in spite of the many benefits to both employees and employers, keeping virtual systems secure has added a layer of complexity to the life of IT professionals. Through the years, the segmentation of users has proven particularly difficult. While this has always been true of VDI, hybrid clouds make segmentation even more challenging, especially for:

- Jumpbox access enforcement
- Zero trust security initiatives

With more than 100 million users worldwide, Citrix Virtual Apps and Desktops are deployed by more businesses than any other virtual solution. It's likely that your organization uses Citrix Virtual Apps and Citrix Virtual Desktops in boosting worker productivity while simultaneously cutting IT costs.

Citrix Workspace provides a complete solution to meet all your business needs. It gives employees the freedom to work from anywhere while cutting IT costs from any cloud — public, on-premises or hybrid — within a modern digital workspace.

But how does your organization manage the key security challenges that commonly exist in virtual environments? For many organizations, the answer to that question is quite simple: those challenges simply aren't addressed properly.

There are five key challenges that pose stumbling blocks in most organizations' efforts to secure virtual environments. This paper describes those key challenges and explains how the Guardicore Centra Security Platform's use of micro-segmentation answers them.

Key Challenges in Virtual App Security

Virtual apps and desktops have revolutionized the workplace. These tools of technology have even rendered the word 'workplace' somewhat archaic. Workplaces are no longer restricted to the confines of a designated physical structure. Instead, "workplace" now refers to the place any given worker chooses to work — anyplace in the world. The ability for workers to carry their entire office with them anywhere they go has wildly expanded the productivity potential of each worker. Simultaneously, virtual apps and desktops have enabled workers to achieve wonderful, life-enhancing work/life balances that, not so long ago, would have been a fantasy.

As with most revolutionary leaps of progress, the many positives of virtual apps and desktops has come at the cost of a few negatives, such as the increased difficulty of ensuring adequate security. Within data centers, the following five areas of concern are the key challenges associated with the deployment of virtual apps and desktops:

1. Digital Crown Jewel Protection. "The idea that some assets are extraordinary — of critical importance to a company — must be at the heart of an effective strategy to protect against cyber threats. Because in an increasingly digitized world, protecting everything equally is not an option." This quote from McKinsey encapsulates the importance of providing the most protection to the most important digital assets. But providing adequate protection to critical assets while simultaneously embracing the many benefits of virtual apps and desktops requires a delicate balance.

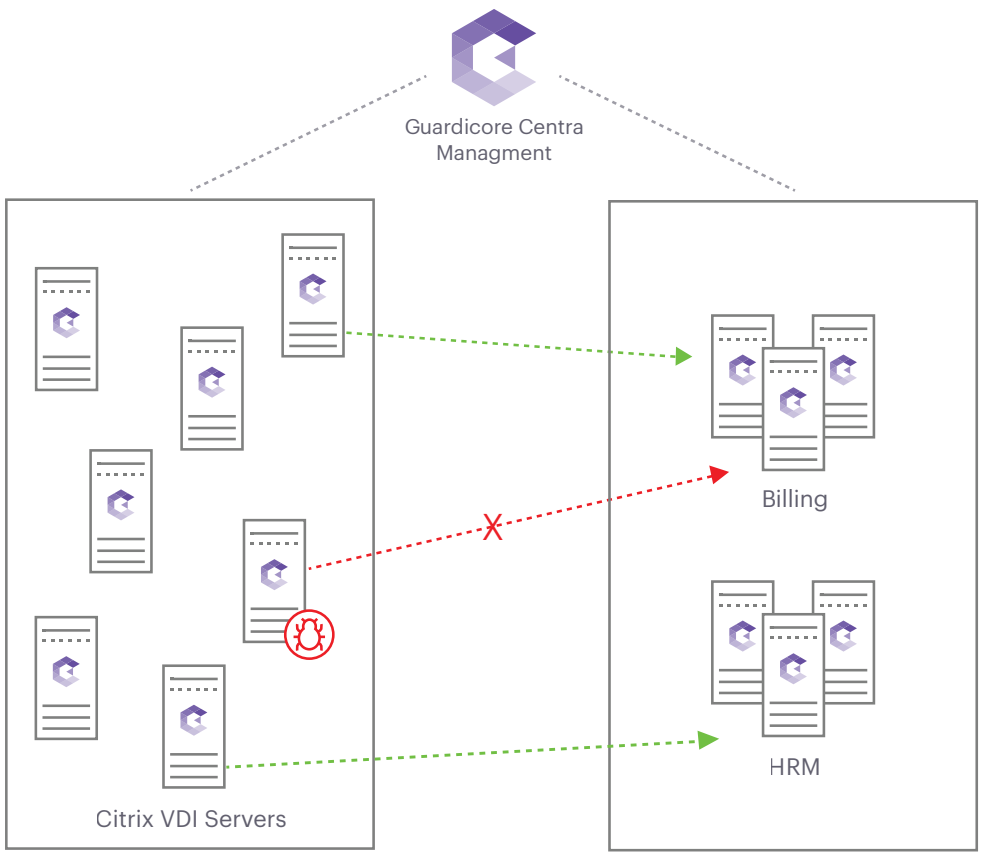
2. Lateral Movement Prevention. Data center security has long focused on creating barriers to unauthorized external intrusions. Within those external barriers, the typical data center offers little resistance to, or vetting of, the east-west traffic that represent normal workflows between servers and applications. But within most data centers, the volume of east-west traffic far exceeds the volume of north-south perimeter traffic

Consider these startling stats: Security research has revealed that dwell time — the time it takes to discover that an attacker has breached perimeter defenses — averages 200+ days. And breakout time — the time it takes an attacker to move laterally from the system they initially breached into other systems — is less than two hours. Combine the two, and it's obvious that, once a north-south breach has occurred, the intruder is likely to enjoy virtually unlimited time and freedom in moving laterally throughout the system.

3. Simplify and Accelerate Compliance. Most industries are facing historically high demands for maintaining compliance with a range of regulatory demands. It's a burden made ever more difficult through the proliferation of virtual environments. As a result, most organizations are actively seeking ways to reduce the difficulties of maintaining compliance while simultaneously boosting the overall success rate of compliance efforts.

4. Secure Cloud and PaaS Adoption. More and more organizations are seeking to leverage the benefits of Platform as a Service cloud computing models. PaaS offers a range of benefits that includes increased efficiency, a need for less in-house development capability, virtually unlimited scalability, future proofing, and many others. But tapping into the benefits of PaaS typically requires that an organization's system and data be exposed to multiple third-party vendors, often resulting in some unique security risks. According to Gartner, "[D]ata security and system availability are critical issues" for companies that use PaaS services. It is critical, therefore, that companies implement infrastructure-agnostic security policies that work consistently across legacy bare metal servers and all forms of cloud.

5. Innovation. The rapidly changing needs and technologies that have become commonplace in today's business environment makes innovation a critical tool for remaining competitive. But maintaining and enhancing security without stifling innovation can be quite the challenge. Doing so requires that security be integrated with application development, but without inflicting the penalties of time-consuming software changes, infrastructure changes or downtime. Ultimately, security must keep pace as innovation spurs the evolution of new and complex business and application needs.



Guardicore enforces a security policy between VDI servers and the applications, reducing the attack surface and providing visibility and detection in case of violations.

How Guardicore Centra Addresses These Challenges in a Citrix VDI Environment

Micro-segmentation is the answer to the problems described above. Network World defines micro-segmentation as "a method of creating secure zones in data centers and cloud deployments that allows companies to isolate workloads from one another and secure them individually." It's a concept that is rapidly gaining recognition as a key security tool in data center environments.

In 2018, Gartner named micro-segmentation as one of ten key security projects that CISOs should focus on to reduce security risks: "This project is well-suited for organizations … that want visibility and control of traffic flows within data centers. The goal is to thwart the lateral spread of data center attacks." As Gartner VP Neil McDonald explained, "If and when the bad guys get in, they can't move unimpeded."

Citrix has noted that with micro-segmentation, "we can restrict the types of data being exchanged and open only the required ports on which each machine should communicate with the others. This can be used to separate the network traffic between large multi-tenant deployments, such as different departments with different data confidentiality levels or a number of tenants in a service provider deployment."

But how can micro-segmentation be used to address each of the five key security challenges noted above? Let's focus on how Guardicore's Centra Security Platform uses micro-segmentation to address each of these key challenges.

1. Defending Critical Crown Jewels. The visibility and control that Guardicore Centra provides makes it easy for security teams to ring-fence their digital crown jewels with precise security policies. Tightly managing how critical applications function and communicate reduces their exposure to security vulnerabilities and threats from the broader IT infrastructure.

The detailed information Centra collects about application functionality, communication flows, and dependencies, is used to create an interactive map of an IT infrastructure. The contextual view provided by this map is useful in refining understanding of how applications work, and is crucial for use in creating powerful security policies that can be deployed in protecting an organization's most critical digital assets.

2. Controlling Lateral Movement. Guardicore Centra helps prevent attackers from using an individual point of compromise as a starting point for lateral movement. Centra makes it easy to see what is happening within an IT infrastructure and tightly controls communications between IT assets.

Guardicore Centra uses network and host-based sensors to collect detailed information about assets and flows in data center, cloud and hybrid environments. This information, combined with labelling information from orchestration tools, is used to display a visual representation of east-west traffic in the environment. The enhanced visibility that results provides immediate benefits in enabling a better understanding of potential lateral movement risks, and it simultaneously lays the foundation for the application of more sophisticated lateral movement security techniques.

With the enhanced visibility of both sanctioned and unsanctioned east-west movement that Centra provides, IT teams can use micro-segmentation to substantially impede the ability of attackers to move laterally. With strong micro-segmentation policies implemented, unsanctioned lateral movements can generate alerts to the security team or even be blocked proactively.

Centra even uses sophisticated deception technology to gain intelligence about an attacker's means and methodologies. Centra can feed an attacker simulated system responses that suggest the attack is proceeding successfully, all while recording and analyzing the attacker's tools and techniques — valuable data that can be used in strengthening security defenses.

3. Enhancing Compliance Efforts. Implementing regulatory compliance controls and ensuring their ongoing effectiveness typically rank among the most important — and most time-consuming — activities that IT teams undertake. The complexity of maintaining compliance only grows more difficult and complex as organizations transform their IT infrastructure over time. Guardicore simplifies compliance by providing visual representations of IT infrastructures. It also offers the ability to create software-defined compliance boundaries around regulated assets. These policy definitions are completely independent from underlying IT infrastructures, so they can adapt as infrastructures evolve, eliminating the need to simply guess whether compliance policies remain effective.

Guardicore provides the ability to see compliance policies work in real time and enables the evaluation and validation of the historical effectiveness of compliance policies. These tools help to ensure the proactive avoidance of compliance gaps while simultaneously simplifying audit activities.

4. Securing Cloud and PaaS Deployments. Many security teams lack detailed visibility into how their business applications work and how effectively disparate firewall rules and VLAN configurations are protecting them. This challenge is magnified when organizations adopt new deployment models like PaaS or migrate application workloads to the cloud. Guardicore removes this complexity from digital transformation by providing a single visibility and security model that works with all deployment models and environments — old and new. On-premise applications running on legacy operating systems can be viewed alongside newer deployment models like PaaS and container services, and protected with a common set of policies. This level of insight transforms security into an enabler of digital transformation rather than a hindrance.

5. Supporting Innovation. Innovation and security are opposing forces in many organizations. As development and operations teams attempt to move quickly to address new business needs, security teams must often ask for delay and caution to ensure that sensitive applications and data are kept safe. Guardicore helps technology and security teams move in the same direction by making it easier to implement strong security controls without slowing application development and deployment momentum. Guardicore provides visibility to how applications work and interact in detail. It helps the design and implementation of security policies that are independent from applications and their underlying infrastructures.

No Need to Micro-Analyze Your Micro-Segmentation Choice

Though a growing number of organizations are recognizing that micro-segmentation is the answer to solving these key security challenges, many are stumbling in their efforts to effectively deploy micro-segmentation. One common mistake, for example, is the attempt to implement micro-segmentation using VLANS or firewalls. But these solutions are typically intertwined within the organization's infrastructure, so that any changes to the infrastructure results in downtime, bottlenecks and lots of coordination among different teams.

Deploying a micro-segmentation software solution such as Guardicore Centra eliminates those obstacles. The deployment process can be managed by a single person using a single pane of glass. Implementing micro-segmentation through Guardicore Centra can, in fact, be achieved up to 20 times faster than through competing solutions. And Guardicore Centra provides more granular visibility and control than any other solution.

For all the above reasons, Guardicore Centra is a great choice for utilizing micro-segmentation in making your Citrix Virtual Apps and Desktops more secure. And Guardicore Centra is now certified as Citrix Ready. It's a partnership that stands ready to transform the security of your cloud and software-defined data center.

To learn more about how Guardicore complements the already-impressive abilities of Citrix VDI, visit the Citrix Ready Marketplace. If you're wondering just how resiliently your network might handle the key security challenges noted in this paper, there's a safe and easy way to find out. Guardicore's free and open source Infection Monkey is a Breach and Attack simulation tool you can use to assess the resiliency of your private and public cloud environments to post-breach attacks and lateral movement.

CITRIX®

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States