Guardicore

Solution Brief

Three Easy Steps to Successful Network Segmentation with Guardicore

- **Reveal:** Best-in-class visibility provides insight into applications, workloads, and communication flows. This enables organizations to easily label and group all assets and to streamline security policy development.
- **Build:** A single click on a communication flow generates automated rule suggestions and quickly builds a strong security policy. Intuitive workflows and a flexible policy engine enables continuous policy refinement and reduces costly errors.
- **Enforce:** Maintain consistent security controls regardless of the underlying infrastructure. Additional integrated breach detection and response capabilities enable organizations to see policy violations in the context of an active breach and quickly contain the attack spread.

Simple and Fast Network Segmentation for Telecommunications Service Providers

Telecommunications service providers need not only to keep up with increasing customer demands but also need to remain competitive by launching new services offerings. This means supporting new 5G infrastructure and cloud technologies to increase flexibility and to improve performance. However, it's essential that security measures keep pace with infrastructure transitions, or service providers may find themselves introducing more risk along with new technologies.

Network segmentation is critical when it comes to managing risks and maintaining a strong compliance posture. It enables telecommunications service providers to protect business continuity while also reducing the overall impact of security breaches by limiting lateral movement.

Challenges with Traditional Segmentation Approaches

Using traditional approaches to segmentation, such as firewalls and VLANs, as well as virtual cloud-based firewalls, can mean facing a lengthy and resource-intensive project. It makes it challenging to keep security at pace with evolving business needs and digital transformation efforts.

Lack of visibility - Successfully designing and enforcing segmentation policies requires a good understanding of application interdependencies and communication flows. Missing this data creates roadblocks when navigating a segmentation project.

Diverse infrastructure - Telecommunications service providers often operate complex infrastructures composed of legacy systems, cloud environments, modern network function virtualization (NFV) delivered using microservices, and more. Managing and enforcing security controls across such a diverse set of technologies on multiple platforms is very resource intensive.

Cost of downtime - Even as regulations and industry standards continue to push for more granular segmentation, achieving it through traditional methods requires a number of network changes, including IP and VLAN re-configuration, which results in production downtime. In the case of many legacy applications, this process can come with significant resource costs, if it's even at all possible.

The Guardicore Centra™ Application Security Platform

Guardicore provides telecommunications service providers an innovative way to achieve network segmentation without the challenges that come with traditional approaches. By leveraging software-based overlay segmentation technology, the Guardicore Centra Application Security Platform helps companies achieve network segmentation in record time, with significant risk reductions across all types of infrastructure without costly network changes and downtimes.

By removing common roadblocks associated with traditional segmentation methods, service providers can successfully pursue projects important to their business, confident that appropriate security controls are in place.

Challenge	How Guardicore Helps
East-West Traffic Visibility	Guardicore Centra provides context-rich visibility into all data center and cloud traffic, whether it is bare metal, virtualized, or containerized. This accelerates security operations and helps organizations make informed decisions on policy creation, breach investigations, and auditing.
Protecting Legacy Assets	Telecommunications service providers often run critical applications on legacy servers, and it's common to see operating systems such as HP-UX, Solaris, and AIX as well as legacy Windows versions. Guardicore Centra can quickly reduce access paths and attack vectors to these legacy assets, reducing attack surface and risk.
Managing User Access	Guardicore Centra enables organizations to enforce least privilege access with flexible security policies. User-specific segmentation policies can be set for each user connecting through VDI, terminal servers, or jumpboxes, avoiding the need for a dedicated terminal server or VDI cluster for each user group and reducing costs.
Protecting 5G Technology	Usually deployed as VMs or containers in general-purpose hypervisors, 5G technology can be difficult to segment and secure with traditional security tools. Guardicore enables customers to adopt these new technologies, getting rid of appliances and bare-metal servers, while also enforcing consistent security controls to reduce risk.
Protecting Private Clouds	For service providers that operate and manage private clouds for end customers, Guardicore Centra also extends the same critical segmentation and visibility capabilities to that service, increasing customer security, satisfaction, and revenue.
Protecting Point of Sales (POS)	Due to their connectivity into networks' core systems and critical applications, physical shops are often targets for attacks. Regulating traffic from POS assets, limiting it to a specific path, and closely monitoring it is an important risk reduction strategy that can be effectively achieved with Guardicore Centra.
Detecting Suspicious Activity	Guardicore Centra's breach detection modules, including Reputation Analysis, Threat Intelligence Firewall, and File Integrity Monitoring, along with the platform's Dynamic Deception technology, helps organizations effectively detect breach attempts as well as discover lateral movement inside data centers.

Case Study:
Telecommunications Services Provider Selects Guardicore to Protect Critical Legacy Assets

The Challenge: Secure Legacy Assets

As one of the leading telecommunications providers in Europe, this organization had revenue-generating applications running on legacy servers, which were vulnerable due to missing security patches and a lack of consistent security controls necessary to manage access.

These thousands of legacy servers were at risk in the event of a breach since they run on a relatively flat network together with other modern assets. The customer determined that if attackers exploited access to just one of the many unpatched legacy machines they could easily move laterally and compromise other critical assets running on the same network.

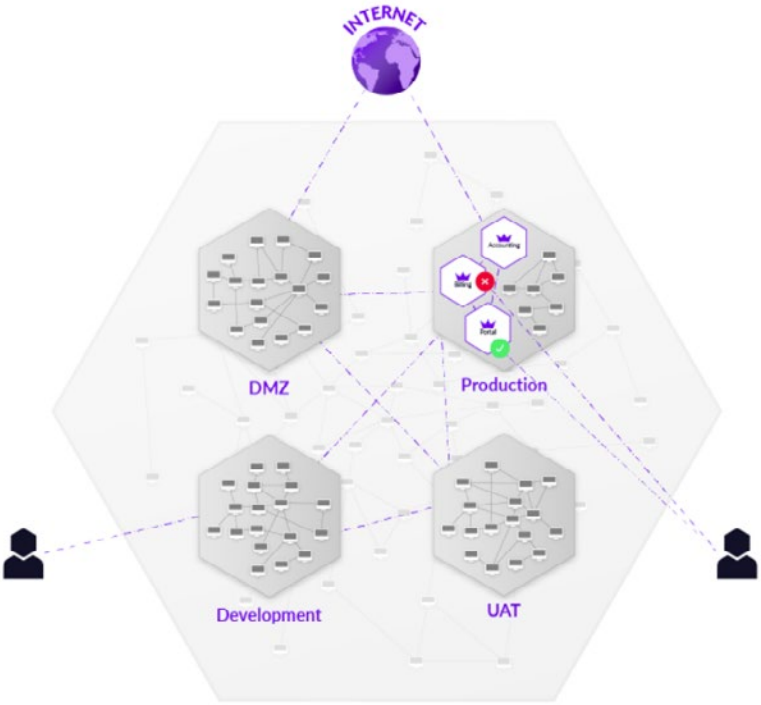
Selecting a Solution: Segmentation without Application Downtime

To mitigate the risk posed by the legacy assets, the customer needed to reduce the attack surface by tightly controlling access paths to and from the servers. However, the physical distribution of those servers and the current lack of visibility into east-west traffic presented a significant challenge.

Additionally, traditional segmentation methods often require implementing significant network changes, including reconfiguring IPs and VLANs, which results in downtime. Therefore, the customer concluded that to isolate the legacy servers using traditional firewalls would be both complex and too expensive, so they looked for alternatives.

Guardicore Centra Application Security Platform

Because Guardicore's approach to network segmentation uses a software-based overlay approach, users can achieve network segmentation in record time without costly network changes and downtime, which made it an ideal solution for securing the customer's legacy assets. By using the Guardicore Centra Application Security Platform, the telecommunications provider was able to dramatically shrink the attack surface across thousands of its most critical servers without any service disruptions, significantly reducing overall risk and the impact of security breaches.



Conclusion

Guardicore has helped some of the world's largest telecommunications service providers maintain security at scale while pursuing innovation and new business opportunities.

The platform enables customers to extend protection anywhere in their environment, including hybrid cloud environments that span on-premises workloads, legacy systems, VMs, containers, and infrastructure as a service (IaaS). This approach provides significant advantages in agility and cost reductions, giving organizations the freedom to choose and change infrastructure technology and providers.

Guardicore MSSP Model

Additionally, managed security service providers (MSSPs) can use Guardicore's software-based overlay segmentation technology to deliver network segmentation in record time and achieve significant risk reduction across hybrid infrastructures for their end customers, all without costly network changes and downtimes.

Service providers can choose to operate the service on Guardicore's SaaS infrastructure, or, as needed, on an MSSP's cloud so they can provide additional value to customers with managed visibility, segmentation, and breach detection services.

Want to learn more about the Guardicore Centra Application Security Platform? 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

v.2.0

Guardicore