GuardiCore for Managed Security Service Providers

The Managed Security Services Landscape

There is a fundamental shift happening in the Managed Security Services (MSS) market driven by a number of factors. The rapid adoption of cloud is forcing service providers to expand tooling and capabilities to protect customer cloud workloads and hybrid environments. Companies are increasingly moving away from prevention-only approaches to security and moving towards proactive detection and response strategies, driving demand for new service deliverables and outcomes. There is a large influx of new entrants into the MSS space, evolving from traditional security solution providers. These and other ever-shifting dynamics are resulting in a rapidly increasing competitive MSS landscape.

Additionally, sophisticated attacks have become progressively more capable of invading and moving laterally (east-west) across hybrid data center environments. Perimeter, endpoint and other preventative technologies alone are no longer sufficient. When there is a breach, traditional security tools and policies fail to detect lateral movements, allowing attackers to dwell inside environments for 191 days on average.[1] This dwell time represents significant risk to a company as well as to the service provider protecting them.

GuardiCore for Managed Security Service Providers

A Managed Security Service Provider (MSSP) must move closer to application workloads to protect their clients' most critical assets. A distributed, flexible strategy, offering continuous visibility and protection within the fabric of a hybrid data center environment is optimal for securing applications and removing the risk of dwell time. Real-time breach detection is key to defense, with a capability to find the "needle in the haystack" amidst massive, dynamic traffic volumes. Beyond detection, key differentiators are the ability to implement and enforce security policies, visualize attacks, isolate attacks automatically (eliminating dwell time) and gain deep analysis that can be leveraged to dramatically accelerate remediation and continuously improve a client's security posture.

The GuardiCore Centra™ Security Platform is specially designed for today's cloud-centric environments, providing a unique combination of application process-level visibility, micro-segmentation, multi-vector breach detection, dynamic deception, semantics-based analysis and automated incident response. The Centra platform proactively engages, investigates and then thwarts confirmed attacks with pin-point accuracy.

Visibility: Foundation for a New Security Model

GuardiCore Reveal™, a key component of the Centra platform, provides unprecedented visualization of applications and processes running across entire heterogeneous environments. This allows partners to gain a deep contextual and intimate understanding of each client environment, discovering new insights that greatly enhances partner value, while further establishing trusted advisor status.

Increase SOC Efficiencies

GuardiCore Centra creates operational efficiencies for MSSPs by reducing noise associated with low-level alerts and false positives, confirming security events with high fidelity and accelerating remediation. Built completely on RestAPI architecture, Centra is an open, flexible solution that integrates with existing security tools, SIEMs and ticketing systems. Covering entire heterogeneous environments in a flexible, lightweight fashion, Centra provides comprehensive security capabilities from a single platform and removes complexity associated with managing multiple point solutions.

---

1   Ponemon Institute. *2017 Cost of a Data Breach Study: Global Overview.* June 2017

Gain Competitive Edge with Differentiated Services

GuardiCore Centra provides MSSP partners with a substantial opportunity to establish market differentiation and increased value-add, enabling numerous MSS offerings including Managed Detection and Response (MDR), Micro-Segmentation (delivered as-a-service), Managed Cloud Workload Protection and other ancillary services such as Incident Response, Threat Hunting and Professional Services (PS). Additionally, GuardiCore allows MSSPs to extend coverage to many additional compliance requirements.

MANAGED DETECTION AND RESPONSE

GuardiCore enables rapid time-to-market with Managed Detection and Response (MDR) capabilities for MSSP partners. This represents a significant opportunity as exponential growth and rapid adoption of MDR services is expected through 2020, according to Gartner.[2] Conceptualized by an elite team with extensive real-world experience in the Israeli Defense Force (IDF), the Centra security platform was specifically designed to provide real-time breach detection and automated response.

Built on a foundation of visibility, the platform discovers and tracks process-level activity across applications and correlates it with network events, providing a dynamic visual map of an entire heterogeneous environment. This alone is a significant differentiator, as visibility of lateral traffic flow is typically non-existent. Continuously monitoring lateral traffic, Centra provides real-time detection of all malicious activity based on user behavior, reputation analysis and security policies. The platform automatically isolates attacks leveraging dynamic deception, assembles high fidelity attack intelligence, and delivers SOC analysts with highly relevant insights and remediation steps.

Enabling next-gen MDR services, GuardiCore helps MSSP partners to provide an upgrade path for existing customers and establish competitive differentiation in the marketplace.

MICRO-SEGMENTATION AS-A-SERVICE

Micro-segmentation is one of the most advanced security methods to protect critical assets, users and data from both outside hackers and malicious insiders. However, micro-segmentation is normally difficult to deploy and manage due to lack of visibility, an in-depth understanding of applications and complexities associated with enforcement across disparate platforms. Not surprisingly, micro-segmentation delivered as a service has been out of reach given these challenges.

GuardiCore eliminates the complexity associated with micro-segmentation from initial installation to ongoing program management. Centra enables a straightforward, phased approach to segmentation starting with global policies, followed by agentless protection between applications and external networks, and finally full-scale micro-segmentation securing traffic within applications. The Centra platform provides the process-level visibility, flexible policy engine, and streamlined deployment and management to ensure successful segmentation engagements.

GuardiCore provides the technology, expertise and customized playbook to enable MSSP partners to effectively deliver Micro-Segmentation as-a-Service (MSaaS), setting yourself apart from the competition and establishing a net new revenue stream.

GuardiCore MSSP Program

The GuardiCore MSSP Program equips partners to deliver and monetize value-added security services with:

- MSSP-aligned "pay-as-you-grow" licensing model—no CapEx and immediate profitability
- Customized go-to-market playbooks
- Training (sales, technical pre-sales and operations)
- Ongoing sales support, demo environment
- No-cost floating licenses to enable pre-sales and short-term PS engagements
- Access to GuardiCore Labs, our premier cyber threat research team
- UI white-label opportunity

Become a Partner

Visit the **GuardiCore Partner Portal** to get more information or to register as a new partner**.**

---

2   Gartner. *Market Guide for Managed Detection and Response Services.* May 31, 2017.

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, the GuardiCore Centra Security Platform is changing the way organizations fight cyber attacks.

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