Guardicore

SOLUTION BRIEF

Guardicore Hunt

Managed threat hunting delivered by Guardicore Labs

Guardicore Hunt is Guardicore's managed threat hunting service, built on Guardicore Centra. The service is provided by Guardicore Labs, an elite team of threat experts with vast experience in combating cyber attacks. The team continuously hunts for anomalous attack behavior and advanced threats, often escaped by standard security solutions.

Our threat hunters work for you to discover adversary actions such as lateral movement, malware execution, communication to Command & Control servers and more. You are notified immediately on any critical incident detected in your network. Then, Guardicore Hunt experts work closely with your team to remediate any compromised asset for a fast response.

> ***I just wanted to thank the Guardicore Hunt team for assisting us with the data breach and quick remediation. This has helped us prevent any breaches on our mission critical systems.***
>
> CIO, Leading Health Center

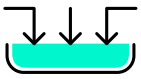
KEY BENEFITS

Uncover ongoing attacks
The Guardicore Hunt team proactively hunts for ongoing and emerging attacks, minimizing dwell time and reducing the time to mitigation.

Empower your team
Guardicore Hunt experts work on behalf of your team to monitor your environment for the existence of adversaries, saving you time, effort and cost.

Get rapid response
You are instantly notified of every critical incident, that gives you the confidence to focus on your business.

Get threat hunting tailored to your environment
By continually monitoring your environment for attacks, the team develops a baseline of your security configurations and can tailor its hunting methods to your specific topology.



COLLECT

- Gather data from Guardicore Centra agents, assets, policies
- Leverage collective intelligence from global customer base

HUNT

Hunt for threats based on Guardicore technology, in-house tools and threat intelligence

INVESTIGATE

Identify tools, persistence, attack scope

RESPOND

- Contain, quarantine compromised assets, support response team
- Get immediate notification on a compromise with findings and recommendations

Key Capabilities

24/7 expert human analysis

Our cybersecurity professionals come from a wide range of fields including security research, offensive security, military intelligence, red team, incident response and data science.

Alerts on real threats

To avoid alert fatigue, the team alerts its customers on real threats only. Armed with data collected from a global customer base, our experts maintain a baseline for a 'healthy' data center and cloud applications communication, which helps us detect the most impactful threats.

Proprietary hunting tools

Guardicore Hunt experts routinely develop advanced threat hunting algorithms such as user and network activity anomalies, executable analysis, log analysis and more, to form a powerful toolset for fast detection and response. Guardicore Insight, a powerful osquery-based tool to query endpoints and servers in real time is included with the service at no additional cost.

Context-rich threat intelligence

Our team of hunters collects indicators of compromise ranging from IPs and domains to processes, users and services, leveraging Gaurdicore's in-house repository of global network sensors (GGSN) as well as a growing number of third-party threat intelligence technologies.

Visibility from network, cloud and endpoint

This combination of data gathered from Guardicore Centra's assets, labels, and policies along with data from Guardicore Reveal for asset insights and Guardicore's osquery-based Insight - all these provide our team with the most comprehensive visibility of your environment.

Immediate notification

As a Guardicore Hunt customer you receive:

» **Threat email notifications** are sent immediately after a threat is detected

» **Periodic executive-level threat reports** with analysis, stats, and metrics to keep your executives or board informed of the high-profile attack campaigns

» **Integration with Guardicore Centra** for easy incident management

About Guardicore

Guardicore delivers easy-to-use Zero Trust network segmentation to security practitioners across the globe. Our mission is to minimize the effects of high-impact breaches, like ransomware, while protecting the critical assets at the heart of your network. We shut down adversarial lateral movement, fast. From bare metal to virtual machines and containers, Guardicore has you covered across your endpoints, data centers and the cloud. Our software-based platform helps you become more secure to enable your organization's digital transformation.