Cyber Security Analyst

Built upon Guardicore's class-leading Centra platform, our Cyber Security Analyst (CSA) service monitors, analyzes, and proactively hunts for new threats, in order to detect and mitigate potential breaches to your datacenter and cloud environments.

Delivered by world-class cyber security experts, this offering extends your security team with a dedicated Cyber Security Analyst to enhance the protection of your environments. Through proactive monitoring and expert knowledge of cyber defense, Guardicore's analysts will help you to reduce your attack surface and accelerate response times in the case of a breach.

Our CSA service is designed for customers who wish to ensure the highest level of security in their datacenter and cloud environments. Whether they are subject to security and compliance requirements, developing incident detection and response policies, or simply need expert help to review and implement current best practice processes and procedures, our team is positioned to assist.

Two CSA package levels are available to meet varying needs:

CSA Essentials:

- **Managed Threat Hunting** - The CSA team seamlessly taps into the vast information reported by Guardicore Centra from across your on-premises and cloud environments and analyzes it on an ongoing basis to zero in on possible threats. Alerts are investigated by an experienced team of researchers, and you are provided with concise, actionable insights about real threats to your infrastructure.
- **High-Severity Incident Email Alerts Information** - Rich email notifications are provided when high-severity security incidents are detected, giving your team the context and guidance needed to respond quickly and effectively.

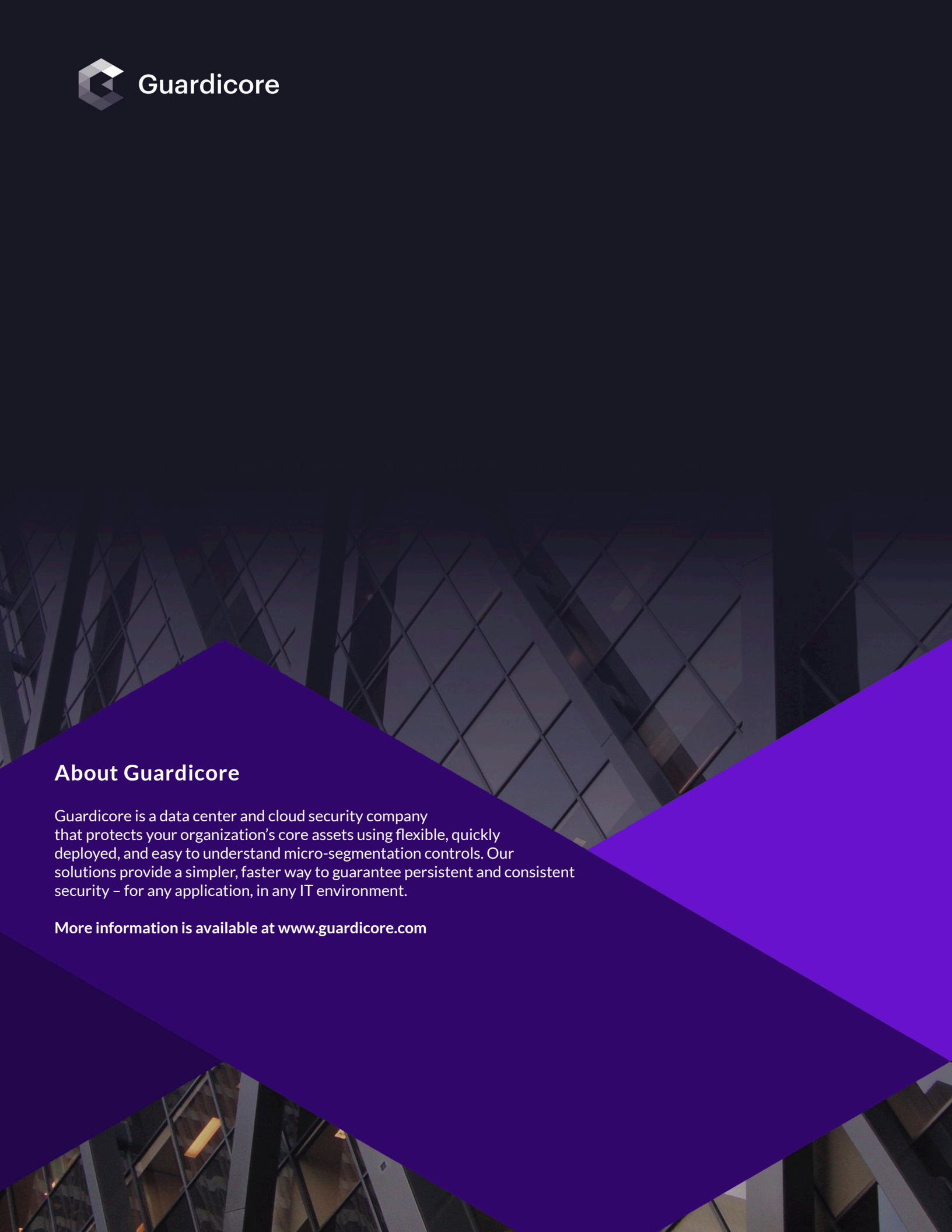
CSA Enterprise:

- **Guardicore Community Insights -** Using its unique visibility across all Guardicore deployments, the CSA team will proactively detect and instantly mitigate new threats in your environment based on attacks detected in other Guardicore instances. The CSA team analyzes these attacks, extracts Indicators of Compromise (IOC), proactively follows their trail in your environment, and stops them.
- **Alert Policy Optimization** - The CSA team continuously optimizes monitoring rules to eliminate false positive and avoid false negative alerts.
- **Investigation and Remediation Support -** When critical security incidents are detected, the CSA team will collaborate with your security team to plan and execute an effective response. Experienced investigators will analyze the attack techniques and impact and provide detailed containment and remediation recommendations.
- **Protection from Emerging Threats** - The CSA team assesses the external threat landscape on an ongoing basis. As new major industry threats and major security vulnerabilities are discovered, the CSA team proactively assesses the potential impact to your infrastructure and provides risk mitigation guidance.

- **Attack Surface Reduction -** Your security team will have access to specialized policy templates created by the CSA team, which will help you protect core IT infrastructure services, reduce your network attack surface, and implement security best practices.
- **On-Demand Expert Access** - Your security team will have direct access to experienced security experts whenever needed to assist with security challenges and provide advice and guidance as new needs arise.
- **Monthly Management Reports -** The CSA team will provide monthly management-level reports that summarize the threat hunting activity executed in the past month with its findings. The report will also provide an overview of the proactive prevention actions that were taken, attack surface reduction policies, configuration fine-tuning, and other optimizations tailor-made to your environment.
- **Early Preview Feature Access -** CSA Service customers will receive early previews of new Guardicore Centra features, and the CSA team will work collaboratively with your team to assess how new product enhancements can further protect your infrastructure from breaches.

Task	CSA Essentials	CSA Enterprise
Managed Threat Hunting	✓	✓
High Severity Incident E-Mail Alerts	✓	✓
Guardicore Community Insights		✓
Investigation & Remediation Support		✓
Protection from Emerging Threats		✓
Attack Surface Reduction		✓
On-Demand Expert Access		✓
Monthly Management Reports		✓
Early Preview Feature Access		✓

Guardicore



About Guardicore

Guardicore is a data center and cloud security company 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.

More information is available at www.guardicore.com