Guardicore

CASE STUDY

Guardicore Helps Blue Bastion Revolutionize Security-as-a-Service Delivery

The Client

Blue Bastion, the cybersecurity division of Pittsburgh-based Ideal Integrations, delivers Managed Detection and Response (MDR) services that help its customers defend their most critical business assets around the clock. The MDR program is built on a unique approach that combines a diverse arsenal of security measures with a highly trained and talented team of security professionals that monitor high-fidelity alerts and vulnerabilities continuously.

The Challenge

Protecting Highly Confidential Data in the Cloud

Blue Bastion has revolutionized the delivery of security-as-a-service by introducing foundational security controls for the protection of assets within dynamic data center environments. Using the Guardicore platform, Blue Bastion deploys micro-segmentation controls that enable its own security analysts as well as its customers to:

- Create and monitor a comprehensive visual map of all applications and activity inside the data center, allowing visibility into all workloads and a full understanding of application-layer communications
- Filter and organize applications into groups and label them for the purpose of setting common security policies-for example, all applications related to a particular workflow or business function
- Define and create rules governing authorized communications between applications
- Test and refine those rules to ensure they are not disrupting normal, authorized traffic

Blue Bastion

"...We needed additional controls and tooling that we could use to shrink the risk surface, monitor for unauthorized lateral movement, add an element of deception, and increase the fidelity of alerts. Guardicore was the only platform we tested that gave us everything we needed to fill those gaps."

- Corey Bussard,
Manager of the Blue Bastion SOC

The Solution

Guardicore Centra™ Security Platform

The Guardicore solution makes it possible to create strong micro-segmentation policies in a matter of minutes per application. Alerts triggered by these policies are focused only on non-compliant traffic, thereby reducing the volume of alerts and limiting them to cases in which a policy has been violated, indicating a likely threat. Policy-based detection helps the Blue Bastion team detect, confirm and contain threats quickly to prevent damage and minimize losses. These granular security controls do double duty, preventing an intruder from gaining malicious access to an application or process while simultaneously alerting administrators to the intruder's presence. Guardicore automatically blocks unauthorized communications and directs threats to a quarantine sandbox for investigation, enabling a swift, real-time response that prevents attackers from reaching their goals.

In contrast, using only a SIEM, it is difficult to ascertain quickly whether an anomaly represents a true threat and, if so, the level of the threat in question. "Our team routinely receives alerts related to reconnaissance traffic, testing perimeter security controls, and even attempts to brute force systems," says Corey Bussard, Manager of the Blue Bastion SOC. "While we monitor all of these very closely, asking our team to chase all of them to a final end-state is not realistic. We knew we needed additional controls and tooling that we could use to shrink the risk surface, monitor for unauthorized lateral movement, add an element of deception, and increase the fidelity of alerts. Guardicore was the only platform we tested that gave us everything we needed to fill those gaps."

According to Bussard, leveraging Guardicore in conjunction with a SIEM has been so effective that it has allowed his team to boil 100 alerts down to one. "We make it a point not to knee-jerk react to every alert coming from the SIEM, especially those associated with typical perimeter recon and surface attacks. Instead, we keep an eye on those while also watching for unauthorized lateral movement via Guardicore. We know if we see an attack followed closely by lateral movement, we have something we need to jump on directly." The high fidelity of incident alerts from Guardicore has also helped reduce the burden of "alert fatigue" that often affects cyber analysts working in 24x7 SOCs. The increased efficiency allows Blue Bastion to support more customers with a smaller team, making its MDR program economical and cost-effective for a substantial segment of the marketplace.

Dynamic Deception Strengthens Breach Detection

Guardicore employs a dynamic deception technology in which attackers are redirected automatically to a decoy based on suspicious failed network traffic. An automated analysis tool analyzes every redirection and distinguishes between low

severity events and real incidents. Guardicore monitors the attacker's activity inside the deception server, registering every operation and system call in a transparent fashion so that the attacker is unaware that they are being monitored.

Blue Bastion discloses the attacker's TTPs and performs complete IoC collection, turning the data collected into actionable alerts and intelligence. This ensures that every alert is real, with a very low rate of false positives. The alerts generated include detailed analysis and forensic information, explained in natural language, while providing forensic evidence and artifacts. These easy-to-read alerts simplify detection and threat hunting.

By combining highly interactive deception, analysis of every failed connection, and automatic redirection with complete monitoring of the attacker's actions, Blue Bastion is able to leverage highly accurate intelligence and reduce the rate of false positives without missing attacks. This allows more efficient and effective deployment of highly skilled security analysts across multiple sites, which translates to maximum value for customers.

Increasing SOC Efficiency with Built-In Reputation Analysis

Guardicore's reputation analysis capability is aimed at identifying threats based on suspicious domain names, IP addresses and file hashes associated with known malicious activity. Non-conforming or unauthorized communications are indicators of compromise—for example, malware installed on a server and attempting to communicate with a known bad IP address or domain name. The Blue Bastion service leverages Guardicore's vast network of attack sensors and deception engines, combined with regular threat intelligence feeds and the insights of Guardicore security analysts to identify "good" and "bad" IoCs, indicating the presence of untrusted activity that warrants investigation. In combination with dynamic deception, reputation services provide real-time alerts with an extremely low false-positive rate, leveraging insights that include detailed information about the attack.

Why Blue Bastion Chose Guardicore

In selecting the technology to bolster its MDR offering, Blue Bastion set forth a list of "must-haves" that included:

- Maximum visibility (preferably up to Layer 7) for data centers and public clouds
- Real-time detection of lateral movement
- Threat intelligence and reputation feeds
- Micro-segmentation capabilities to shrink the attack surface and prevent compromise of assets
- Support for multi-customer deployments, allowing end customers to control some of the functions within the platform

Guardicore was the only vendor with a platform that delivered on all these requirements, with the added benefit of dynamic deception. “It was either Guardicore or a stack of technologies from two or three different manufacturers,” says Bussard. “That wasn’t going to work for us.”

The Guardicore Centra platform with Guardicore Centra visibility serves as the centerpiece of Blue Bastion’s technology tool set. The firm uses Guardicore to bring visibility to customer data centers and cloud assets that had been previously lacking, and to implement micro-segmentation to protect against unauthorized lateral movement.

The Right Partner Makes the Difference

The marketplace for managed security services is changing quickly. The movement of traditional data centers to hybrid cloud infrastructures poses new and more complex challenges for enterprise customers who need to secure their valuable assets. Conventional perimeter defenses won’t protect workloads and applications as they migrate among multiple cloud environments. Those assets become ripe targets for attackers who have become adept at exploiting a critical blind spot in data center defenses, namely lateral traffic movement. Security professionals need to shift their attention to protecting the assets themselves within the data center.

MSSPs with the agility to pivot toward these challenges stand to gain a significant competitive advantage. The trick is having the right answers, the right tools and the right partner. Guardicore has spent years honing a solution set uniquely designed to address changing data center security requirements - the industry’s only integrated platform encompassing micro-segmentation, threat detection and incident response. As the Blue Bastion experience demonstrates, partnering with Guardicore is a way for an MSSP to quickly add significant value to its offering, and deliver the combination of deep visibility, process-level protection, SOC efficiency and compliance readiness that enterprises demand today.

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**

Guardicore