guardtime

Black Lantern™ Security Appliance

Anti-Tamper Hardware Platform

What is Black Lantern Security Appliance?

Black Lantern Security Appliance is an integrated hardware and software platform, purpose built to mitigate both remote and physical attacks against your infrastructure and applications. Black Lantern completely changes the protection paradigm by being able to identify, defeat, deter, and react against nation-state level reverse engineering attempts or cyber-attacks against both itself, its hosted applications and your network-based critical assets.

Black Lantern is a Hardened KSI® Gateway

Black Lantern Security Appliance comes with a built in KSI Gateway running in protected environment to ensure continued operations even when your infrastructure expands into areas where you may no longer have physical control over the hardware. Black Lantern guarantees the integrity of your system, and proves it through the KSI instrumentation.

Black Lantern is a Highly Secure Compute Platform

The Black Lantern combines the usual capabilities of an Application Server with additional metro-class encryption, communication, and active defense measures. Black Lantern Products are capable of defending themselves from Advanced Persistent Threats regardless of deployment location or physical access to ensure QoS and SLA for the applications it hosts.

Not only can Black Lantern protect itself against remote attacks, it is also capable of defending itself from physical attacks – where an attacker has the device on a reverse engineering bench.

This level of hardening is an industry first, and absolutely necessary when your infrastructure expands into areas where you no longer have physical control over the hardware. Even when you have physical control over the hardware, the threat of malicious insiders still exists. Black Lanterns are designed to survive in the most harassing environments.

Black Lantern Hard- and Software

Black Lantern software is digitally signed and encrypted at rest with KSI and NIST / ETSI approved encryption algorithms. The hardware is incapable of executing unsigned code - it will not boot if the software and hardware runtime environment is not authentic.

Black Lantern uses advanced ASICs with customized tamper protection features and escalation reaction monitors for added security given a variety of physical attack vectors.

The hardware is also resistant to cryptanalysis attacks, such as statistical power analysis on invasive attacks. All of the executable software is monitored during run-time; it's monitored by both, software and hardware. This mitigates threats relating to the use of "mod chips" for the purposes of altering data streams in and out of the Security Appliance. End-to-End protection and resilience is afforded to guarantee delivery of your services.

In addition to the active monitoring of executable code during run-time, the architecture prohibits the introduction of executable code after the software has been authenticated, decrypted and executed. All executable code is read-only, through custom processor enforcement with hardware-based tamper reactions.

Latency for Incident Response becomes sub millisecond due to hardware adaptation and acceleration of your application code. Importantly, Black Lantern cannot be manipulated to attack other systems in your network infrastructure.

Connectivity

Communication channels are authenticated and encrypted using ephemeral keys with perfect forward secrecy. This means that if an attacker recorded any of the Security Appliance traffic, they could not decrypt it.

All traffic to and from the Security Appliance is also encrypted to protect against side-channel attacks.

Resiliency

Black Lantern defends itself from denial of service attack by policing traffic at the data-link layer (OSI layer 2). The Black Lantern's layer 2 is content-aware - meaning it can identify specific traffic and de-prioritize everything else. This ensures that Black Lantern can sustain its performance while it is the target of a Denial of Service attack.

It is also possible to throttle traffic from a single client node in the event that single device attempts to flood the Black Lantern with requests. Since our network stack is content-aware at the hardware level, we can rapidly identify and report any traffic that might indicate the presence of a rogue device in an infrastructure.

This means that your services run by Black Lantern will remain uninterrupted under the harshest of conditions.

Hardware Features

- PPC based real-time operating environment with JVM runtime
- Secondary x86 based operating environment, monitored by real-time integrity hooks over the PCIe bus
- Hardware encryption SoC
- Real-time, high-precision networking with multiple 10G fiber and 1G copper interfaces

Black Lantern Protects Assets Against:

- Advanced Persistent Threats (APT-s)
- Privileged Unlawful Access (Insider Threat)
- Distributed Denial of Service (DDOS)
- Side Channel Attacks
- Introduction of Executable Code
- Boot Code, Service and Operating System Modification
- Physical Access to Hardware
- Low-Level Reverse Engineering
- Cryptanalysis Attacks
- Zero-day Exploits

Selected Use Cases:

- Hardened KSI Gateway for provisioning of KSI services in austere environments
- Hardened Application Server for processing and storage of PII or other sensitive information
- Runtime environment for selected mission critical application components

info@guardtime.com
guardtime.com

guardtime