Solution Brief

[redacted]

ThreatOptix Ultra: The Most Advanced Linux Defense Technology

ThreatOptix Ultra

ThreatOptix has developed Ultra, a novel threat protection suite, including both threat detection and automated incident response.

Utilizing a persistent light-weight agent, as well as a zero-installation Scouter, Ultra protects a wide array of Linux devices - everything from cloud containers to on-premises servers and embedded appliances.

The Ultra technology has been engineered from the ground up to mitigate Linux attacks. As a result, Ultra has a very low footprint on both hosts and networks. Ultra is designed to be used on performance- and mission-critical systems that other solutions fail to protect.

Once a threat is detected, the Ultra suite has a set of automated incident response tools to mitigate even fileless threats and restore systems to normal operation.

Key Capabilities

Advanced Detection

ThreatOptix Ultra ingests data from an array of customizable sensors and then utilizes ML to behaviorally detect both known and yet-unknown threats, uniquely providing attribution, and keeping alert fatigue down.

This treasure trove of data can be fed into the Ultra protection tools to remediate the threats, as well as be fed into other existing systems to integrate with existing SOC process and tools.

Ultra can target a wide array of systems, including x64, ARM64 and MIPS.

Capabilities Include:

- Persistent monitoring using Agent technology
- Detects known and unknown malware attacks, with no run-time limitations
- Recognizes code similarities and identifies who is behind the attack in real time
- Behavior detection based on real-time events
- Network discovery (wireless/wired), mapping surrounding and server's inventory
- Breach detection, determine infection radius
- Memory Analysis, detect diskless threats, exploitation attempts, process injections
- Real-time Network analysis and a fully integrated intrusion detection technology with EDR capabilities

Advanced Protection

Data gained from continuous monitoring by the Ultra sensors can then be used to both undo damage done by threats, **including file deletion** – as well as be used to generate IR reports for further investigation and root cause analysis.

Intelligent Monitoring

- Events for Data Investigations such as full process memory snapshot, memory threat analysis
- Network intrusion detection capabilities
- Wireless network analysis

Cloud Protection and Monitoring

- Containers and Microservices ready - no installation needed
- Quick and seamless deployment, compatible with Kubernetes, AWS

Seamless Deployment with Blistering performance

- ThreatOptix's advanced Linux protection provides seamless deployment and interoperability.
- High performance: ThreatOptix technology is written in machine code without any preliminary requirements. This reduces operational costs and energy consumption.
- Compatible with 3rd party logging technology, deployment takes minutes
- Agentless technology, zero installation and extremely high performance
- Not cloud dependent, on-premises, appliance and virtual machines instance

Reduce SOC work – less noise, intelligently distill actionable information from the network and Linux hosts

Information Collection

Collecting information from the network

Simple initial setup, on top of existing management infrastructure

Agent

Lightweight persistent information collection

Scouters

Read-only information collection from Linux hosts

Breach Detection & Blast Radius

Once a threat is detected, the Ultra suite has a set of automated incident response tools to mitigate even fileless threats and restore systems to normal operation.

Get a demo

Contact us at: hello@threatoptix.ai