PRODUCT OVERVIEW

Endpoint Threat Analytics Module

LogRhythm
The Security Intelligence Company

Endpoints have long been a frequent targets for attacking the network because of the numerous ways that they can be compromised. Attackers employ a variety of methods to infect desktops, laptops, servers, and mobile devices, including watering holes/phishing/spear phishing scams, and malicious websites as part of a "land and expand" strategy to compromise the organization. Yet despite the obvious need for endpoint behavioral analytics, particularly with the proliferation of the mobile workforce and extensive adoption of BYOD policies, in many organizations it has lagged behind a reliance on traditional, signature-based products for endpoint threat protection. When faced with increasingly advanced and rapidly evolving custom malware and zero day attacks, a more sophisticated endpoint monitoring solution is a crucial component of any holistic security intelligence program.

Endpoint Analytics

- ☑ Malware Detection
- ☑ Configuration Assessment and Monitoring
- ☑ Compromised Host Prevention
- ☑ Security Best Practice Enablement

LogRhythm's Endpoint Threat Analytics module helps organizations quickly detect and respond to the threats targeting their endpoints and discover when compromised devices are being used for malicious activity by attackers. The Endpoint Threat Analytics module includes a sophisticated set of advanced behavioral analytics rules and out-of-the-box alarms that deliver a holistic picture of threats targeting the endpoint. This provides security administrators with the visibility to quickly find devices that are being attacked or already compromised with all relevant event context, drastically reducing the time it takes to neutralize the threat before extensive damage occurs.

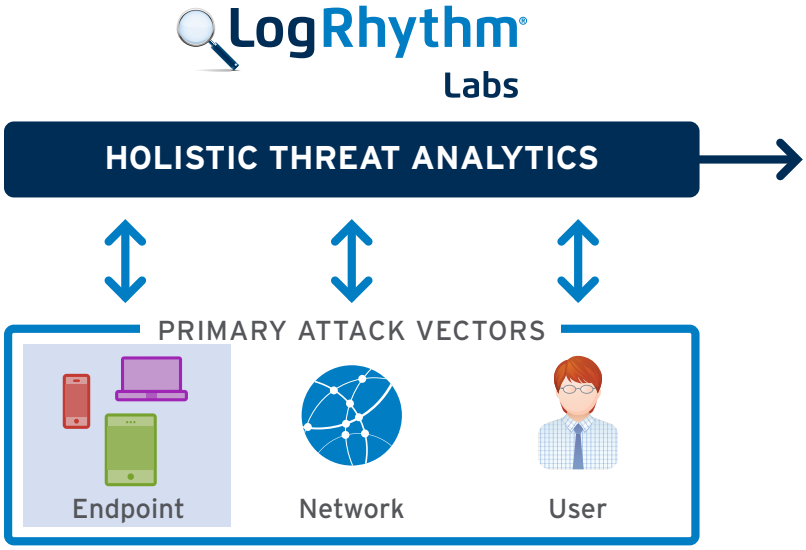
How It Works

The Endpoint Threat Analytics module analyzes existing host logs and data collected from LogRhythm's System Monitors, using a comprehensive collection of advanced behavioral analytics rules for LogRhythm's AI Engine that detect, prioritize and neutralize threats targeting an organization's endpoints. In addition to detecting malware activity and malicious behavior tied to zero day attacks, the Endpoint Threat Analytics module is able to find unauthorized local accounts, misconfigurations and changes to access privileges suggestive of local account abuse and endpoint compromise. The module comes with a straightforward deployment guide with recommended tuning and setup instructions for simple adherence to best practices and rapid ROI.

Malicious Software
- Malware Outbreak
- Abnormal Process Activity
- New AutoRun Process
- Novel Software Installation
- Local Security Override

Host Access Attempts
- Pass The Hash
- PowerShell Execution
- Local Account Created And Used
- Multiple Object Access Failures

Windows Firewall Events
- Multiple Firewall Changes
- Process Added To Firewall
- Firewall Rule Added/Modified
- Security Event Then Firewall Change



The sheer volume of endpoint devices in an enterprise network, each of which is a potential access point for attackers, creates a plethora of holes in any organization's network defenses. LogRhythm's Endpoint Threat Analytics module takes a comprehensive approach to real-time monitoring and analysis of endpoint behavior using a variety of techniques to defend the network from endpoint based attacks. It empowers customers by detecting the initial security event, prioritizing which activities pose the greatest threat, and initiating automated actions to neutralize attacks before they cause significant damage.

Endpoint Manipulation: Once attackers have compromised an endpoint, they will use it as a platform for running software to automate additional malicious activity. The Endpoint Threat Analytics module uses a number of techniques to detect activity indicating that an external attacker has breached perimeter defenses or that a malicious insider has launched an attack from within. It includes out-of-the-box behavioral analytics rules that alert security administrators to unusual endpoint activity, such as unauthorized software installation, new AutoRun processes or suspicious Powershell activity tied to malware activity. All alarms provide immediate drilldown access to a complete set of forensic detail for rapid remediation.

System Configuration Changes: Attackers facilitate propagation throughout an enterprise network by making configuration changes to endpoints that make it easier to perform malicious activities. LogRhythm's Endpoint Threat Analytics module is capable of detecting an extensive number of subtle changes to endpoints and alerts security administrators for further investigation. It delivers multiple out-of-the-box rules that can detect changes to host firewalls, directory services, the Windows registry, network access, and host system/security monitoring processes in real time. These events are automatically correlated against an extensive array of user and network data to identify who initiated the action and from where for immediate remediation.

Communication with Suspicious IP Addresses: Network communication to suspicious IP addresses and IP ranges is an excellent indicator of a malware outbreak or successful breach, yet many organizations have no way of automatically detecting when suspicious traffic is associated with known bad actors. LogRhythm's Network Threat Analytics module delivers several out-of-the-box rules that detect suspicious network activity and can automatically match that data against up-to-date threat intelligence data delivered by the LogRhythm Threat Intelligence Ecosystem. These rules automatically surface by prioritizing which activity is the most threatening, including network communications to/from blacklisted or non-whitelisted geographic.

Host Firewall Monitoring: Malware is frequently designed to covertly open lines of communication with an external destination, such as a command and control system, to create a sustained point of contact for continued malicious behavior. LogRhythm's Endpoint Threat Analytics module includes rules specifically designed to detect the addition of new processes, such as to a host firewall, changes to firewall configuration rules (add/edit/delete rules) in conjunction with other suspicious events, multiple firewall changes in a short period of time and more. Immediate detection of unauthorized changes to device firewall configurations immediately exposes clear indicators of compromise and allows security administrators to respond to endpoint breaches before they can cause more extensive damage.

Malware Activity: Custom malware is frequently designed to hide its footprint by not logging process activity or by altering activity logs after the fact. The Endpoint Threat Analytics module leverages forensic data provided by LogRhythm's Endpoint Monitor to detect malware that has evaded traditional detection before it can cause major damage. The module includes several rules that alert security administrators to unusual software activity, such as a non-whitelisted processes starting on an endpoint. Additional context that identifies critical or vulnerable endpoints reduces false positives and automatically prioritizes events. An out-of-the-box SmartResponse plug-in can immediately stop any unauthorized process before it causes any damage.