DATA SHEET

GURUCUL

zscaler™

Gurucul Security Analytics and Operations Platform Integrates with Zscaler Solutions

Advanced Threat Detection and Response

Gurucul Security Analytics and Operations Platform encompass advanced threat detection models powered by both trained and adaptive machine learning (ML) models, unlike other solutions that rely solely on rule-based correlation. Gurucul detects the full scope of high-priority, malicious attack campaigns, and can take the necessary steps to eradicate the attack from the environment before cybercriminals or malicious insiders can inflict damage. The Gurucul platform automatically collects, correlates, enriches, and stores data from applications, platforms, network, and threat intelligence. With this comprehensive set of contextual security information, the platform then applies its behavior analytics models. The models are both pre-tuned and adaptive to detect threats aligned with specific use cases, data telemetry, industry verticals, as well as threat and compliance frameworks (MITRE, PCI-DSS, etc.). While other solutions are 100% black box, Gurucul is the only solution that is 100% transparent, open, and customizable, allowing users to create models, workflows, and playbooks.

The Challenges with Current Threat Detection and Investigation Platforms

Existing point cybersecurity solutions don't provide actionable context about risks they may detect. Conventional technologies focus on events, and event correlation, providing filtering, rules, and basic analytics to display alerts. Unfortunately, most products still flood the Security Operations Team with a myriad of false positives and unseen true positives. This makes it hard to identify the actual risk.

Gurucul takes a different approach, with a highly versatile security platform built on a foundation of analytics, across a wide array of telemetry, and data sources that are focused on delivering prioritized risk, through contextualized correction. The solution prioritizes high-risk users and entities, reducing analysts' workload significantly. Instead of investigating hundreds of alerts from silo products, analysts are provided with a small number of high-priority, high-fidelity, highly accurate threats to investigate.

Gurucul's Enterprise Risk Engine for Validated Risk-Driven Response

While Gurucul detects and performs threat-hunting use cases with its machine learning and data science techniques, the platform also introduces much more relevant context and incorporates risk scoring as it integrates with the Zscaler Security Service Edge (SSE) platform. Gurucul assigns a risk score for every user and entity for which anomalies are triggered. Gurucul uses a risk-based approach to help analysts prioritize incidents for investigation, which enables customers to achieve a 90%-95% efficiency rate for true positive and impactful incidents to improve the variety and quality of investigations.

Integrations

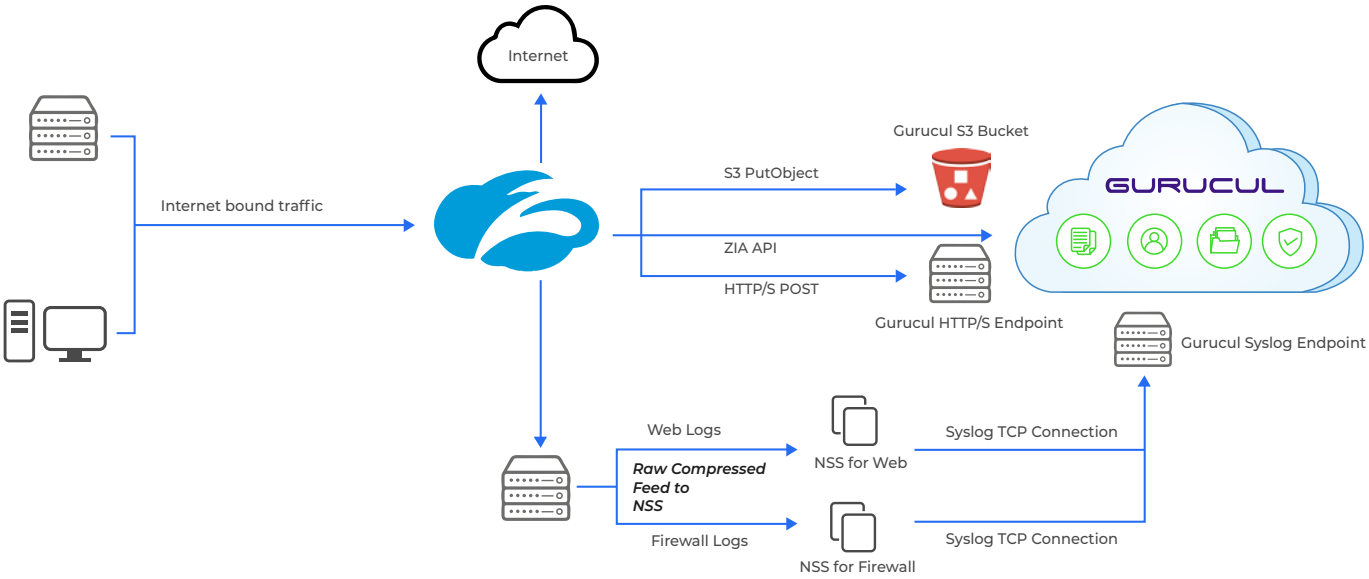
The Gurucul Security Analytics and Operations Platform drives high-efficacy threat detection and automated response with machine learning-based behavior analytics. There are several integrations with Zscaler solutions, all focused on detecting risky anomalous behavior before a malicious actor can do harm.

- ML-based models for detecting network and behavior anomalies
- Provide enriched context, along with other event sources, to detect compromised users and hosts
- Alert prioritization using risk-scoring
- Threat intelligence enrichment for known malicious sites and dark web activity

Supported Data Ingestion Mechanisms

The Gurucul Platform has native integration with Zscaler using the following ingestion mechanism:

- SIEM Connector that provides a consumable data stream in syslog.
- S3 Bucket
- 3rd party SIEMs, such as Splunk



Use Cases

Zscaler Private Access

Remote access solutions are subject to external attacks, such as brute force, tracking user location, which can be performed based on the geolocation. Gurucul can ingest Zscaler Private Access events and feed these into the UEBA to detect abnormal password guessing, brute force, and account validation through location abnormalities. Location anomalies are also extended to simultaneous multi-user login checks.

Zscaler Advanced Threat Protection

As part of the Zscaler Internet Access suite, ZIA provides, among other capabilities, advanced threat protection, looking for in-flight abnormal and malicious data patterns and identifying known behavior, such as malware, and command and control network activity. This data is fed into the Gurucul Platform and correlated with behavior, identity, and other malicious activities to pinpoint breached user accounts used in advanced attacks.

Zscaler DLP

The DLP portion of Zscaler Internet Access suite controls documents in accordance with corporate policies. Where users are remotely dispersed, the Zscaler Internet Access DLP can check and report on the movement of cleartext and encrypted documents to drop locations, such as unsupported cloud storage accounts. Details of how documents are handled are one piece the Gurucul Platform uses to detect abnormal behavior and TTPs, leading to the detection of attacks, such as data exfiltration and insider threats.

Zscaler Cloud Sandbox

Gurucul ingests sandbox data, such as file hash, file description, etc., from Zscaler Cloud Sandbox and feeds this metadata into its malware classifier to understand the intent and risk behind known malware. Based on the type and severity of the identified malware, the Gurucul Platform can further increase a user's risk score. The integration ensures timely analysis and detection of threats to improve the productivity of analysts by providing additional contextual information to investigate, analyze and respond to malicious attacks where malware may have been used.

Zscaler Cloud Firewall

Zscaler Cloud Firewall data is used to track and verify inbound and outbound transactions, such as a proxied connection, where the outbound connection is verified against a 3rd-party reputation list. In this scenario, the connection is allowed by the proxy, but dropped by the URL filtering function on the firewall. Gurucul tracks both parts of the data flow through events, reducing the overall impact on the user when the firewall disallows the connection. The fact that the host is manifesting behavior detected as C2 raises the initial alert level, but due to the firewall containment, the overall priority is reduced. Analysts have access to all event data needed for forensic analysis if a breach occurs The Gurucul Platform speeds-up investigations by allowing

analysts to sort, group, and filter the log data related to a specific incident. Integrating Zscaler Cloud Firewall with the Gurucul Platform allows analysts to quickly identify a breach and recover quickly.

Enhanced Detection of Phishing Attacks

Spear phishing is the most common way to gain unauthorized access to any environment. Typically, upon receiving a spear phishing email with a malicious link, the next-gen firewall and/or sandbox would have analyzed the email looking for malicious content, a link to a known site, checking the email sender against any rough reputation lists. Likewise, any sandbox would look for abnormal behavior, or suspicious email recipient, text mining, etc. The firewall or proxy would check the destination website once the link has been clicked. If the URL is an unknown or uncategorized site, the zero-day URL would be ruled out by the firewall, and since the email recipient spoofed, it would be ruled out by the sandbox. If the link was clicked and the site was on a known URL list, it would have been dropped by any firewall reputation or Proxy URL filtering, but this is after the fact and a single point of reference.

The Gurucul Platform would see the same malicious email, under a different lens than the sandbox, firewall, and proxy. In this scenario, the focus would be on the email itself and if a link was clicked, similar user behavior techniques would also be applied. Gurucul would ask the following questions about the origin, any subject or body text, user/peer behavior in the context of the email, and any links:

- Why would only these recipients receive this email when the content should also be received by other peers? Peer group-based activity deviation behavior analytics would be applied here.
- Why is the link in the email uncategorized? Persona behavior plus reputation lookup analytics would be applied here. For example, normally this user goes to football (Manchester United 99.9%), business (Gartner 68%, Forrester 32%), and news sites (BBC, 98%, CNN 2%), but the link in the email has no category, especially in accordance with the user behavior and the email sender.
- Why would this host visit this website when the user/identity doesn't normally visit this category? Abnormal host behavior by the user's day-to-day activities would be analyzed.
- Look for unusual character sequences based on text mining.

Anti-Malware

After the URL and email delivery use case, the Gurucul Platform uses the MD5, SHA256 to identify any potential malicious executable. This action provides a description, like Remote Access Trojan, IMBot, Screen Scrape, PUP, and so on, for the malicious file. Gurucul not only ingests the sandbox classification but also indicates the hierarchical differences between the impact of the malware types and scores them according to their associated impact or risk.

By combining behavioral analytics with reputation data, the system can put events like Spear Phishing into the context of the user and any peer behavior, highlighting abnormalities in the content. The Gurucul Platform uses cross-product data, network activity, user activity, and peer activity to add context to each event and classify its authenticity.

User Enrichment

Zscaler allows external 3rd-party components to pull user information stored from a wide range of repositories. Gurucul can interface with the API to obtain user-to-host mappings from a variety of sources with a single API call.

Response Capabilities

Since Zscaler is an SSE platform, the use of outbound application filtering is paramount to securing identified malicious patterns, such as C2 out to the web, internal exfiltration (T1048) between enclaves, and/or exfiltration out to web services (T1567.002). Other indications of compromise can be controlled, but are usually short-lived and controlled by global policies, such as brute force attempts, horizontal and vertical scans, as well as abnormal protocol usage.

For more information, please visit https://gurucul.com.

About Gurucul

Gurucul is a global cyber security company that is changing the way organizations protect their most valuable assets, data and information from insider and external threats both on-premises and in the cloud. Gurucul's real-time Cloud-Native Security Analytics and Operations Platform provides customers with Next Generation SIEM, XDR, UEBA, and Identity Analytics in a single unified platform. It combines machine learning behavior profiling with predictive risk-scoring algorithms to predict, prevent, and detect breaches. Gurucul technology is used by Global 1000 companies and government agencies to fight cybercrimes, IP theft, insider threat and account compromise as well as for log aggregation, compliance and risk-based security orchestration and automation for real-time extended detection and response. The company is based in Los Angeles. To learn more, visit gurucul.com and follow us on LinkedIn and Twitter.

Gurucul | 222 North Pacific Coast Highway, Suite 1310 | El Segundo, CA 90245 | 213-259-8472 | sales@gurucul.com | www.gurucul.com