Technical Validation

Comprehensive Security for Modern Web Applications and APIs with the ThreatX WAAP Platform

Deploying a Cloud-based, Attacker-centric Approach for Real-time and Scalable Prevention and Protection

By Alex Arcilla, Senior Validation Analyst

October 2021

This ESG Technical Validation was commissioned by ThreatX and is distributed under license from ESG.

Introduction

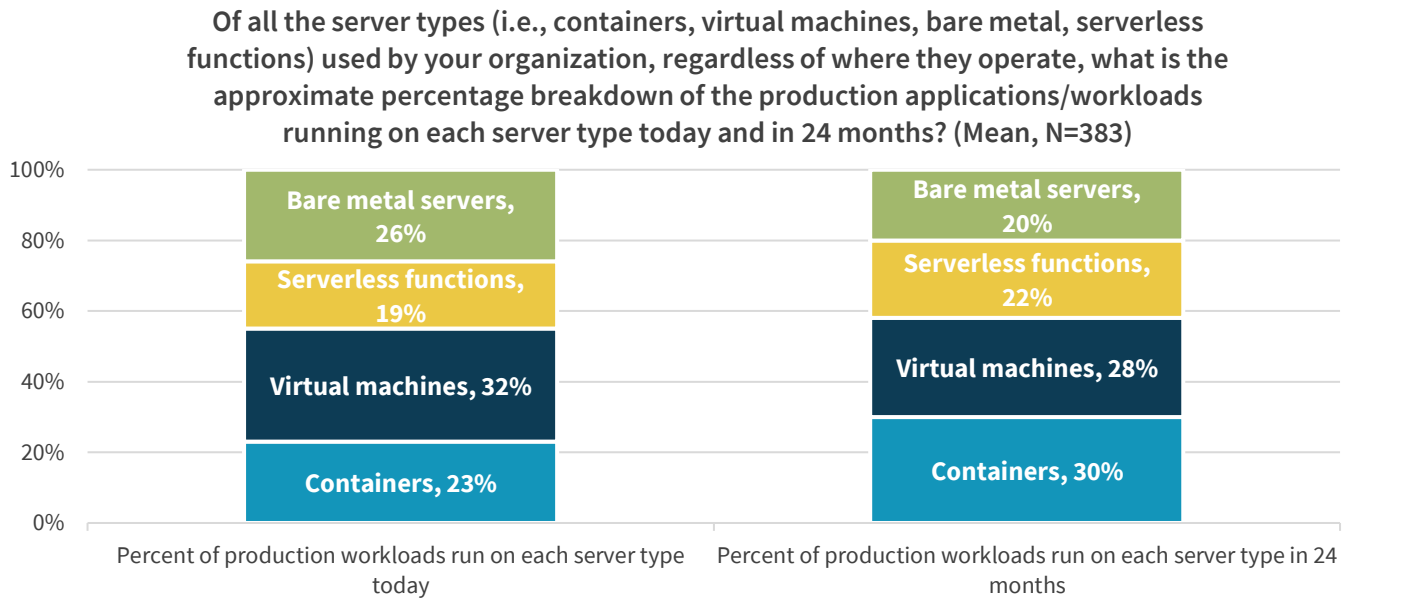
This ESG Technical Validation documents our review of the ThreatX Web Application and API Protection (WAAP) platform. We evaluated how the cloud-native, attacker-centric platform can help organizations to comprehensively secure applications without the need to augment their existing security program with additional tools or products.

Background

To speed up application development and deployment, organizations are increasingly using containers and microservices architectures so that they can meet business needs with little delay. As a matter of fact, ESG uncovered that, by 2023, organizations expect to increase their usage of containers—from 23 to 30%—while simultaneously decreasing their use of bare-metal servers—from 26% to 20%—when deploying applications, as shown in Figure 1.[1]

As organizations rely less on monolithic application architectures, organizations must now contend with a disjointed and dynamic attack surface, especially when deploying applications in the public cloud. No longer can organizations depend on a traditional web application firewall (WAF) for application security, especially when attacker techniques evolve and multiply. One attacker may end up requiring a multitude of WAF rules, which can lead to unwanted false positives, maintenance complexity, and management costs.

Figure 1. More Organizations Relying on Containers by 2023



Source: Enterprise Strategy Group

Cyberattacks and threats on today's application architectures are more sophisticated, as they utilize numerous techniques that can span multiple phases of an attack—from reconnaissance to data exfiltration or system corruption. Traditional WAFs have become less effective, as they only filter out and prevent known, signature-based, and isolated attacks. And as ESG research found, 31% of respondents indicate that a top challenge for securing cloud-native applications is a lack of understanding of the threat model faced today. WAFs are also less effective since they are ideal to protect a handful of applications but do not scale easily to handle an increasingly complex set of rules as the number of first- and third-party applications grow.

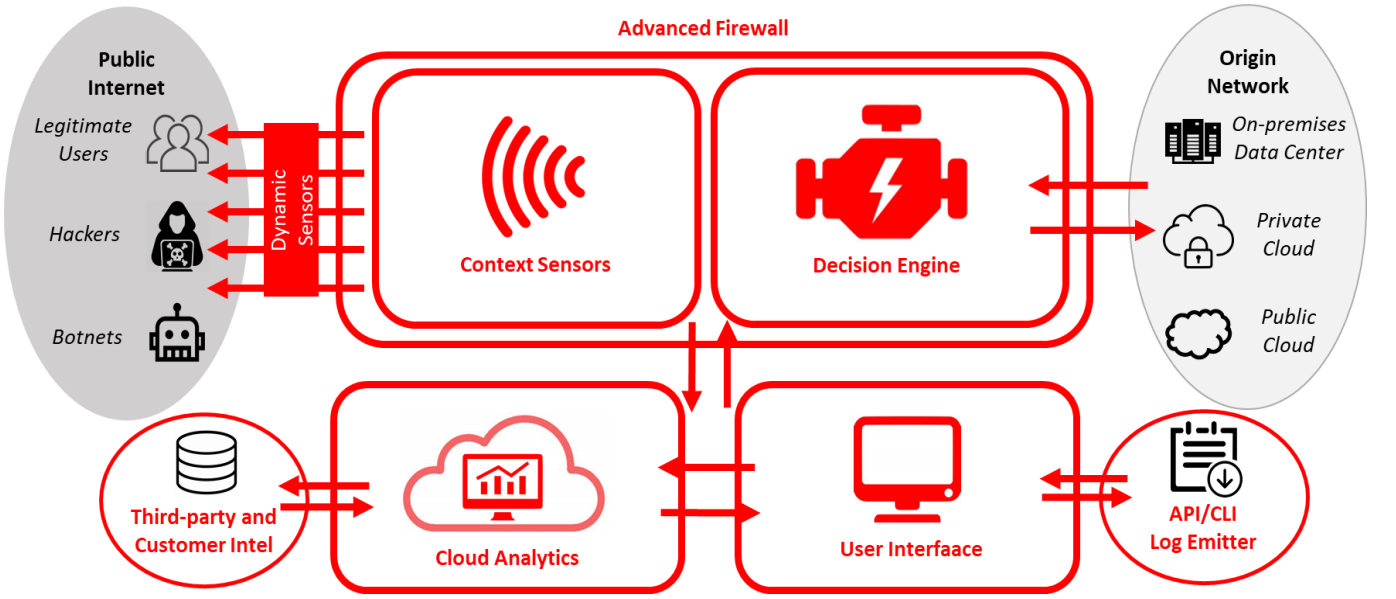
[1] Source: ESG Master Survey Results, *The Maturation of Cloud-native Security: Securing Modern Apps and Infrastructure*, June 2021. All ESG research references in this technical validation have been taken from this master survey results set.

ThreatX WAAP Platform

The ThreatX WAAP platform, offered as a cloud-hosted managed service, is designed to identify and mitigate Layer 7 cyber-attacks while minimizing false positives. Unlike WAFs that protect only against known signatures and attacks, this platform uses an attacker-centric behavioral risk model to protect cloud-based applications against unknown or zero-day attacks, including DDoS, Bot-based attacks, API abuse, and exploitations of vulnerabilities. Deploying and scaling the platform to protect any number of applications deployed on-premises or in public and private clouds is simple with its Docker-based architecture.

The ThreatX platform consists of (see Figure 2):

Figure 2. The ThreatX Security Container



Source: Enterprise Strategy Group

- Context sensors – Deployed at or near the origin application server, the reverse proxies scan all incoming traffic and requests generated by end-users, hackers, or botnets to detect and log possible security events. The sensors use a variety of tools such as application and API profiling, an advanced parsing engine, and flow validation. When appropriate, the sensors will engage progressive IP interrogation techniques to identify and fingerprint "users." This interrogation helps delineate humans versus bots and compares and correlates across multiple inbound IPs.
- Decision engine – Leverages behavior-based security software developed with embedded intelligence to evaluate inputs from multiple context sensors (over time) to determine behaviors that may represent malicious intent. Risk scores are calculated to determine the appropriate actions to be taken against specific attackers.
- Cloud analytics – Analyzes data continuously collected from the entire network of deployed sensors, as well as third-party and customer intelligence, and identifies attack patterns in real time across the security kill chain. New entities and the suspicious behaviors are updated in the cloud platform and distributed to the entire network of deployed sensors. This includes inputs from daily vulnerability testing performed by ThreatX support teams.
- Advanced firewall – Based on threat intel, behavioral signatures, and updated risk scores from the decision engine, manages appropriate responses ranging from continued monitoring, blocking, interrogation, tarpitting, or blacklisting/whitelisting traffic before entering the organization's network.

- **User interface dashboard** – Supports how application owners and security operations center (SOC) analysts administer and manage applications and APIs. This tool is used to respond to identified attacks and threats, with features such as notifications, attack prioritization, and risk metrics, and report on related trends.
- **Proactive security operations center (SOC) support** – Provides proactive notification of threats and attacks crowdsourced across multiple ThreatX customers and consultation on recommended remediations and best practices.

Because the ThreatX WAAP platform focuses on preventing attackers from compromising network and application security, organizations no longer have to purchase and integrate multiple security products that focus on specific tasks, such as DDoS and bot protection, decreasing cost, operational complexity, and overall risk.

ESG Technical Validation

ESG performed evaluation and testing of the ThreatX platform remotely on a variety of applications and APIs deployed in a public cloud environment. We observed how the ThreatX platform delivers fast time to value, decreases false positives, and provides actionable insight.

Fast Time to Value

While organizations can purchase point solutions addressing different attack types, the onus is on the organization to integrate these disparate tools so that they share data and provide a comprehensive, easy-to-consume view of security risk across an enterprise network. Integrating such tools in-house is not easy to accomplish and can create visibility gaps.

The ThreatX platform operates with a single-risk engine that correlates attack activity across a variety of tactics, techniques, and procedures (TTPs) so that individual attackers, or entities, are identified. All components of the ThreatX platform share and act upon the same data, enabling organizations to gain a unified and comprehensive view of current attacker activity and the risks posed to the organizations' applications in a short period of time.

ESG Testing

ESG began with the Live View of the ThreatX dashboard, showing the current state of application security. (An Explorer View enables a security administrator to view historical data over a desired timeframe.) After choosing to view data over the past 12 hours[2] across all domains, we noted the information that the dashboard communicated at first glance, including (see Figure 3):

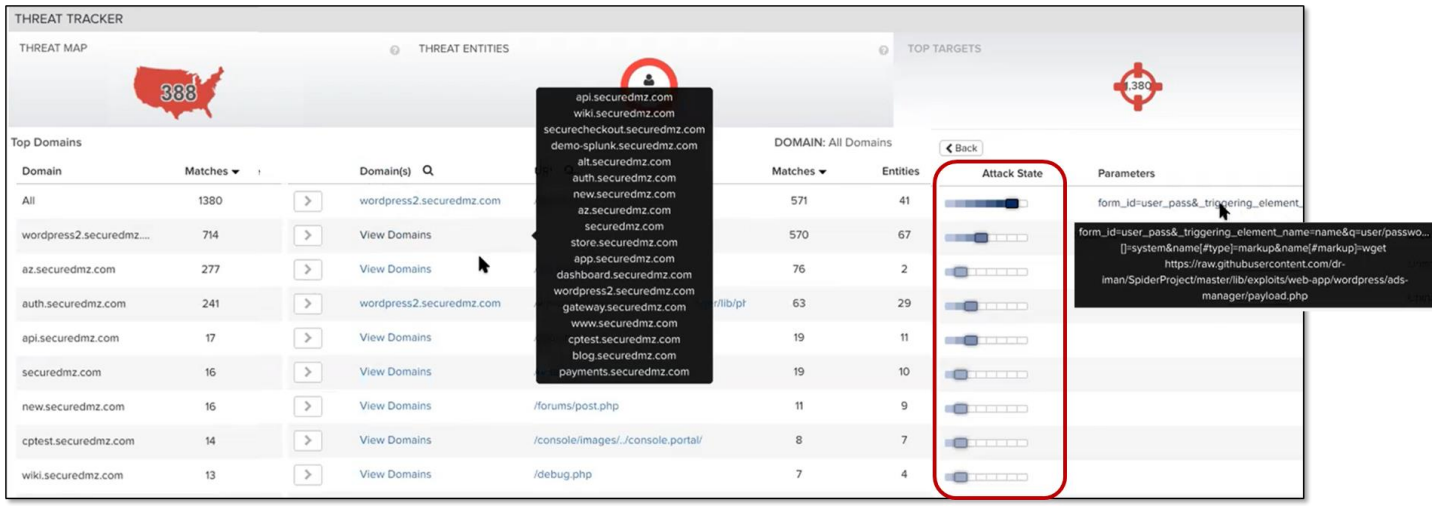
- The overall threat score, accounting for all entity activity, recorded every 15 minutes (displayed as the line chart).
- Key metrics, specifically **Suspicious Matches**, **Suspicious Entities**, **Blocked Entities**, and **Blacklisted Entities**.
- Top attack entities by location with associated threat risk score.
- Global map denoting application traffic, color coded to indicate overall security risk (with green meaning least risk).

[2] All ThreatX software interface figures in this report use data from the same 12-hour timeframe defined at the beginning of ESG's evaluation.

Figure 3. ThreatX Live View – Threat Map and Key Metrics

To show the extent of entity activity, ESG navigated to the **Top Targets** view in the dashboard. The identified targets were sorted by those that experienced the most attacks identified by ThreatX (see Figure 4). If more than one domain was attacked, we could hover over the "View Domains" link to see all affected domain names. We could also view attack parameters used by the identified number of entities, such as entering random usernames and passwords.

Figure 4. Examining Extent of Attacks on Domains



To reinforce the magnitude of security risk faced by the identified *Top Domains*, we examined their "*Attack State,*" showing how far along attacks have progressed. While the *Attack States* of many domains were in the early stages (e.g., scanning the organization's application environment, mapping out potential points of entry), the *Attack State* of the first entry revealed that 41 entities have progressed farther, attempting to exploit exposed vulnerabilities. With this intelligence, administrators already know where to focus efforts to minimize security risk.

Why This Matters

According to ESG research, 40% of surveyed organizations find that the prospect of using multiple cybersecurity controls in securing cloud-native applications is a prominent challenge, as this approach will increase both cost and complexity. While point solutions can address specific attack types well, integrating these tools allows organizations to assess the real-time state of application security with a unified set of data.

ESG validated that ThreatX offers organizations faster time to value, as organizations can leverage this single platform to assess the security of their web-based applications without needing to integrate multiple disjointed and vendor-specific tools and their data. We observed how the ThreatX platform provides administrators with a comprehensive view of application security by focusing on the attackers as opposed to single, isolated attack signatures. With this approach, organizations no longer have to write rules for every single attack or threat that occurred in the past. Instead, organizations focus on the entities initiating the attacks and track how widespread those attacks were (such as the number of domains or paths taken) and how they evolved.

Lower False Positive Rate

Experiencing high false positive rates is counterproductive, as organizations waste time and resources remediating events that, while triggering a predefined rule or policy, do not pose any security risk. With the ThreatX platform's attacker-centric approach, organizations can achieve lower false positive rates by focusing on blocking and blacklisting individual entities based on how attack patterns evolved over time, using varying approaches at all stages of an attack.

ESG Testing

We navigated back to the Threat Dashboard (Live View) shown in Figure 3 and focused on the Key Metrics. Based on the Metrics noted by the red boxes, we found 2,144 *Suspicious Matches* to existing security rules, then grouped and correlated those matches with 275 *Suspicious Entities*.

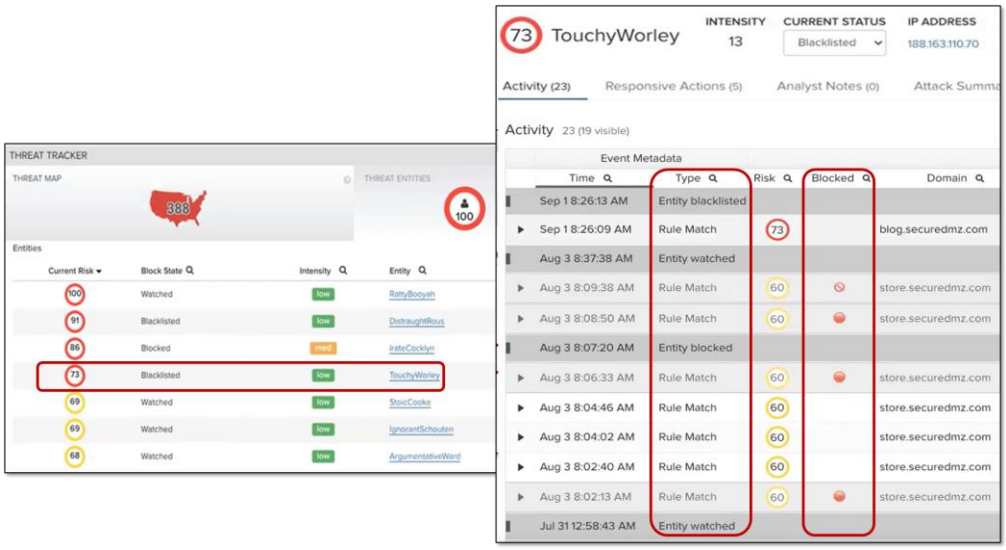
Of those *Suspicious Entities*, one was noted as a *Blocked Entity*. To move to the *Blacklisted Entities* list, the platform used baseball's "three-strikes" rule. When an entity moved to the *Blocked* state, it remained within that state for 30 minutes. If both security administrators in the organization and the ThreatX customer support team determine that the entity exhibited continuing damaging activity, the entity would be classified as a *Blacklisted Entity* and denied access. If not, the entity would no longer be classified as *Blocked*. However, if the entity entered the *Blocked* state two more consecutive times, that entity would be placed onto the *Blacklisted Entities* list.

ThreatX names "entities" by combining an old-time pirate name with a modifier to help in remembering that named entity across multiple applications, multiple customers, and especially when attacks are coming from multiple IPs.

This unique identifier drastically improves the visibility of attacks across the ThreatX infrastructure.

ESG observed the three strikes rule in action by first clicking on the "TouchyWorley" entity in the Threat Entities list (see Figure 5). By examining the *Event Metadata* and *Blocked* columns, we saw the actions that ThreatX took against this entity and how the entity was blocked three times before the platform declared it a *Blacklisted Entity*. Following this rule enables both the administrator and the ThreatX customer support team to ensure that the entity is indeed a bad actor and should be blacklisted.

Figure 5. Classifying Entities as "Blocked" or "Blacklisted"



Why This Matters

High false positive rates distract an organization from dealing with vulnerabilities and potential attacks that can damage its security posture and its business operations severely.

ESG validated that the ThreatX platform can decrease false positive rates with its attacker-centric approach to securing an organization's modern applications. We observed that focusing on entities helps to protect against evolving and related attack patterns instead of using static rules to block specific attack patterns and potentially block legitimate traffic or requests. Organizations can increase their efficiency in maintaining their security posture with fewer errors.

Delivery of Actionable Insight

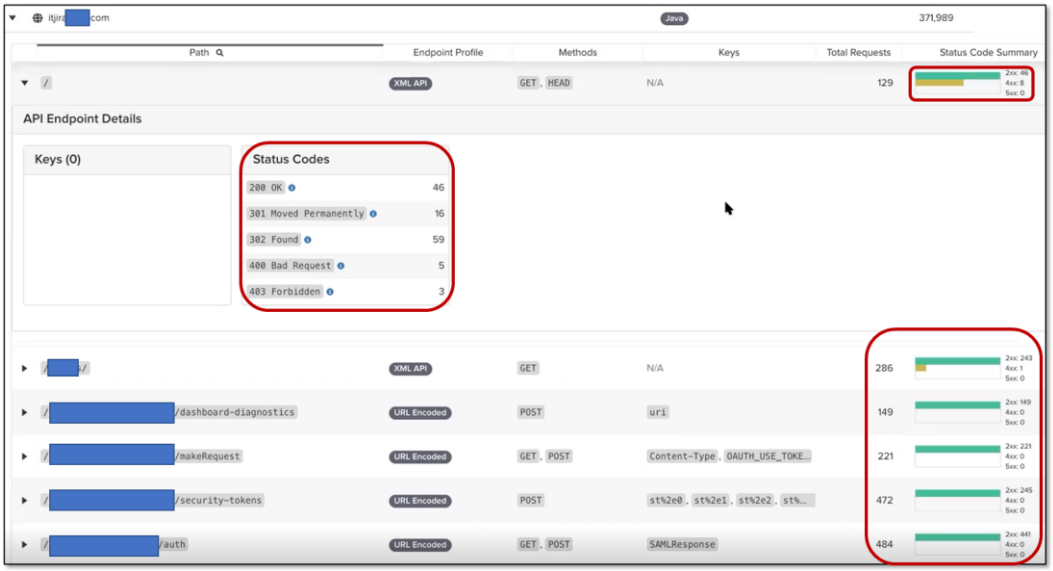
Organizations need actionable insight just as quickly as they need to identify attacking entities and their behavior to mitigate any damage to the business. With the ThreatX platform, organizations can immediately identify where issues lie and act accordingly with little delay.

ESG Testing

One clear example that shows how ThreatX delivers actionable insight quickly was displayed in Figure 4 in the **Top Threats** view. ESG saw that the platform already organized those domains in order of decreasing attack severity. An administrator already knows which domains and paths to examine first to mitigate those attacks and related entities.

ESG also examined how the ThreatX API catalog could provide actionable insight. We navigated to the API Catalog in Figure 6 to view how the API Catalog tallies 200 - 500 HTTP response status codes at the application and API levels. Using this view, we saw that an administrator can already pinpoint both the applications and the APIs that have recorded 400 and 500 status codes, indicating potential malicious activity. With the API Catalog, ESG noted that we were provided with detailed insight so that we could direct our attention immediately to those APIs under possible attack.

Figure 6. Tallying Status Codes for Web-facing Application and Individual APIs



Why This Matters

Identifying who and what has attacked your application environment is one thing, but mitigating the attacks posed by those bad actors quickly is just as, if not more, important to minimizing any damage to your business. Accomplishing this requires gaining actionable insight into malicious activity.

ESG validated that the ThreatX platform delivers actionable insight that organizations can use to determine the proper remediation with little time and effort. Throughout our testing, we observed how the platform identifies those entities and threats that should be addressed first to minimize security breaches. We also saw how the API catalog delivers the same level of insight, enumerating HTTP response status codes at the application and API levels so that organizations know how to direct any corrective action.

The Bigger Truth

Organizations with modern, cloud-native applications face a variety of security challenges to prevent or mitigate bad actors from disrupting business operations. Cybersecurity incidents experienced by ESG research respondents in the last 12 months specifically related to cloud-native applications and infrastructure include targeted penetration attacks, "zero-day" exploit(s) that took advantage of new and previously unknown vulnerabilities, and attacks that resulted in the loss of data due to the insecure use of APIs. As these and other challenges increase and expand, using the traditional WAF and add-on products adds to complexity in security visibility and monitoring. This complexity increases as organizations focus on blocking isolated attacks and requests as they occur and creating individual rules and policies. Ongoing management becomes more complicated and time-consuming and increases the risk of higher false positive rates.

The ThreatX platform has been designed to provide security for an organization's web sites, web applications, microservices, and API endpoints by focusing on mitigating attacking *entities* as opposed to individual and isolated *attacks*. With its single-risk engine, the platform monitors and correlates evolving TTPs with entities so that organizations can identify bad actors from their behavioral patterns at any stage of an attack and remediate with maximum effect.

ESG validated that the ThreatX platform delivers the following benefits:

- **Faster time to value** – Since the ThreatX platform continuously monitors and correlates TTPs with specific bad actors, ESG saw how organizations immediately gain a unified and comprehensive view of current attacker activity and the risks posed to the organizations' applications. We noted that the potential for attack is communicated in numerous ways: organizational threat scores, maps of current entity activity, and prioritized lists of entities and targets.

- **Low false positive rates** – Leveraging both data collected within the organization's application environment and the crowdsourced customer data from the ThreatX customer support team, ESG verified that organizations have better knowledge of entities and their attack patterns. Decisions about blocking or blacklisting entities are made with improved intelligence, thus decreasing the chances of wasting time and resources in blocking legitimate traffic

- **Delivery of actionable insight** – Because the ThreatX platform identifies the attacking entities, where the attacks have occurred within the application's architecture, and how far the attacks have progressed, ESG noted that organizations have improved insight so that they can perform the correct actions to prevent any further damage.

One item that ESG should note is the fact that potential customers may have multiple security tools and products in place with related established processes. It is important that ThreatX continues to show the potential of decreased effort in securing applications so that they are open to change and improvement.

If your organization is looking to secure its web sites, applications, microservices, and API endpoints comprehensively without increasing false positive rates, ESG believes that you should take a closer look at the ThreatX platform.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.