Enterprise Strategy Group™

TECHNICAL VALIDATION

Comprehensive Web App and API Protection With ThreatX by A10 Networks

An On-premises or SaaS-delivered Platform for Real-time, Scalable Prevention and Protection

By Alex Arcilla, Senior Validation Analyst, and Tony Palmer, Practice Director
Enterprise Strategy Group

June 2025

Contents

Introduction 3
Background 3
ThreatX by A10 Networks Web App and API Protection Platform 4
Enterprise Strategy Group Technical Validation 5
Enterprise Strategy Group Analysis 5
Lower False Positive Rate 8
Enterprise Strategy Group Analysis 8
Delivery of Actionable Insight 10
Enterprise Strategy Group Analysis 10
Conclusion 11

Introduction

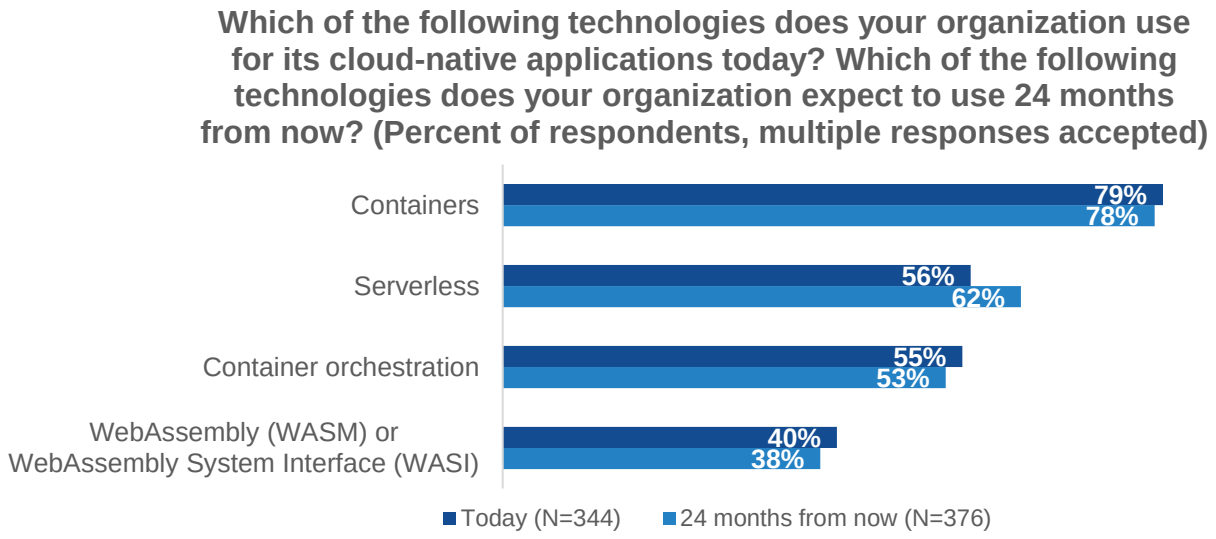
This Enterprise Strategy Group Technical Validation documents our review of the ThreatX by A10 Networks Web Application and API Protection (WAAP) platform. We evaluated how the SaaS or on-prem, attacker-centric platform can help organizations comprehensively secure applications without the need to augment their existing security program with additional tools or products.

Background

To speed up application development and deployment, organizations have been increasingly using containers and microservices architectures so that they can meet business needs with little delay. Enterprise Strategy Group research revealed that the vast majority of organizations (79%) use containers for their cloud-native applications today, and a similarly large majority (78%) expect to continue leveraging containers for at least the next 24 months, as shown in Figure 1.[1] Containers provide an excellent environment for running microservices, ensuring consistency, scalability, and portability across different platforms and deployment environments.

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. Organizations can no longer depend on a traditional web application firewall (WAF) for application security, especially when attacker techniques have evolved and multiplied. One attacker might end up requiring a multitude of WAF rules, which can lead to unwanted false positives, maintenance complexity, and management costs.

Figure 1. Containers Continue to Serve as a Key Cloud-native Support Component



Source: Enterprise Strategy Group, now part of Omdia

Cyberattacks and threats on today's application architectures are more sophisticated, utilizing 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. According to Enterprise Strategy Group research, 36% of respondents indicated that a top

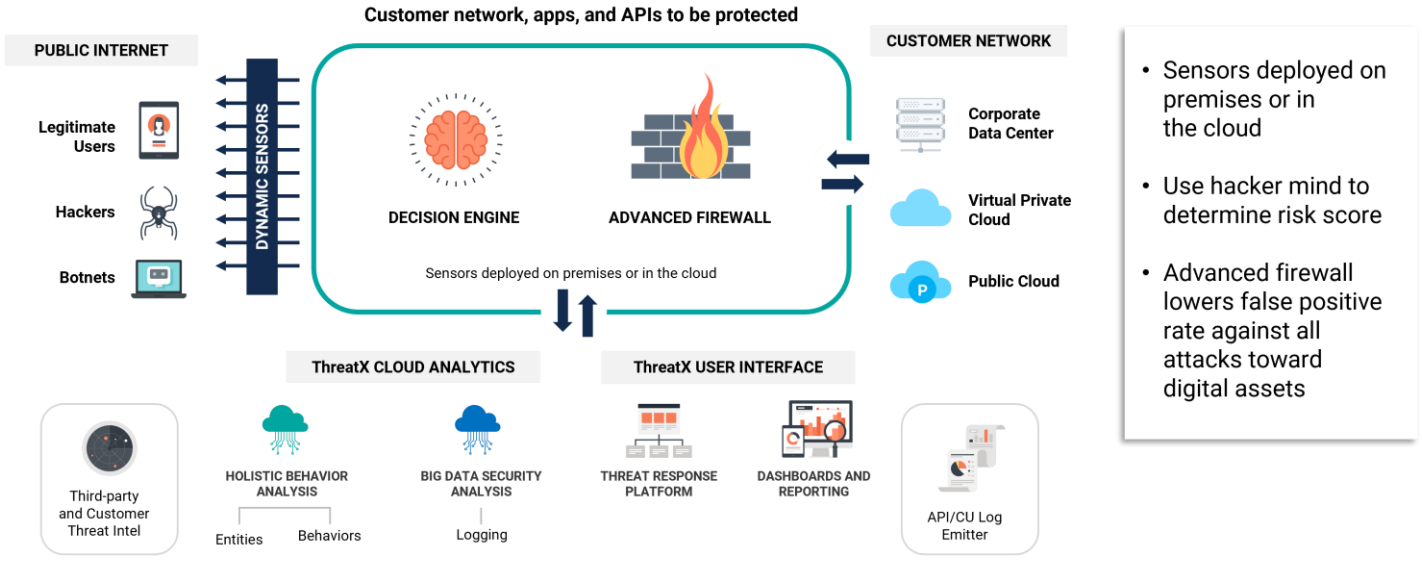
[1] Source: Enterprise Strategy Group Research Report, *Application Modernization and the Role of Platform Engineering*, October 2024. All Enterprise Strategy Group research references and charts in this technical validation have been taken from this research report.

challenge with applications based on a microservices architecture is applying security policy consistently, while 32% cited providing secure configurations as a top challenge. WAFs are ideally suited to protect a handful of applications but do not scale easily to handle an increasingly complex set of rules and, therefore, can become less effective as the number of first- and third-party applications grows.

ThreatX by A10 Networks Web App and API Protection Platform

The ThreatX platform, offered as a SaaS and/or on-premises solution, along with a security operations center (SOC) as a managed service, is designed to prevent, detect, and mitigate Layer 7 cyberattacks while minimizing false positives. Unlike WAFs, which protect only against known signatures and attacks, the ThreatX 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 meet the demands of applications and to protect any number of applications deployed on premises or in public and private clouds is simple with the ThreatX platform's Docker-based architecture (see **Error! Reference source not found.**).

Figure 2. ThreatX by A10 Networks



Source: A10 Networks and Enterprise Strategy Group, now part of Omdia

- **Context sensors:** Deployed at or near the origin application server, the context sensors scan all incoming traffic and requests generated by end users, hackers, or botnets to detect and log possible security events. The sensors employ a number of capabilities such as application and API profiling, an advanced parsing engine, and flow validation. When appropriate, the sensors will engage progressive interrogation techniques to identify and fingerprint "users." This interrogation helps delineate humans versus bots and compares and correlates across multiple inbound IPs.
- **Decision engine:** The decision engine leverages behavior-based analytics developed with embedded intelligence to evaluate inputs from multiple context sensors (over time) to determine behaviors that might represent malicious intent. Risk scores are calculated to determine the appropriate actions to be taken against specific attackers.
- **Cloud analytics:** This feature 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 suspicious behaviors are updated in the cloud platform and distributed to

the entire network of deployed sensors. This includes input from ThreatX SOC teams regularly updating for known common vulnerabilities and exposures, zero day, and threat intelligence gathered from scanning the dark web.

- **Advanced firewall:** Based on threat intelligence, behavioral signatures, and updated risk scores from the decision engine—and in conjunction with rules from the ThreatX SOC and customers—the system manages appropriate responses. These responses may include continued monitoring, blocking, interrogation, tarpitting, or blacklisting/whitelisting traffic before it enters the organization's network.
- **User interface dashboard:** This dashboard supports how application owners and 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, risk metrics, and related trends.
- **Proactive SOC support:** SOC support provides proactive notification of threats and attacks crowdsourced across multiple ThreatX customers and consultation on recommended remediations and best practices. The team also assists with numerous other activities, including rules management, policies, product configurations, Secure Sockets Layer certificate management, and more.

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.

Enterprise Strategy Group Technical Validation

Enterprise Strategy Group 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.

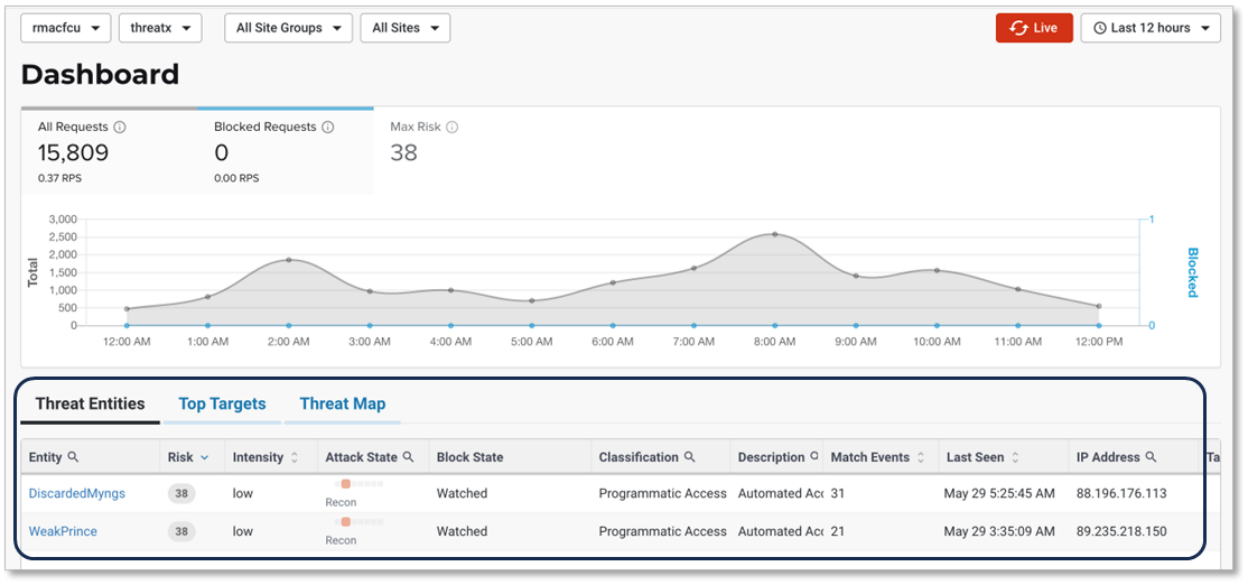
The ThreatX platform operates with a single-risk engine that correlates attack activity across a variety of tactics, techniques, and procedures (TTPs) so that individual attackers, or entities, are identified. All components of the ThreatX platform share and act upon the same data, enabling organizations 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.

Enterprise Strategy Group Analysis

We 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: the overall threat score, accounting for all entity activity, recorded every 15 minutes (displayed as a line chart); key metrics, specifically suspicious matches, suspicious entities, blocked entities, and blacklisted entities; and top attack entities by location with associated threat risk score (see Figure 3).

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

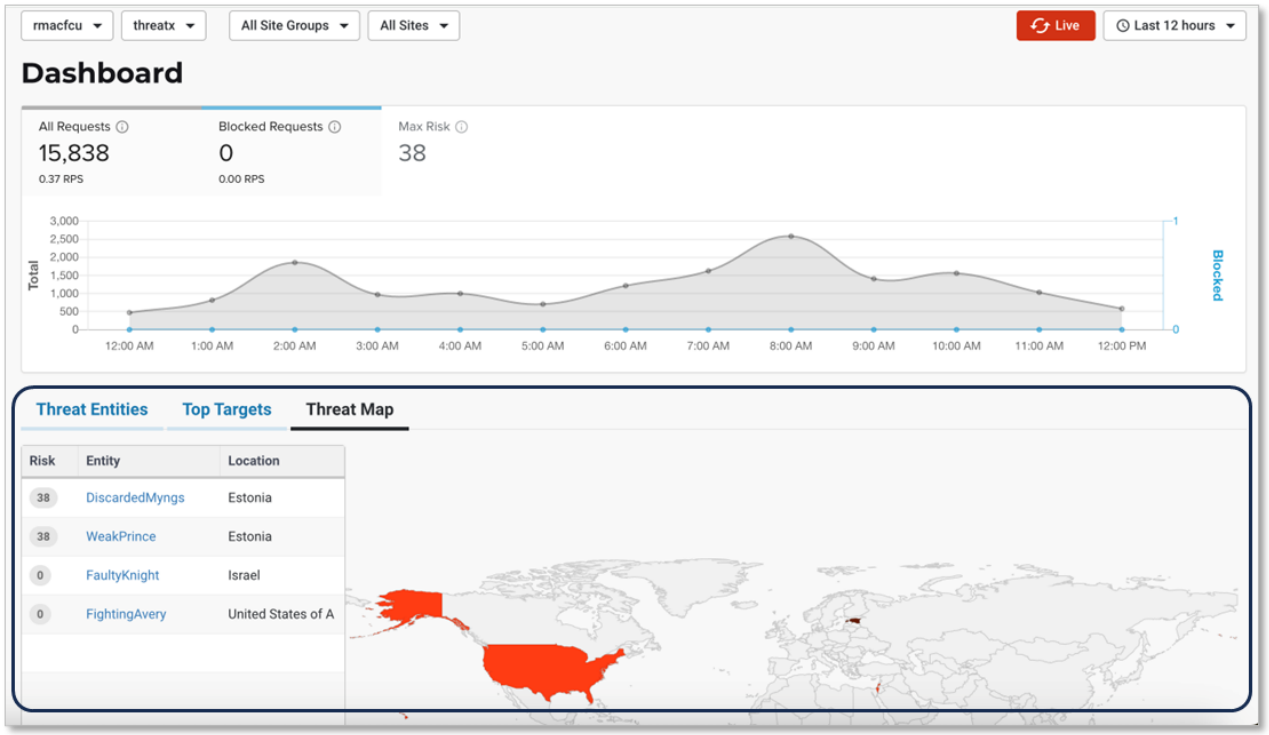
Figure 3. ThreatX Threat Entity View



Source: Enterprise Strategy Group, now part of Omdia

A global map denotes application traffic, color-coded to indicate overall security risk (see Figure 4).

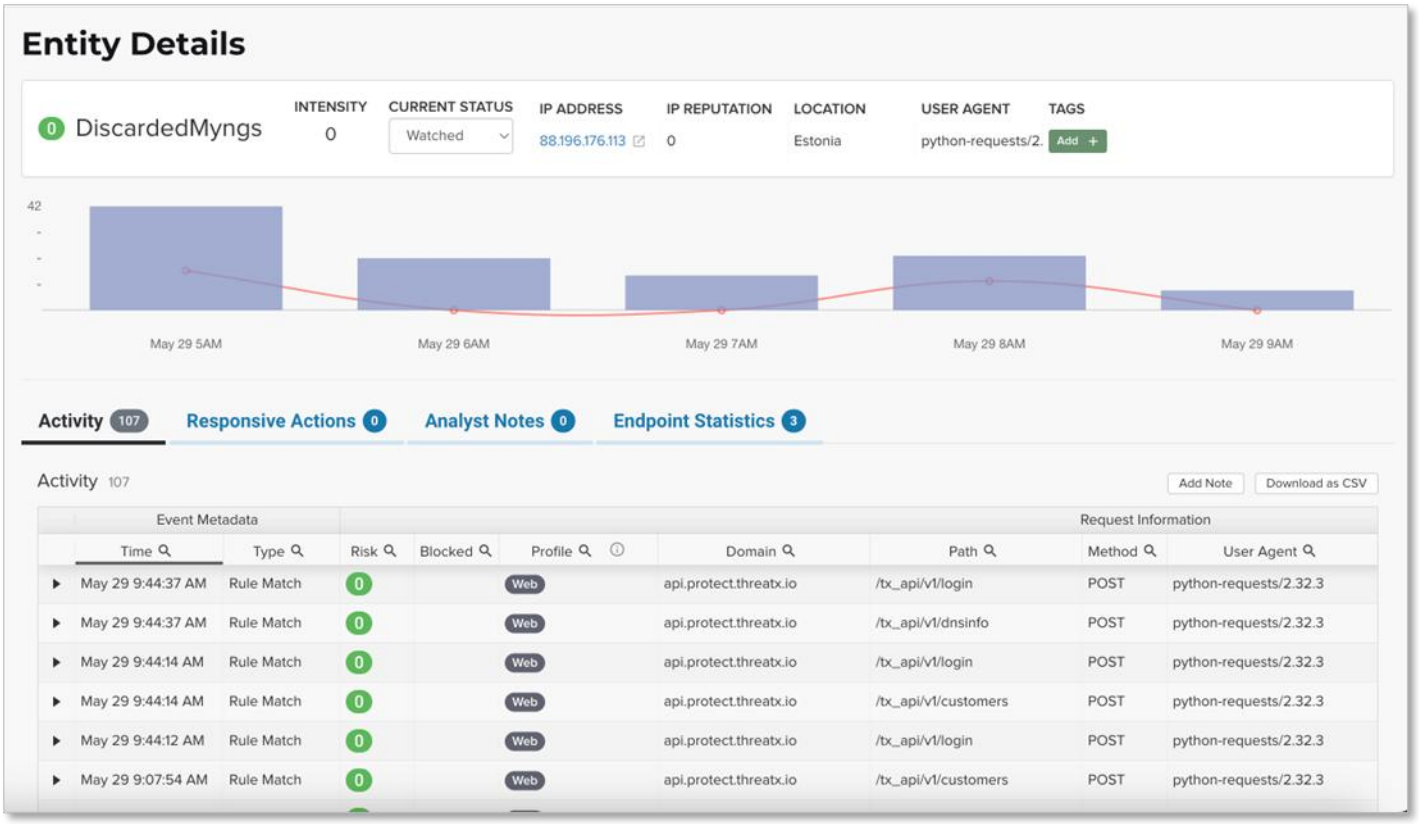
Figure 4. ThreatX Threat Map



Source: Enterprise Strategy Group, now part of Omdia

To show the extent of entity activity, we 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 5). If more than one domain was attacked, we could click into the entity's detail view and see all the affected domain names. We could also view attack parameters used by the identified number of entities, such as entering random usernames and passwords.

Figure 5. Examining the Extent of Attacks on Domains



Source: Enterprise Strategy Group, now part of Omdia

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 further, attempting to exploit exposed vulnerabilities. With this intelligence, administrators already know where to focus efforts to minimize security risk.

Why This Matters

According to Enterprise Strategy Group research, 39% of surveyed organizations cited enhancing application development security as a key driver to adopt platform engineering, a discipline focused on streamlining and securing the software development process. The prospect of using multiple cybersecurity controls to secure cloud-native applications can present a significant challenge, as this approach will increase both cost and complexity. While point solutions can address specific attack types well, integrating these tools enables organizations to assess the real-time state of application security with a unified set of data.

Enterprise Strategy Group 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 need 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.

Additionally, because all of this effort is assisted by ThreatX SOC team members, the barrier to entry is lessened and little administrative knowledge of the solution is required to make it immediately effective.

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.

Enterprise Strategy Group Analysis

We navigated back to the Threat Dashboard 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.*

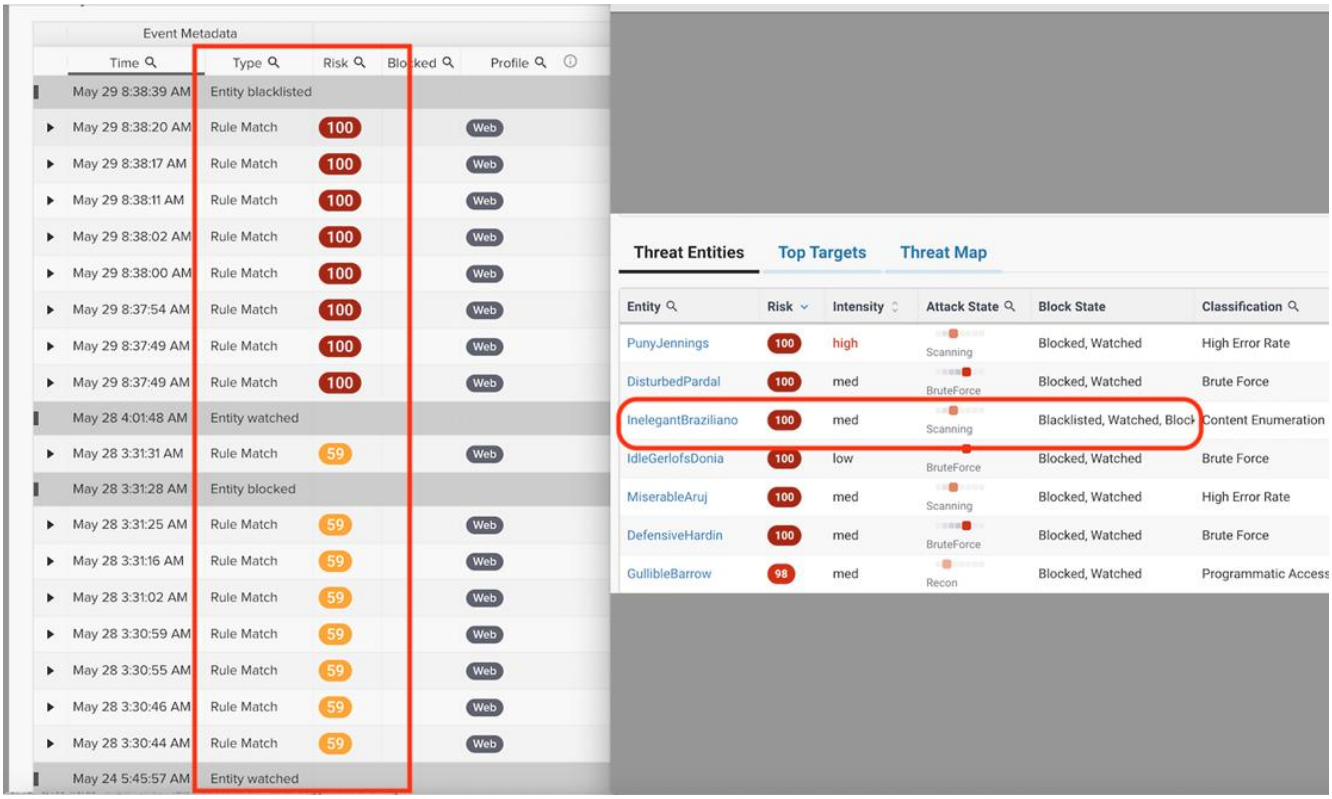
ThreatX names "entities" by combining an old-time pirate name with a modifier to help in remembering that named entity across multiple applications, multiple customers, and especially when attacks are coming from multiple IPs.

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

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.

We observed the three strikes rule in action by first clicking on the "TouchyWorley" entity in the Threat Entities list (see Figure 6). 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 6. Classifying Entities as "Blocked" or "Blacklisted"



Source: Enterprise Strategy Group, now part of Omdia

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.

Enterprise Strategy Group 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

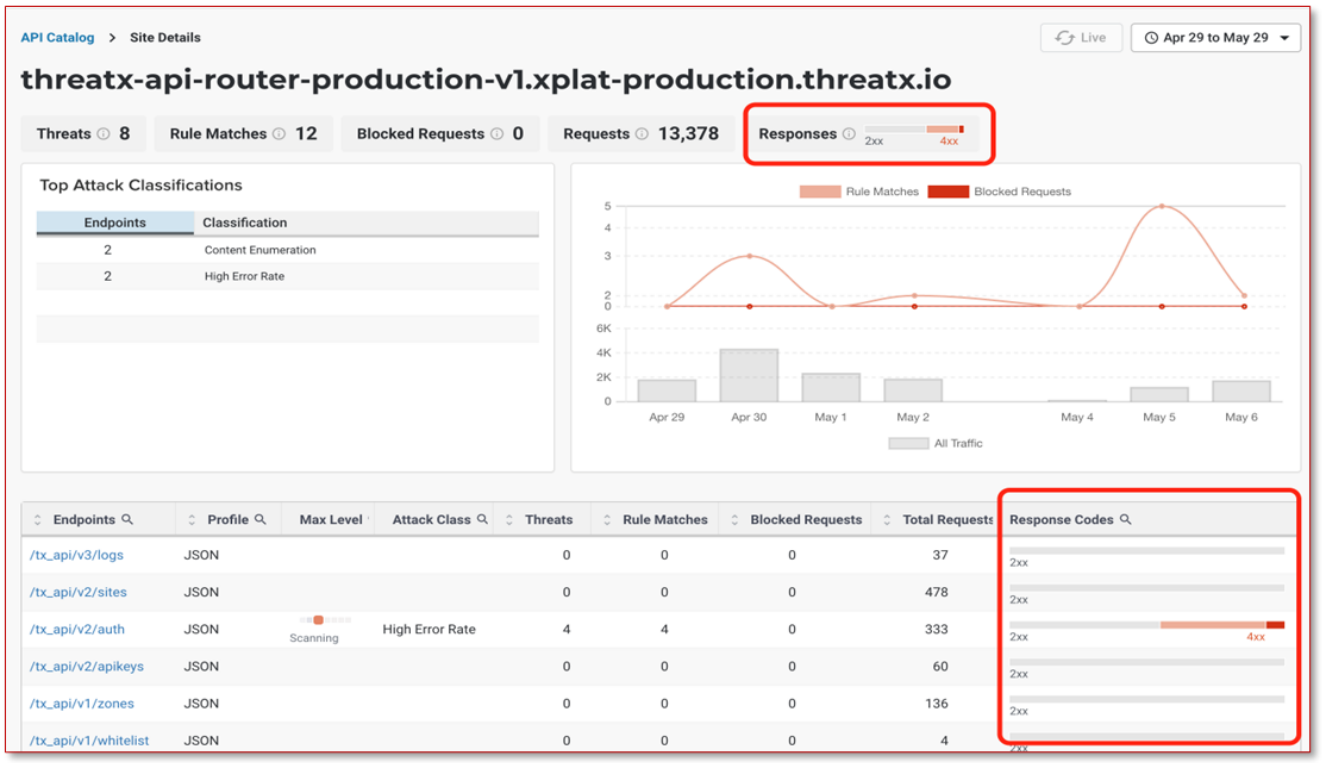
Organizations need actionable insight just as quickly as they need to identify attacking entities and their behavior to mitigate any damage to the business. With the ThreatX platform, organizations can immediately identify where issues lie and act accordingly with little delay.

Enterprise Strategy Group Analysis

One clear example that shows how ThreatX delivers actionable insight quickly is shown in Figure 7 in the **Top Threats** view. We saw that the platform had 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.

We also examined how the ThreatX API catalog could provide actionable insights. We navigated to the API Catalog in **Error! Reference source not found.** 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, ThreatX provided detailed insight so that we could direct our attention immediately to those APIs under possible attack.

Figure 7. Tallying Status Codes for Web-facing Application and Individual APIs



Source: Enterprise Strategy Group, now part of Omdia

Why This Matters

Identifying who and what has attacked an organization's 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 the business. Accomplishing this requires gaining actionable insight into malicious activity.

Enterprise Strategy Group 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.

Conclusion

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 Enterprise Strategy Group 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.

A10 Networks' ThreatX platform is designed to provide security for an organization's websites, 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.

Enterprise Strategy Group 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, Enterprise Strategy Group 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, Enterprise Strategy Group 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, Enterprise Strategy Group noted that organizations have improved insight so that they can perform the correct actions to prevent any further damage.

An important item of note is the fact that potential customers might 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, Enterprise Strategy Group believes that you should take a close look at the ThreatX platform by A10 Networks.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com