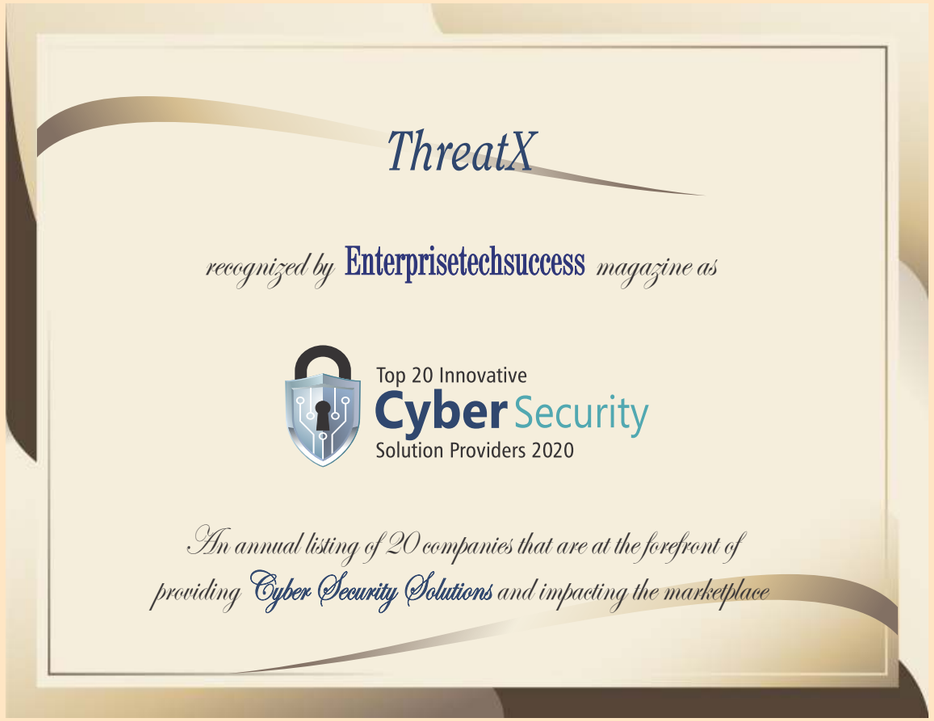
Enterprisetechsuccess
Platform Connecting Technology

Top 20 Innovative
Cyber Security
Solution Providers 2020

ThreatX

Powering Businesses with Unparalleled Expertise, An Innovative Culture and the Highest Standards of Efficiency



ThreatX: One Platform For All Your Application Security Woes

Gene Fay
CEO at ThreatX

www.threatx.com

Web application firewalls (WAFs) were enough for a world where security itself was not so challenging. Up until a few years ago, web application threats were less common and sophisticated, bots were easier to detect, and malware was still in its infancy.

All that has changed. The threat landscape has undergone a major transformation over the years, and security professionals are up against a much larger variety of complicated and challenging threats today. When compromised by cyberattackers, businesses face not only financial loss or regulatory penalties, but also damages to their reputation.

Traditional WAF products fall short on several fronts. They were built to protect data centers; they are not good with mobile application programming interfaces (APIs). They were meant to protect traditional architectures, not clouds. And, they are neither flexible nor scalable.

ThreatX, founded by Bret Settle and Andrew Useckas in 2014, is a web application and API protection + Bot management + distributed denial-of-service (DDoS) mitigation (WAAP++) platform for hybrid cloud environments.

"ThreatX was founded with the mission to create a web application security product that simply worked. Traditional WAF products are notoriously difficult to deploy and maintain, often never fully utilized to protect more than 10-15% of a company's applications, leaving many applications exposed and vulnerable," says Bret Settle, Chief Strategy Officer, ThreatX.

ThreatX Is Much More Than a Legacy WAF

ThreatX is built from the ground up to address shortcomings of traditional/legacy WAFs. It offers:

A unified solution

ThreatX delivers a WAAP++ multi-functional platform that combines web application security, API protection, Bot management, and DDoS mitigation into a single solution. ThreatX also brings together traditional signatures, behavioral analysis, active engagement, and deception to deliver a single automated answer.

"Most WAFs have taken a "Frankenstein" approach by bolting endless modules together. They may check the boxes, but they don't work together and actually make life harder for security staff," adds Bret.

API-native

ThreatX can help address API-centric attacks such as support for WebSockets, detection of host enumeration, and custom rules to identify expensive application calls. ThreatX's behavioral analysis automatically learns appropriate application behaviors and can alert on deviations.

"Many WAFs have begun adding API protection, but support is typically limited," says Andrew Useckas, Chief Technology Officer, ThreatX.

Cloud-native and ready for modern and emerging architectures

Traditional and legacy WAFs are architected for appliances and require a variety of independent modules that need to be enabled and configured. Even as they port to the cloud, the process is slow and complex, often taking weeks to deploy.

"Traditional WAFs run into many problems when they move to the cloud. Many WAFs are only cloud-accessible, while ThreatX is cloud-native and ready for modern and emerging architectures," says Gene Fay, CEO, ThreatX.

ThreatX is also container-native, allowing the solution to scale horizontally independent of cloud service providers.

"A multi-national liquor distributor was using a legacy application and was not able to deploy it across more than a small percentage of their web applications. ThreatX helped them to deploy ThreatX WAAP++ across hundreds of applications in weeks and go into blocking mode swiftly," adds Gene.

Two-way behavioral analysis

Unlike traditional WAFs that are architected for signatures and single behaviors (or signals), ThreatX uses behavioral analysis in two ways. One to profile normal application behavior to detect anomalies, and second by profiling attacker behaviors, techniques and infrastructure, and tracking attacks across all phases of an attack.

This protects organizations from targeted threats or attacks that do not match signatures or blacklists and evolve over multiple steps and phases of attack.

Continuous, risk-based security

Thanks to continuous analysis, ThreatX can not only catch threats that would be missed by traditional atomic detections but can also give insight into a wide range of behaviors on the protected site. The solution can also automatically unblock an IP as the risk level drops.

> *"ThreatX was founded with the mission to create a web application security product that simply worked. Traditional WAF products are notoriously difficult to deploy and maintain, often never fully utilized to protect more than 10-15% of a company's applications, leaving many applications exposed and vulnerable."*

Top 20 Innovative Cyber Security Solution Providers 2020
Enterprisetechsuccess Platform Connecting Technology
July, 2020

Low false positives and negatives

Security teams need to be able to understand what their security infrastructure is doing and why. This is especially crucial for incident response (IR) and hunt teams.

"WAFs have been plagued by false positives (good web traffic that gets blocked by the WAF) for years. Alternatively, many security tools have tried to avoid false positives by turning thresholds down so that only the most egregious threats are detected, leading to false negatives. ThreatX brings together signatures, application profiling, attacker profiling, active engagement, tracking across multiple phases of attack, and deception to deliver a unified, risk-based decision," says Brett.

This approach avoids false positives by not relying on any one technique exclusively and avoids false negatives by having multiple backup techniques to detect a threat.

"ThreatX arms security staff with a variety of insights, including details of suspicious behaviors associated with an attacker, historical trails of all events including pre and post blocked attack, and the aggregated and individual risks associated with those behaviors, thus giving a 360-degree view of the risks," adds Gene.

AppSec-as-a-service (ASaaS)

The ThreatX risk engine provides pre-correlated scores that can trigger automated responses (blocking, tarpitting, etc.) and security orchestration, automation and response (SOAR) workflows. Organizations can also outsource AppSec tasks to ThreatX as a service to gain additional access to talent or ongoing triage and response to alerts and events.

ThreatX also provides a second set of eyes on the customer environment to identify potential signs of problems that might otherwise be missed.

"Traditional WAFs require constant care and feeding at a time when AppSec talent is in scarce supply. The constant tuning and maintenance work still leave coverage gaps. ThreatX's automated self-tuning capabilities leverage advanced analytics to ensure efficacy and enable security teams to focus scarce time elsewhere."

At the Helm

Gene Fay, CEO

Gene has a long track record as an executive at technology companies, including COO at White Ops, General Manager at Resilient Systems (acquired by IBM), and VP of Worldwide Sales and Global Alliances of Network Intelligence (acquired by EMC and integrated into RSA). Gene

> *"ThreatX delivers a WAAP++ multi-functional platform that combines web application security + API protection + Bot management and DDoS mitigation into a single solution."*

> *"Thanks to continuous analysis, ThreatX can not only catch threats that would be missed by traditional atomic detections but can also give insight into a wide range of behaviors on the protected site."*

has extensive experience building high-impact teams at early-stage startups in storage, virtualization, and cybersecurity. He has specific expertise in go-to-market strategies, marketing, customer success, and channel development. Gene holds a BS and an MBA from Northeastern University, where he guest-lectures on topics such as product management, marketing, and sales.

Bret Settle, Chief Strategy Officer

Bret has served in multiple executive roles for Corporate Express/Staples and BMC Software and has extensive knowledge of the software development and security products industries. Bret has been responsible for enterprise security in multiple roles and has been an innovator throughout his career and has a proven track record of building and developing high performing organizations and

Andrew Useckas, Chief Technology Officer

Andrew has a varied career ranging from ethical hacking, penetration testing, and security product development for the US Department of Defense, senior consulting positions for fortune 500 enterprises, and corporate CISO responsibilities for large enterprises. Andrew has an exceptional blend of software development skills combined with extensive knowledge and experience of the network and security industries.

Conclusion

With more applications, changing architecture, increasing sophisticated threats, the job of a security professional will keep getting tougher every day. Adding to the difficulties is the need to work in lockstep with DevOps teams. There is a perfect storm of security challenges brewing. As legacy WAFs fall short in delivering solutions that help, ThreatX's cloud-native WAAP will help you detect, diagnose, prevent, and eliminate all those threats.

Headquarters/Location: Louisville, Colorado, USA

Website: www.threatx.com

Management: Gene Fay, CEO; Bret Settle, Chief Strategy Officer; Andrew Useckas, Chief Technology Officer