

CIOReview

ISSN 2644-237X

CIOREVIEW.COM

SEPTEMBER 18, 2020

The Navigator for Enterprise Solutions



Awarded by CIOReview

ThreatX



Awarded by CIOReview

The annual listing of 10 companies that are at the forefront of providing Enterprise Security solutions and transforming businesses

ThreatX

Delivering the X-Factor into Web Application Protection



Gene Fay

Over time, in human history, battlefields have expanded from land to sea to air. Today, with the snowballing of ubiquitous technologies, it has put forth another essential arena for conflicts – cyberspace. Cyberwarfare could turn any component of an IT network infrastructure into a compromised link on a virtual battlefield, and its repercussions would be felt in the real world. As organizations have substantial assets and value manifested in digital form, cybersecurity has thus become a top organizational concern. However, current cybersecurity strategies are intermittent and getting overwhelmed by new and sophisticated threats in today's evolving threat landscape. For instance, software applications have become one of the most targeted parts of the security perimeter, and the traditional web application firewall (WAF) solutions are failing to rise to the diversified and advanced threats.

These ever-evolving threats that the software applications face warrants a cutting-edge solution, and that's what ThreatX puts forth. ThreatX is an advanced web application and API protection (WAAP) solution created by some of the well-known experts in the white hacking and penetration testing arena. With the sea of competition in cybersecurity today, what keeps them ahead of their competitors is their comprehensive knowledge of the adversaries in the cyberthreat landscape. "Unlike our peers who approach WAAP from the perspective of testing, content delivery network (CDN), and other capabilities, we have built ThreatX from the ground up with an attacker-centric mentality," says Gene Fay, CEO of ThreatX.

A major reason behind taking such an approach is because of the current trends in the application development landscape. Software app development has become agile today. Companies release applications and updates on a daily or even hourly basis, but the integration of cybersecurity best practices haven't kept up with this agile schedule. Traditional WAF solutions often meet with limitations while encountering security breaches such as the low coverage on hybrid cloud environments, because



ThreatX's behavior-based solution delivers complete protection and deep threat visibility by combining behavior profiling, collective threat intelligence, and advanced analytics

of low accuracy and low intelligence. ThreatX, however, goes above and beyond the current standards of web application protection and offers its clients an in-depth analysis of trends and web application vulnerabilities. Its behavior-based solution delivers complete protection and deep threat visibility by combining behavior profiling, collective threat intelligence, and advanced analytics.

ThreatX, moreover, doesn't require organizations to slow down their application development process. The company's 'WAAP + bot management + DDoS solution' can be deployed across applications remarkably fast, and this agility helps in securing the weak links that would otherwise be exposed and attacked. Moving beyond static signatures, ThreatX also provides a detailed analysis of the threat landscape of an organization, thereby reducing false positives, minimizing operational costs, and improving agility with the evolving threats. ThreatX, thus, offers an all-in-one platform that can be deployed in hours, not days or weeks.

Notably, ThreatX's behavior-based approach to threat determination is a very compelling choice in today's market of application protection. ThreatX continuously learns from what it observes. It then uses that knowledge to automatically identify and block potentially malicious and suspicious behavior without applying conditions or rules, which is necessary with legacy and traditional WAFs. This approach helps organizations differentiate between real threats that need heightened attention and those that could be monitored for additional suspicious behavior.

Another 'X-Factor' that ThreatX delivers is its multi-tenant capability. A company that manages numerous web applications can view and monitor all of them all through a single dashboard. This consolidated view of all web applications provides ThreatX customers with greater visibility into the entire attack kill chain, allowing them to see what's going on when. These attributes have earned ThreatX an epithet among its customer base as "the best-kept secret in cybersecurity," remarks Fay.

ThreatX's remarkable agility has enabled them to overcome even the toughest challenges for its clients. For instance, a major liquor distributor found it challenging to deploy security measures for more than 10 or 15 percent of its web applications and APIs using a competitive WAAP solution. ThreatX was able to deploy its platform to protect more than 400 of the client's applications in three weeks. "It took three weeks because we could only move as fast as the client was able," said Fay. "We have another example of a major manufacturer, where we deployed across 1000 applications in 72 hours and brought them into full blocking mode."

ThreatX has an international customer base and is looking forward to tripling that in the next 12 to 18 months. "A lot of CIOs and CEOs that I talk to have said that they will only deploy a WAF if the solution can help them consolidate their application protection," concluded Fay. "ThreatX's WAAP++ platform allows them to do precisely that, and we are quite excited about our future." 