THREATX

DATA SHEET

Cyber Insurance Critical Controls

How ThreatX Can Help

ThreatX's API and Web Application Protection platform addresses some of the common critical controls cyber insurers evaluate when determining what policy they will extend to their clients.

Insurers, like security practitioners, know that threat actors search for and pursue targets with the lowest barriers to entry, which requires a greater emphasis on comprehensive cyber risk management. They also know that web applications continue to be the number one source of data breaches, according to the *Verizon Data Breach Investigations Report*. In addition, Gartner predicts that by 2022, APIs will be the preferred attack vector and the new number one source of data breaches.

Underwriters typically look at a myriad of key controls.

ThreatX helps customers address the five controls highlighted in red »

The 10 most common controls our customers have shared with us based on inquiries from their insurers:

1 **Managed Vulnerabilities** TX
2 **Patched Systems & Applications** TX
3 Protected Privileged Accounts
4 Prepared & Tested Incident Response Plans
5 **Protected Network** TX
6 MFA Controlled Access
7 Hardened Device Configuration
8 **Secured Endpoints** TX
9 Phishing-Aware Workforce
10 **Logged & Monitored Network** TX

Managed Vulnerabilities and Patched Systems & Applications

By conducting routine vulnerability scans and yearly pen testing exercises to simulate cyberattacks, organizations can uncover and remediate existing vulnerabilities on their network before threat actors have a chance to exploit them.

With hundreds of vulnerabilities revealed every month for multiple applications, APIs, and systems, it should be no surprise that unpatched vulnerabilities are consistently a leading cause of intrusions into systems, with

web applications being the current number one attack vector and source of data breaches, and APIs expected to be the number one source shortly. When systems are not patched in a timely manner, attackers will inevitably seek to exploit these vulnerabilities.

ThreatX's 24/7 Managed SOC continuously monitors for new and existing vulnerabilities that can affect customer applications. When new, relevant CVEs are published, ThreatX notifies customers and provides short- and long-term patching recommendations, including patching of applications and web services. ThreatX also provides virtual patching of zero-day vulnerabilities — as was the case when the Log4j2 vulnerability was publicized — to ensure assets stay protected until a permanent patch can be delivered.

Protected Network

Most organizations that have been breached use web application firewalls (WAFs) to protect their networks. Legacy WAF technology is often outdated, underutilized, not properly configured, and extremely difficult to scale.

WAF Shortcomings

Legacy WAFs are underutilized because they are difficult to deploy, configure, tune, and maintain while significantly constraining resources from even the most well-staffed cybersecurity teams. Once deployed, these tools flood teams with false positives while consistently failing to effectively identify and block malicious actors because of their outdated, signature-based approach. Therefore, "organizations that do have a WAF typically only deploy in front of the top 15% of their applications and even then, 80% are inevitably compromised in some capacity," according to the *Verizon 2020 Data Breach Investigations Report*.

Finally, modern attackers understand how to avoid the tripwires and detection thresholds that are native to signature- and rule-based solutions and inherent in every legacy WAF – an outdated approach to a modern problem. Attackers do this by blending multiple techniques throughout various phases and time scales during their campaign. Legacy WAFs depend on attackers being common and loud and were built to block isolated attacks, so naturally they struggle with detecting and stopping modern attacks, which are constantly evolving their patterns.

ThreatX Network Protection

ThreatX was built for the modern enterprise and to combat modern threats. Deploying and scaling the platform is incredibly straightforward. ThreatX is a docker-based container deployment with a simple DNS redirect, making getting up and running quick, easy, and scalable. Customers can deploy in any cloud, on-prem, in ThreatX's cloud, or any combination of the three. On average, customers can deploy within 30 minutes and get into full blocking mode within 24 hours.

Next, ThreatX takes an attacker-centric approach by applying a behavioral-based detection methodology. Rather than only depending on static rules or looking at individual signatures and making a binary block decision, ThreatX will look at each unique entity interacting with the API or application, monitor its behavior, create a profile based on its activity, then monitor the entity and inevitably block the actor if it surpasses a specific risk score.

continued »

Lastly, ThreatX takes a true platform approach to Layer 7 by providing WAF, API, Layer 7 DDoS, and bot protection via a single risk engine. This approach provides an integrated view for full visibility into each threat entity, regardless of the attacker's combination of techniques or time scale. ThreatX automatically correlates this data and applies automated prevention to the customer's environment, resulting in full-spectrum protection, unrivaled blocking efficacy, fewer false positives, and little to no tuning.

Secured Endpoints

Cyber insurers place heavy emphasis on having advanced anti-malware solutions on servers, mobile devices, and individual workstations to identify malicious programs and contain their spread. Indeed, solutions that enable organizations to identify attacks on their endpoints and mitigate data leakage are critical to a sound risk management program.

! Today, more and more insurers are beginning to address API endpoints, which are running rampant in today's enterprise due to the proliferation and speed at which new applications and microservices are being developed.

Thus, it is critical for organizations to catalog, monitor, detect, and respond to attacks on these assets just as they would on workstations, servers, and mobile devices.

ThreatX's API Threat Assessment capability analyzes and profiles legitimate, suspicious, and malicious API use to discover and enumerate the API endpoints deployed in the service of ThreatX-protected applications. While monitoring API interactions in real-time, ThreatX accurately detects real API endpoints and catalogs active tech stacks and markup encodings. Security administrators and operators will see a new layer of detail – the API endpoints that are actually deployed and exposed in support of their applications. The risk that those endpoints are subjected to is expressed in actionable terms, precisely where the attacker is aiming.

Logged & Monitored Network

Logging and monitoring network activities empower organizations to understand whether something nefarious may be happening and to ensure an attacker's actions are identified and blocked early in the kill chain. Doing this at scale and in a timely manner requires visibility, automation, and operator expertise, which many vendors and cybersecurity teams lack – simply due to labor shortages.

ThreatX Risk Monitoring

As previously referenced, ThreatX monitors all Layer 7 web application and API activity deployed behind ThreatX using advanced attacker behavior profiling and active engagement capabilities to combat even the most sophisticated attackers. ThreatX actively models the risk of API and

application users via many techniques, including machine learning, cluster analysis, fuzzy logic, heuristics, threat intelligence, and behavioral rules. API and application users are given a risk score between 1 and 100 based on their accumulated activity, intensity, and fingerprint. The risk model looks for tell-tale escalation up the kill chain, and the entity's activity is stored as evidence for future actions. The entity's activity is correlated across multiple customer sites and even different ThreatX customers, providing a real-time feedback loop that inoculates all ThreatX customers when a risky entity is identified.

This risk monitoring approach provides the lowest false-positive and false-negative rates in the industry, while automatically correlating activity to discern malicious actors and applying automated blocking, preventing them from breaching or harming the enterprise. Most insurers will contend that automated technology (such as our correlation, risk scoring, and blocking techniques) combined with operators monitoring the network events and anomalous behavior is essential. ThreatX agrees – equally as crucial to the actual tech are the people behind it.

ThreatX SOC

ThreatX is delivered via a 24/7 SOC, which is staffed with subject-matter Layer 7 experts. Working as an extension of your organization, ThreatX will handle the day-to-day administration of the ThreatX platform while fine-tuning the solution to meet the specific needs and unique threats of customer environments. ThreatX will proactively work to deter, disrupt, and deny malicious attackers to significantly reduce the chance of compromise or system downtime. ThreatX's application experts will also provide security and ops monitoring, IR, threat hunting, vulnerability monitoring and virtual patching, as well as custom countermeasure development.

When organizations partner with ThreatX, not only are they leveraging a best-of-breed technology, but they also receive the benefit of adding world-class application security expertise to their organization via ThreatX's managed service. This lets organizations offload work to ThreatX's highly skilled security experts for around-the-clock proactive monitoring as well as streamlined threat response support. Partnering with ThreatX empowers security teams to focus on high-priority projects while providing a better ROI, reducing risk, and driving operational efficiencies.

Conclusion

Ultimately, it's important to note that "compliance is not security." Just because your organization receives a favorable cyber insurance policy does not mean your company is secure. That said, companies that partner with ThreatX put themselves in a favorable position to strongly address some of the key controls insurers consider when rendering a policy. More importantly, ThreatX can help mitigate the probability of having to draw on that policy after falling victim to a breach on web applications and APIs, while providing continuous monitoring and curbing labor shortages.