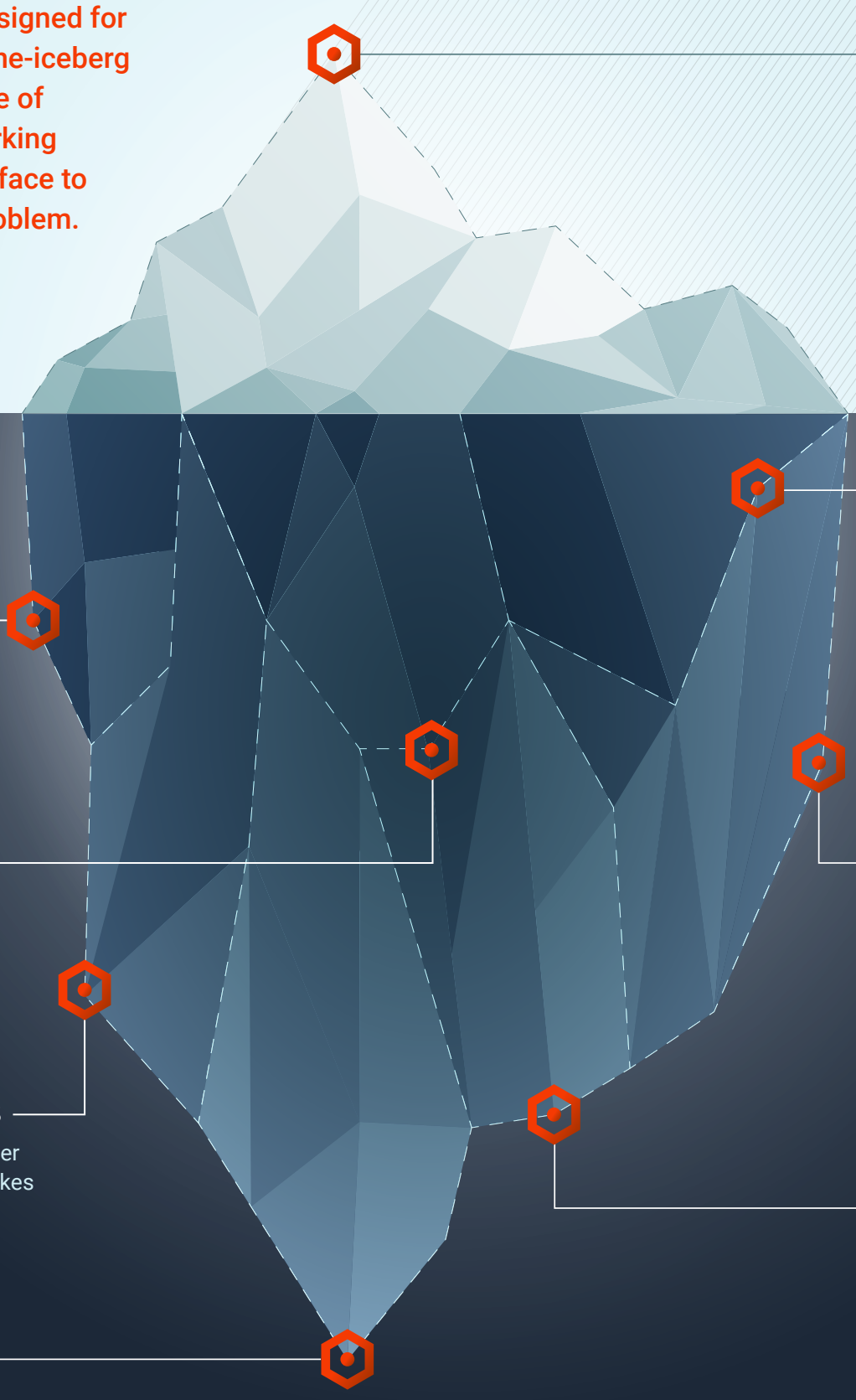
THREATX

The Modern Threat Landscape

Your legacy WAF was designed for the easy-to-spot, tip-of-the-iceberg attacks, not the multitude of less-obvious attacks working together beneath the surface to create a Titanic-sized problem.



OWASP Signature-Based Attacks

Attacks based on the OWASP Top 10 that have detectable signatures.

ATTACKS WORKING TOGETHER BELOW THE SURFACE

Misconfiguration

Taking advantage of a misconfiguration in the way that a system is set up, or looking for a way to misconfigure a system.

Credential Stuffing

Exploiting user credentials that were stolen in a previous breach.

Account Takeover (ATO)

Includes attacks like credential stuffing, brute force, or password spraying.

Feature Abuse

Conducting massive queries to the database in an attempt to slow down performance and/or interrupt availability.

Evasion Techniques

Employing tactics like varying user agents or spoofing TLS handshakes to disguise or redirect attention from attacks.

Layer 7 Denial of Service

Disrupting an application by driving massive amounts of traffic to a target application.

Malicious Bots

Weaponizing many of the other attack types listed here by using bots.

ABOUT THREATX: ThreatX's web application and API protection (WAAP) platform makes the world safer by protecting web applications and APIs from all threats, including DDoS attempts, BOT attacks, API abuse, exploitations of known vulnerabilities, and zero-day attacks. Its multi-layered detection capabilities accurately identify malicious actors and dynamically initiate appropriate action. ThreatX effectively and efficiently protects web applications and APIs for companies in every industry across the globe. For more information, visit: www.threatx.com

Learn more about the hidden iceberg that is the modern threat landscape in *What Lies Beneath: What You Need to Know About the Modern Threat Landscape*.

LEARN MORE →