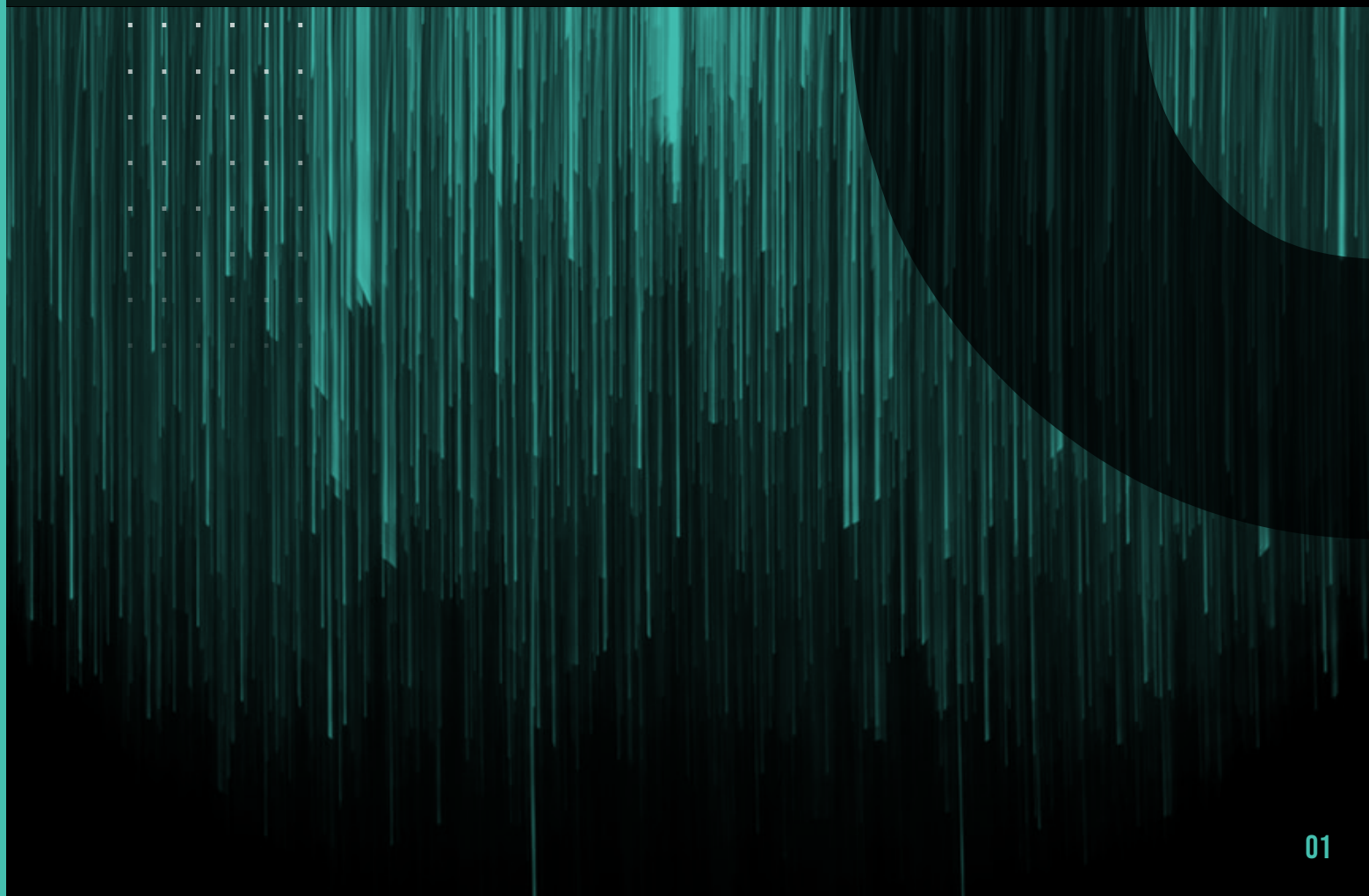
CONTRAST SECURITY

PERIMETER SECURITY NOISE LEAVES APPLICATIONS VULNERABLE TO ATTACKS

WHITE PAPER

EXECUTIVE OVERVIEW

When it comes to protecting running applications, traditional perimeter security solutions lack sufficient visibility to differentiate which attacks can impact an application. These kinds of defenses sit in front of applications, without the necessary context to determine if a potential threat should be blocked. As they must "guess" as to the validity of a threat, this results in a high degree of inaccuracy.[1] In addition to leaving applications vulnerable to unknown and zero-day attacks, these outdated approaches create more work for security teams due to the fact that they generate large numbers of false positives and cannot scale to meet expanded traffic and new applications, all while slowing deployment cycles each time software is updated.



PERIMETER DEFENSES AREN'T NEARLY ENOUGH FOR APPLICATION PROTECTION

"The reality of application attacks accounting for the majority of breaches necessitates better protection for production applications. Over the last couple of decades, network protection has moved closer and closer to the application—from the firewall to the intrusion prevention system to the web application firewall (WAF)."[2] This evolution has happened because the better organizations understand applications, the more accurately they can detect and block attacks. But as organizations are exposed to new sophisticated threats, many traditional perimeter defenses (especially WAFs) are inherently too slow to keep up with all the attacks targeting today's applications.[3]

While Layer 7 traffic analyzers can see traffic, they lack the application context to understand what that traffic means and how the data will be used. Unlike simple parameter-based applications of the 1990s and early 2000s, modern applications use JSON objects or network-optimized binary exchanges that cannot be understood due to the lack of context—namely, knowing if and how the application will use the data. Defenses that rely on a single network transport inspection cannot evaluate the way that data is parsed, decoded, and pieced together with other parts of the application.

The lack of insight from network-based technologies results in false positives, false negatives, and excessive tuning that is slow to keep up with all attacks targeting today's applications.

Many organizations today depend on WAFs as their main (if not only) source for application protection. WAFs typically perform two kinds of threat detection:

- **Blacklisting** uses signature-based detection and blocking of known threats and cannot identify threat variants or zero-day attacks. While a perimeter defense is useful for screening out many basic attacks, blacklisting cannot keep up with new attack variations, so attackers continuously find ways to bypass them.[4]

- **Whitelisting** observes and makes a model of acceptable application behaviors. It records legitimate behaviors over time and prevents requests that don't match the model behavior. Whitelisting is specific to the application being monitored, which makes it feasible to enumerate good functions—instead of trying to catalog every possible malicious request. Unfortunately, perimeter defenses like WAFs often lack enough time to complete the behavior modeling process before the next version of the application is deployed.

A STUDY THAT ANALYZED ALL THE VULNERABILITY DISCLOSURES BETWEEN 2010 AND 2019 FOUND THAT AROUND 55% OF ALL THE SECURITY BUGS THAT HAVE BEEN WEAPONIZED AND EXPLOITED IN THE WILD WERE FOR TWO MAJOR APPLICATION FRAMEWORKS—WORDPRESS AND APACHE STRUTS.[5]

While WAFs and perimeter defenses do offer some positive security benefits, they also have a number of shortcomings. Developers and IT staff often struggle with the fact that WAFs are not fully application programming interface (API)-enabled and that they require complex manual setup. At the same time, security teams require full-time staff just to manage constant WAF rules. And the lack of API support for technology such as REST and gRPC becomes a roadblock when organizations try to deploy into Infrastructure-as-a-Service (IaaS) public clouds.

More specifically, when it comes to effective runtime application security (AppSec) in the digital transformation era, the strategy of relying on perimeter defenses alone leaves organizations at higher risk of application-based attacks due to solution limiters such as:

- Limited (perimeter) visibility and protection
- Poor accuracy (a lot of false positives)
- Slow to deploy
- Costly to maintain
- Difficult to scale
- Evolving compliance requirements

ONE OUT OF FOUR DATA BREACHES LAST YEAR WERE THE RESULT OF ATTACKS THAT EXPLOITED WEB APPLICATION VULNERABILITIES.[6]

LIMITED VISIBILITY AND PROTECTION

When threat detection is done at the perimeter, those signature detections have no visibility into whether the application is actually vulnerable. “WAFs operate in front of the application and therefore lack the context needed to determine if a given input should be blocked. This need to approximate or guess the result of a given input results in a high degree of inaccuracy. This inaccuracy may lead to a given attack being successful.”[7]

Attackers often scan for various attack vectors across the internet rather than targeting applications directly with customized attacks. Unable to see inside their own perimeter, network-based defenses do not know if and how applications will respond to an ever-growing list of attacks on an ever-growing list of web APIs. This lack of application-centric context means that application defenses have no idea which part of the code, library, or function may be under attack.

Because of the inherent limitations of protection on the application perimeter (i.e., WAFs), organizations need to prioritize blocking runtime threats inside the actual application itself to detect and block variant and zero-day threats. If the runtime is left unprotected, there is an elevated attack risk to applications that can result in disruption of normal operations or a critical data breach.

HALF OF MALWARE ARE CAPABLE OF BYPASSING TRADITIONAL SIGNATURE-BASED DEFENSES.[8]

POOR ACCURACY

Perimeter defenses rely on signature-based protection such as blacklists and heuristics to anticipate potential known threats. This approach leads to missed threats (false negatives) that then target application code, APIs, and/or libraries—well beyond the reach or capabilities of a perimeter security solution.

Simultaneously, perimeter defenses also generate an overwhelming number of false-positive alerts—probes that don't represent an actual threat to a running application. Sorting the actual threats from the noise requires human attention—which increases the time spent by security teams on manual processes. Security analysts must research, verify, and ultimately dismiss these potential threats.

Increasing headcount to handle this workload isn't a practical option, since a majority of companies are already straining to fill skilled security positions. Over half of cybersecurity professionals indicate their organization is at moderate or extreme risk due to staff shortages, and AppSec is an area where the gaps are the most glaring.[9] With the status quo of perimeter defenses, these hard-to-find professionals spend too much time correcting the tool instead of having the applications report accurate information from the inside about what matters and when.

The demand on security increases further because security teams need to provide additional clarity for DevOps to interpret findings and additional orchestration to make it actionable. Nearly three-quarters of DevOps teams report being inadequately prepared to deal with the security requirements of AppSec.[10] Unfortunately, because signature-based perimeter solutions are unable to differentiate real attacks (exploits) from attempted attacks (probes), security teams often end up turning off perimeter defense blocking due to alert fatigue, which significantly increases application risk.

A MAJORITY (62%) OF ORGANIZATIONS REPORT THAT THEIR CYBERSECURITY TEAM IS UNDERSTAFFED—AND 70% SAY FEWER THAN HALF OF CYBERSECURITY APPLICANTS ARE WELL-QUALIFIED FOR THE JOB.[11]

SLOW TO DEPLOY

Perimeter-based AppSec solutions require coordination with network teams to ensure they see the right traffic. Security teams must also communicate and schedule with development teams to configure tools. In the case of perimeter-based AppSec, security teams must also manually set up static rules manually and then constantly redefine and tune them over time. These limitations add to the burden on human staff while slowing down secure application deployment and management processes. Ultimately, these demanding team coordinations produce unnecessary high setup costs to deploy, configure, and maintain a perimeter AppSec defense.

HARD TO SCALE

Traditional defenses also present issues when it comes to scalability. WAFs need to be expertly tuned with each new code deployment for effective monitoring and protection. This is especially impractical for DevOps environments that depend on continuous integration/continuous deployment (CI/CD) and elastic cloud workloads.

Many traditional perimeter defenses also require redeployment when applications move or change infrastructure. As a result, development flows are interrupted for manual patch management and redeployment. Tuning disrupts applications and slows growth speed. Patching and redeployment processes are typically complex and also expensive due to staff overhead expenses (e.g., development, operations, project management). Changes may impact security, but no new application value is created, and there's no business growth—only maintenance being done.

Containerized applications often scale to meet demand: As application usage increases, more nodes are spun up. However, as application usage decreases, those nodes spin down. When security is inside the application, the security capabilities automatically scale up and down as part of this demand. Embedded security does not require additional configuration or separate scaling procedure.

The lack of elastic scalability and subsequent dependence on manual workflows ultimately leads to a high volume of false positives from perimeter defenses (WAF) at scale. And this inability to scale effectively restarts the cycle of manual maintenance—which distracts security teams from attending to actual vulnerabilities.

RESEARCH REVEALS THAT MORE THAN ONE-QUARTER OF ALERTS ARE FALSE POSITIVES. SECURITY TEAMS SPEND AN INORDINATE AMOUNT OF TIME CHASING ALERTS THAT TURN OUT TO BE FALSE POSITIVES.[12]

COMPLIANCE

Industry standards and regulatory legislation are becoming increasingly strict and specific in their requirements for protecting private data. At the same time, the average number of exposures present in an application today is the same as it was two decades ago—26.7 serious vulnerabilities.[13] Current standards such as National Institute of Standards and Technology (NIST) and Payment Card Industry (PCI) now have specific requirements for advanced AppSec capabilities that must be addressed by developers.[14]

At the same time, the added damage of a breach that also violates security compliance with strict regulations such as the European Union's General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA) in the United States can come with stiff punitive penalties in addition to other financial losses.

THE COMBINED COSTS OF EQUIFAX'S DISASTROUS DATA BREACH—CAUSED BY A FAILURE TO PATCH A KNOWN WEB APPLICATION SECURITY FLAW—TOTALED OVER $1.38 BILLION.[15]

APPLICATION SECURITY NEEDS TO GO BEYOND THE PERIMETER

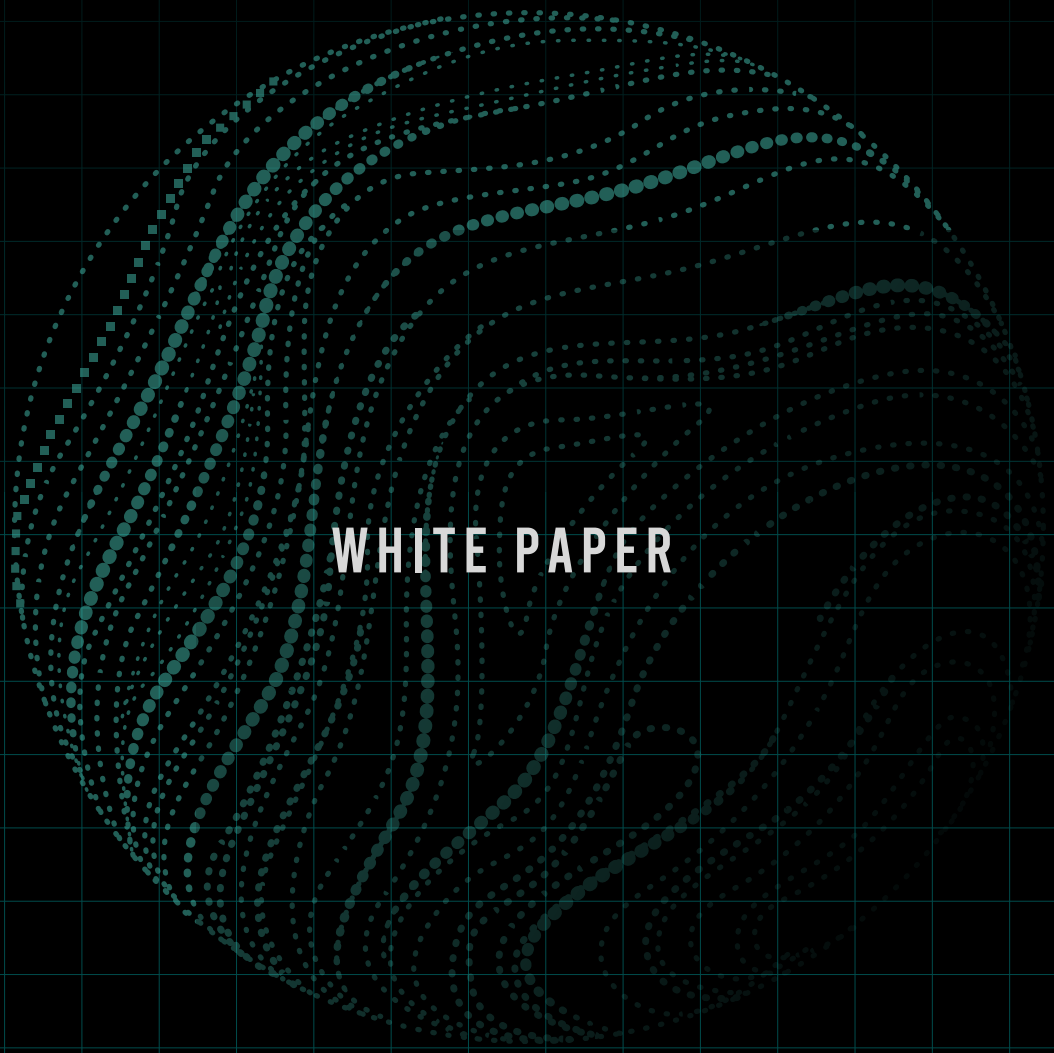
Traditional methods of applying only signature-based AppSec solutions at the perimeter leave code susceptible to risk where it matters most—on the inside, during runtime operations. Without visibility on the inside of how an application works, security leaders cannot scale their teams to effectively meet the demand of application teams and their increasing release cycles.

Security leaders currently lack the ability to effectively protect running applications. They need new AppSec tools to complement or replace outdated or insufficient solutions.

To address increasing exposure and sophisticated threats that target runtime applications, security teams need AppSec protection that can compensate with the necessary visibility, accuracy, scalability, and ease of deployment to keep pace with modern application vulnerabilities without generating false positives and false negatives.

---

1 Alexander J. Fry, "Runtime Application Self-Protection (RASP), Investigation of the Effectiveness of a RASP Solution in Protecting Known Vulnerable Target Applications," SANS Pen Testing, April 15, 2019.
2 Ibid.
3 "Understanding and Selecting Runtime Application Self-Protection," Securosis, October 21, 2019.
4 Tuomo Makkonen, "Cloud WAF Comparison Using Real-World Attacks," Medium, March 6, 2020.
5 Catalin Cimpanu, "WordPress and Apache Struts account for 55% of all weaponized vulnerabilities," ZDNet, March 17, 2020.
6 "2019 Data Breach Investigations Report," Verizon, April 2019.
7 Alexander J. Fry, "Runtime Application Self-Protection (RASP), Investigation of the Effectiveness of a RASP Solution in Protecting Known Vulnerable Target Applications," SANS Pen Testing, April 15, 2019.
8 "As malware and network attacks increase in 2019, zero day malware accounts for 50% of detections," Help Net Security, December 13, 2019.
9 "Strategies for Building and Growing Strong Cybersecurity Teams," $(ISC)^2$ Cybersecurity Workforce Study 2019, accessed February 10, 2020.
10 Tim Freestone, "AppSec Instrumentation Addresses AppSec Skills Shortage," Security Boulevard, March 9, 2020.
11 Ibid.
12 Michael Hill, "Over a Quarter of Security Alerts Are False Positives," Infosecurity Magazine, March 17, 2020.
13 "Malware and ransomware attack volume down due to more targeted attacks," Help Net Security, February 5, 2020.
14 "Security and Privacy Controls for Information Systems and Organizations," NIST, March 2020.
15 Jai Vijayan, "2017 Data Breach Will Cost Equifax at Least $1.38 Billion," Dark Reading, January 15, 2020.



WHITE PAPER

CONTRAST SECURITY

240 3rd Street
Los Altos, CA 94022
888.371.1333

Contrast Security is the world's leading provider of security technology that enables software applications to protect themselves against cyberattacks, heralding the new era of self-protecting software. Contrast's patented deep security instrumentation is the breakthrough technology that enables highly accurate assessment and always-on protection of an entire application portfolio, without disruptive scanning or expensive security experts. Only Contrast has sensors that work actively inside applications to uncover vulnerabilities, prevent data breaches, and secure the entire enterprise from development, to operations, to production.