CONTRAST SECURITY

EBOOK

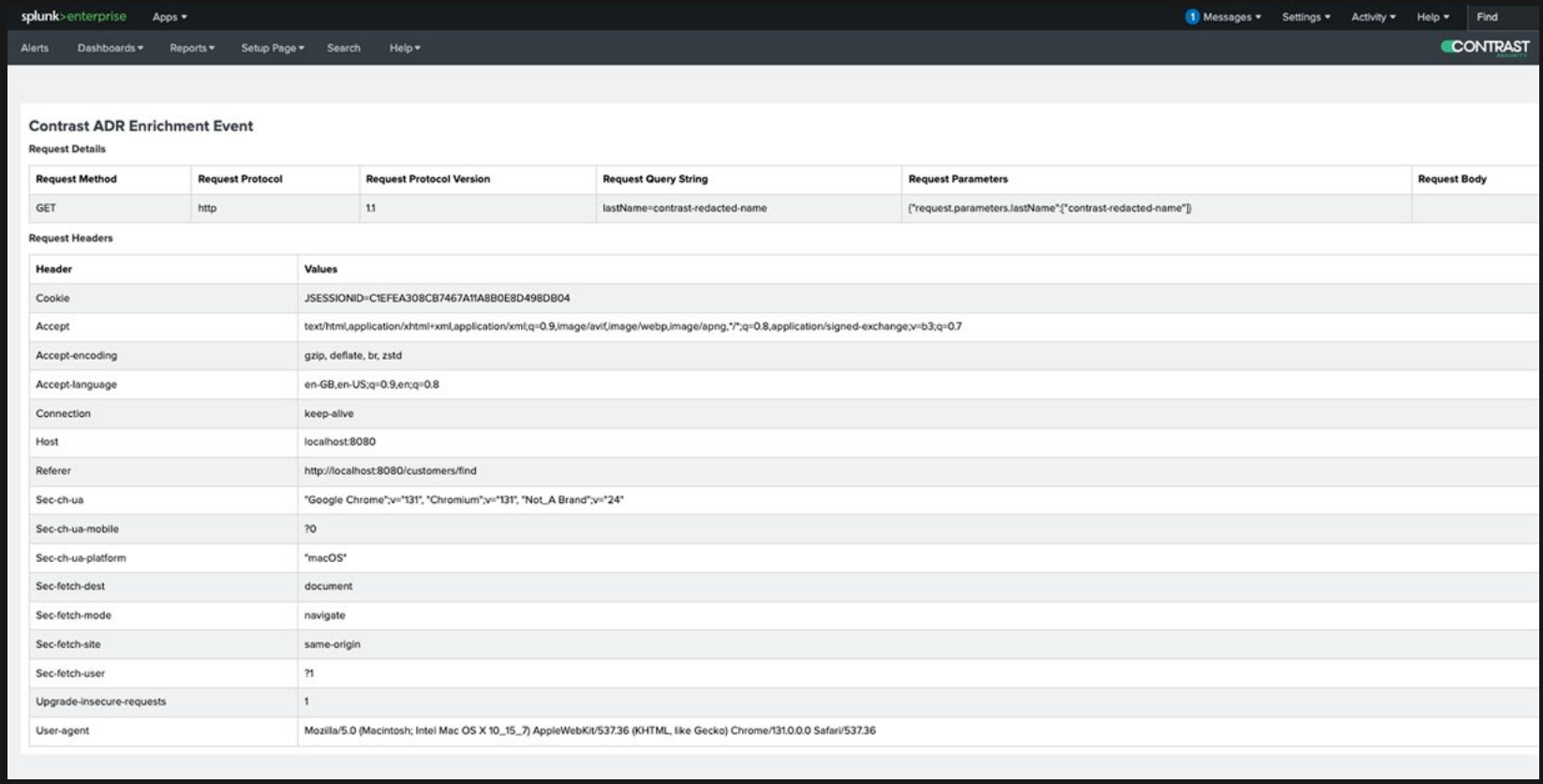
Benefits of integrating Splunk and Contrast ADR

TABLE OF CONTENTS

Introduction

Contrast Security Application Detection and Response seamlessly integrates with Splunk, delivering deep application insights that empower Security Operations Center (SOC) teams to identify and respond to sophisticated attacks faster.

Among all the tools and technologies available today to SOC teams and SecOps professionals, what makes this integration unique? This eBook provides further details on why this integration is needed today, how it works and how it benefits organizations looking to more effectively detect and respond to modern attacks.



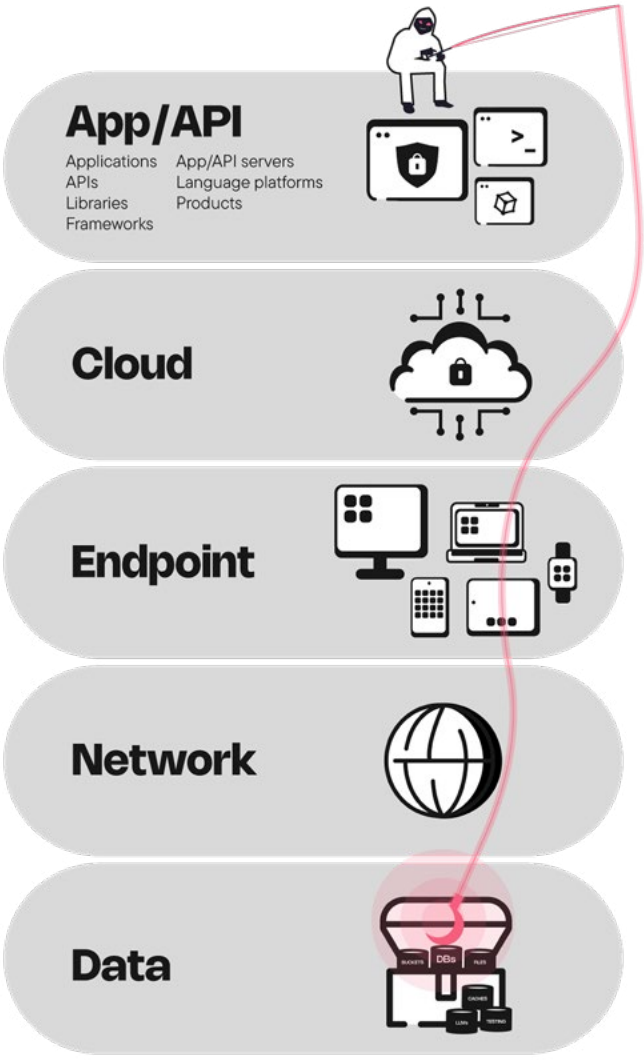
Why do SOC teams need more visibility for the application layer?

Overall, organizations have gotten much better at securing their networks, endpoints and even their cloud environments. Securing these layers is far from perfect, of course, but defenses here have improved significantly over the past few years.

As a result, attackers have begun targeting the application layer more earnestly. The number of data breaches caused by an exploited vulnerability rose 280% year-over-year, according to the 2024 Verizon Data Breach Investigations Report (DBIR).

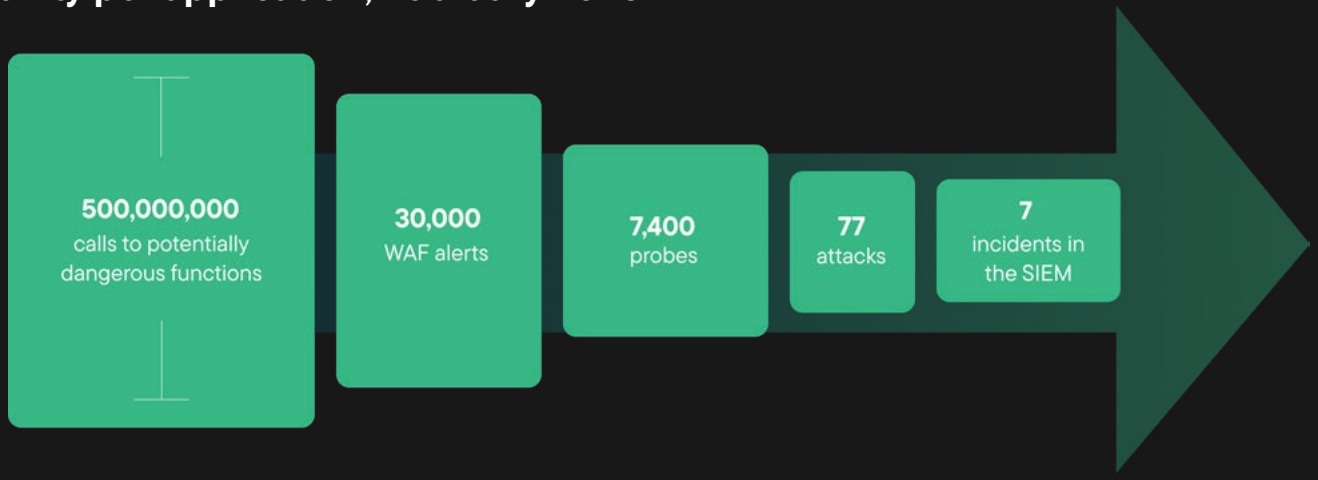
78% **of cybersecurity professionals reported experiencing an API security incident in the past 12 months.**

What can explain this dramatic rise? For one, organizations are releasing more software and more code than ever before. After all, so much of modern life — banking, shopping, making medical appointments, etc. — is facilitated by software and applications. Thus, the value that an attacker gets from successfully hacking an application grows, too.



According to Contrast Security internal data, the typical application or Application Programming Interface (API) gets attacked successfully around 50 times a month. These are attacks that are confirmed to reach their intended vulnerability and are about to launch the exploit. These numbers do not highlight signatures or theoretical attacks, only what's actually a dangerous anomaly.

Security activity per application, February 2025



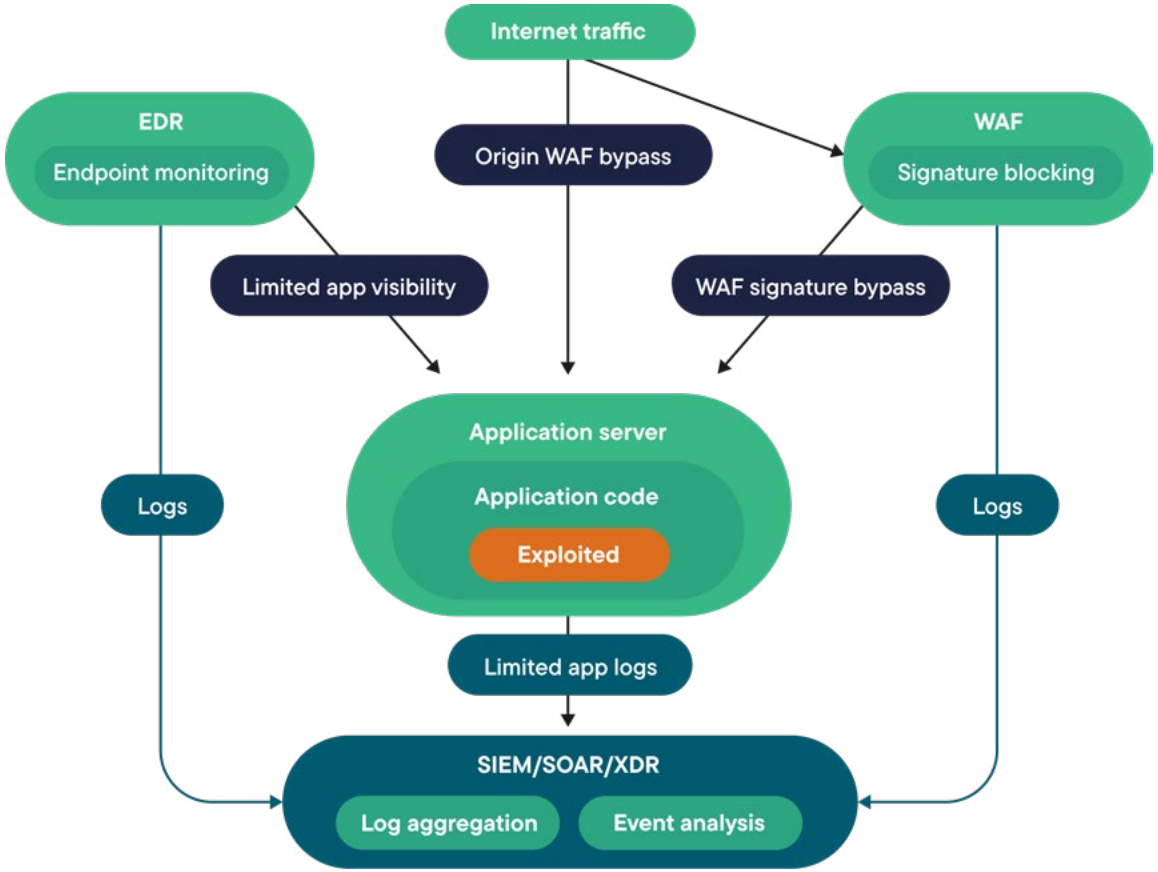
In addition, the teams on the front line of cybersecurity at major organizations, such as SOC analysts, have historically lacked requisite visibility into the application layer. In particular, the main tool in place to protect live applications at many businesses is a Web Application Firewall (WAF). While WAFs are helpful in many regards, they rely on static signatures or known patterns to identify threats, two methods that sophisticated attackers can evade. Further, most WAFs generate a high number of false positives or alerts that aren't clearly actionable.

Consider this: There was a 50% increase in zero days being exploited year-over-year, according to Google Threat Analysis and Mandiant. Here, WAFs will have no chance to stop these kinds of attacks, as they can only conceivably block known attacks — and even then a WAF may not provide full, adequate protection.

Beyond WAFs, tools like Endpoint Detection and Response (EDR) and Cloud Detection and Response (CDR) solutions are invaluable in the escalating fight against increasingly sophisticated adversaries. However, these tools do not provide comprehensive protection, particularly for applications. By the time an attack that originates in the application layer reaches the network or an endpoint, it's probably too late to fully contain the damage.

WAF		Contrast ADR
Strength	**Weakness**	**Solution**
Protects against common web attacks such as Distributed Denial of Service (DDoS) attacks and certain cross-site scripting attacks. Reduces load off your application servers by blocking network traffic of simple and common web application attacks.	Relies on static signatures or known patterns to identify threats: two methods that sophisticated attackers can evade. High number of false positives or alerts that aren't clearly actionable.	Contrast ADR provides deep visibility into the application layer, allowing you to detect and block attacks at their source before they can cause damage or spread throughout your environment. ADR is designed to minimize false positives and provide actionable insights, enabling you to focus on the most critical threats.
EDR		**Contrast ADR**
Strength	**Weakness**	**Solution**
Monitors and protects endpoints (e.g., desktops, laptops or servers.)	No way to know if code inside the application is manipulated.	With deep visibility into application behavior and data flows, your teams can identify anomalies and potential threats that may have bypassed traditional security tools.
Detects suspicious activity and investigates incidents at the operating system and network level.	Can miss attacks that occur entirely within the application layer.	ADR real-time threat detection and response capabilities enhance the overall security architecture by providing an additional layer of protection against sophisticated attacks.
Provides response capabilities to contain and remediate threats on the operating system level.	SOC may have to wait until an application is compromised before EDR detects the threat.	ADR enhances proactive threat detection capabilities, so you can identify and mitigate application-layer attacks earlier.

Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) solutions are only as good as the underlying data they're capturing and working with. Without good data on what's really happening in the application layer in real time, SOC analysts can't be as effective as they need to be.

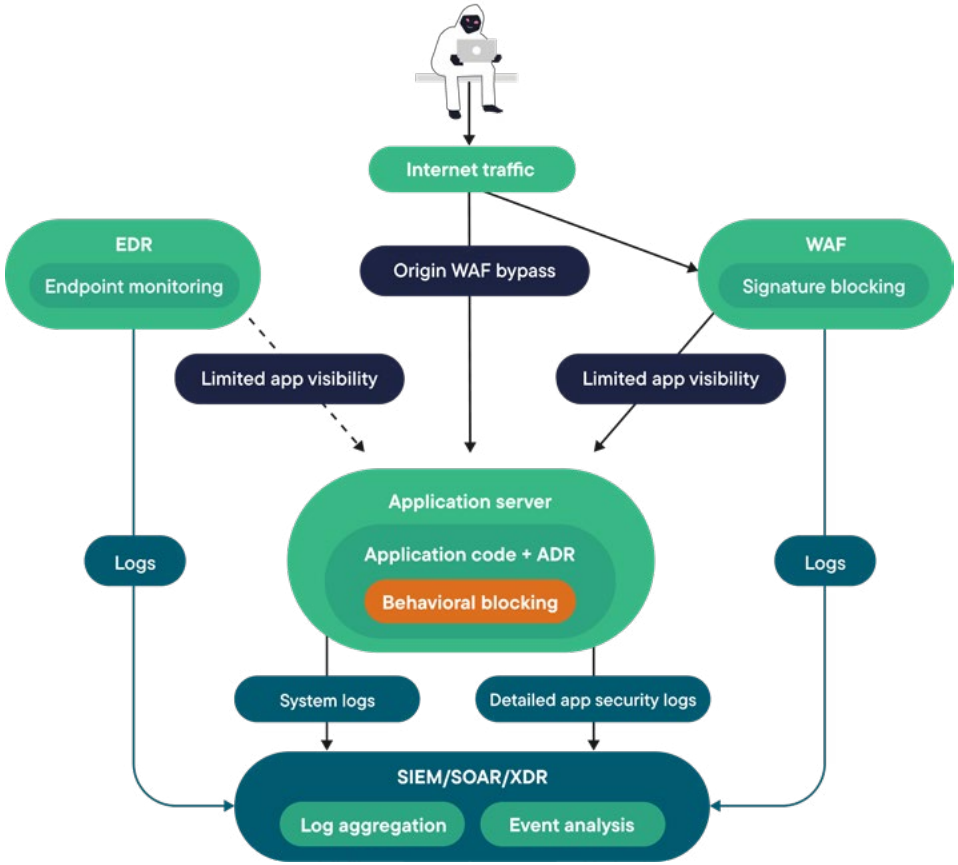


But the integration between Contrast ADR and Splunk solves this problem.

Understanding the partnership

This integration seamlessly blends Contrast's deep application-layer insights with Splunk's powerful SIEM capabilities, enriching the Splunk Dashboard and searches with crucial application context. This provides a unified view of the security landscape and strengthens an organization's overall security posture.

Contrast ADR instruments applications from within, providing deep and continuous visibility into application behavior and identifying attacks with high accuracy. This real-time security telemetry is seamlessly integrated into Splunk, enriching security events with crucial application context. This empowers security teams to identify sophisticated attacks that bypass traditional tools, accelerate investigations and remediate with correlated data.



Key benefits and use cases

The integration of Splunk and Contrast ADR enables the SOC to detect application threats, investigate with context and eliminate the noise. Let's dive into each one of these benefits.

Detect application threats

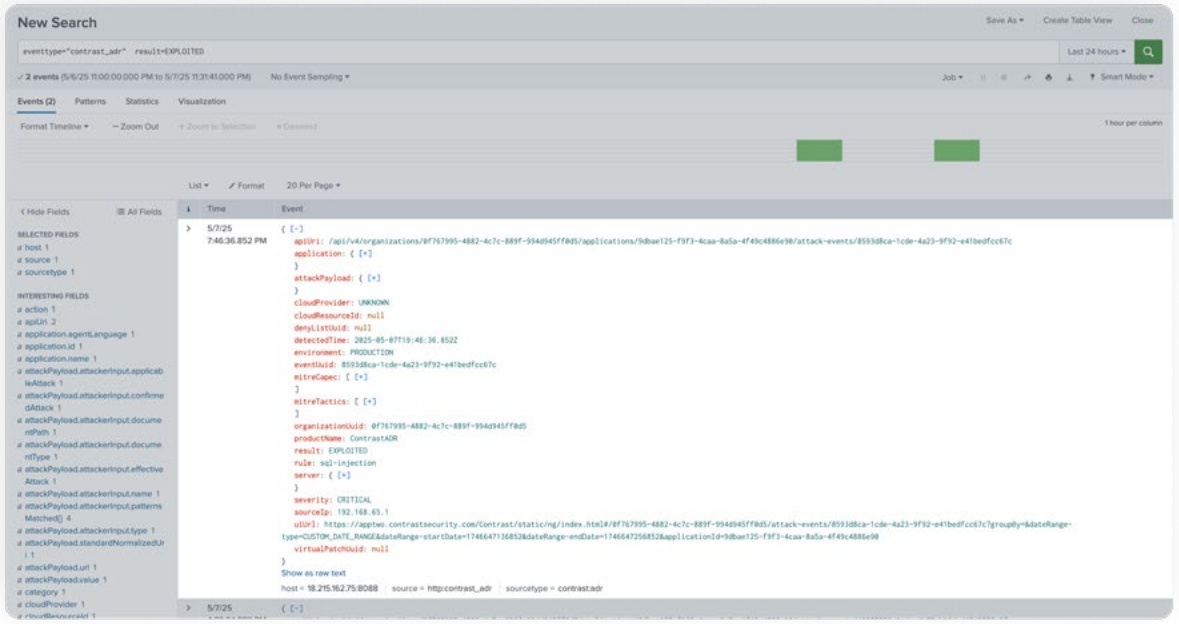
Traditional security tools offer limited visibility into the application layer, leaving organizations vulnerable to attacks that exploit application-specific vulnerabilities. Contrast ADR instruments applications to provide continuous visibility into their behavior, enabling the detection of attacks that bypass traditional security measures.

Contrast ADR also enables SOC teams to detect and respond to zero-day exploits. Contrast ADR uses deep instrumentation to observe actual application behavior, allowing it to detect anomalous activity indicative of attacks, even if they've never been seen before. This real-time threat data is fed into Splunk, enabling security teams to quickly identify and respond to zero-day attacks targeting their applications.

Investigate with context

Traditional security tools lack visibility inside of applications, making it difficult to hunt for threats concealed within complex codebases. Attackers can exploit this blind spot to hide malicious activity and evade detection.

Integrated with Splunk, real-time data from Contrast ADR empowers security teams to identify sophisticated attacks, understand the full context of attacks (including the specific code being exploited) and guide responses with runbooks for faster and more consistent incident response.



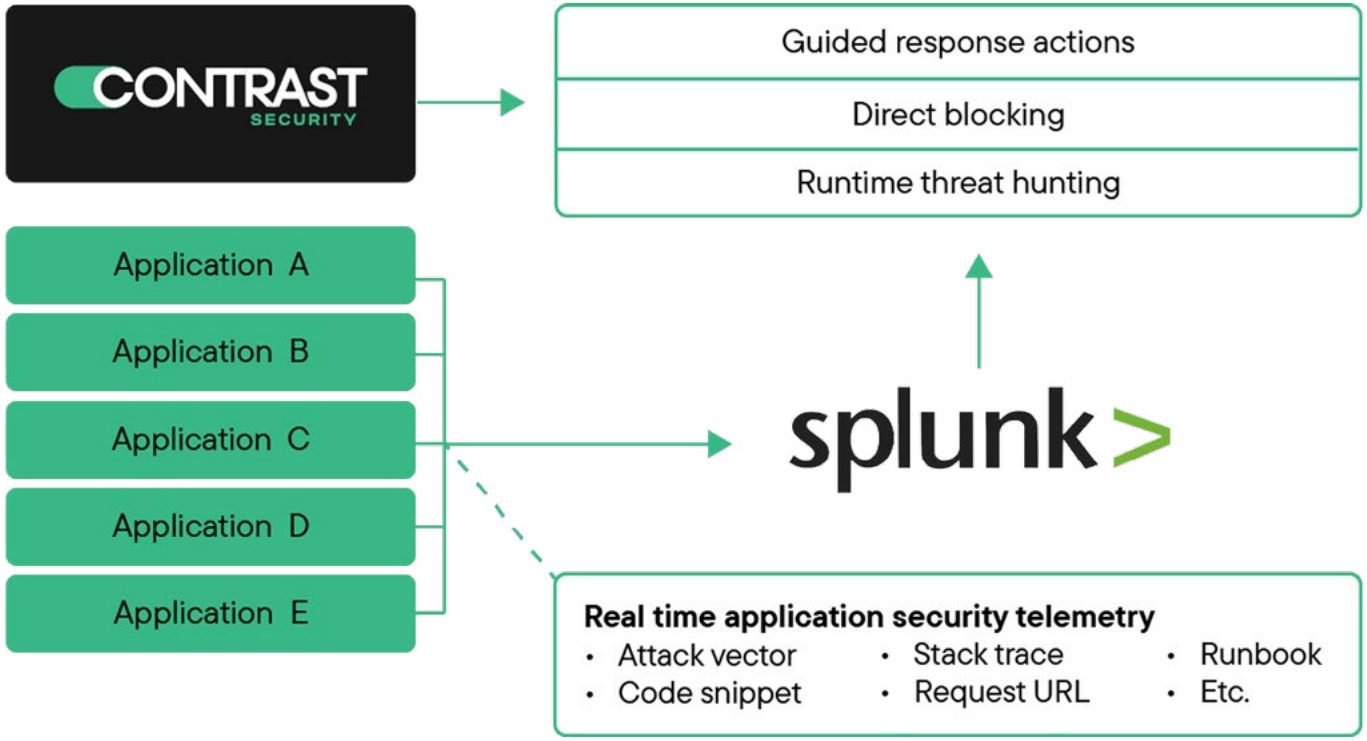
Eliminate the noise

Thanks to this integration, SOC teams focus on actual application threats with precise, actionable alerts within Splunk. This ensures that teams are only responding to and investigating real issues and not false positives.

Specifically, Contrast ADR instruments applications to provide deep visibility into their runtimebehavior, empowering threat hunters to identify suspicious activity within the application layer. By feeding accurate telemetry into Splunk, security teams can leverage Splunk's powerful search and analysis capabilities to hunt for Indicators of Compromise (IOCs), uncover hidden threats and effectively identify suspicious patterns of data exfiltration.

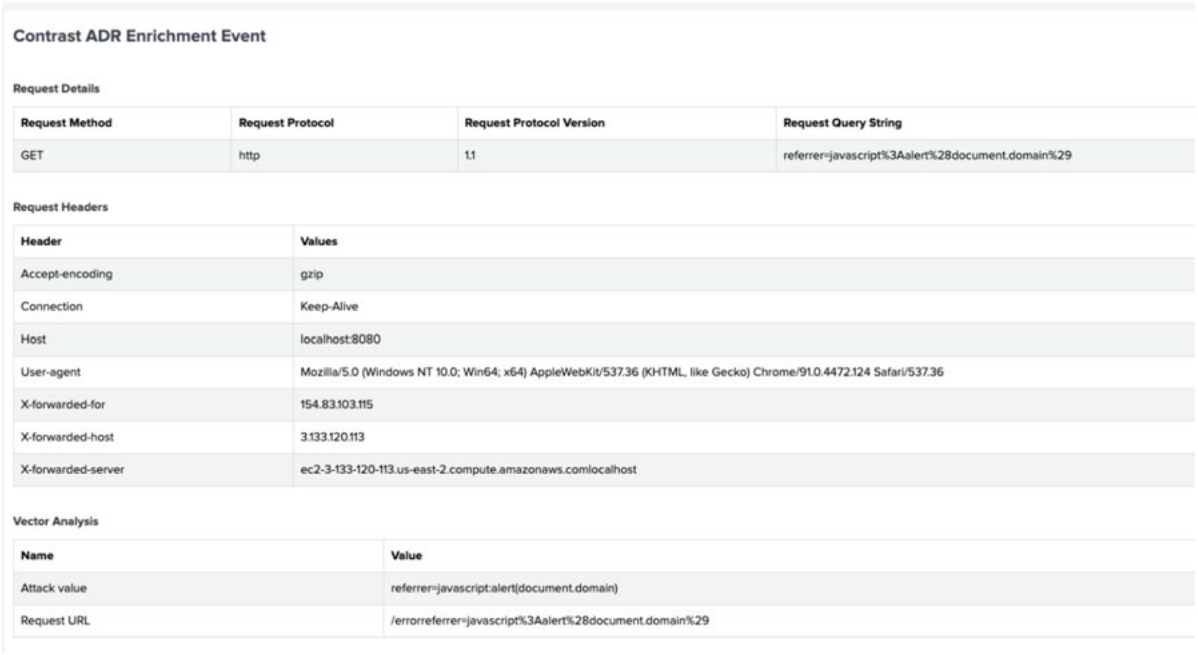
By combining high-confidence application security insights with broader security context, SOC teams can achieve a unified view of their security landscape to significantly reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) for application attacks. This integration empowers organizations to protect their critical applications and data from increasingly sophisticated attacks leveraging the application layer.

How this integration works in real life



Real-time data is seamlessly integrated into Splunk, enriching security events with crucial application context. To get a sense of how this integration works, consider what happens with an unsafe deserialization attack.

Imagine an enterprise web application that exchanges data with a Javascript user interface in the browser. The developer simply followed common coding patterns and "serialized" data objects in the browser into a stream of bytes that are "deserialized" back into objects in the web application. The developer didn't realize that they had inadvertently introduced a serious unsafe deserialization vulnerability, and it made it into production.



Contrast ADR Enrichment Event

Request Details

Request Method	Request Protocol	Request Protocol Version	Request Query String
GET	http	1.1	referrer=javascript%3Aalert%28document.domain%29

Request Headers

Header	Values
Accept-encoding	gzip
Connection	Keep-Alive
Host	localhost:8080
User-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
X-forwarded-for	154.83.103.115
X-forwarded-host	3.133.120.113
X-forwarded-server	ec2-3-133-120-113.us-east-2.compute.amazonaws.comlocalhost

Vector Analysis

Name	Value
Attack value	referrer=javascript:alert(document.domain)
Request URL	/errorreferrer=javascript%3Aalert%28document.domain%29

The ADR platform

The ADR platform continuously monitors the entire application stack in real time. During routine operations, ADR detects an attack that leverages this unsafe deserialization vulnerability. The system generates a detailed incident report containing the complete HTTP request details, including the payload; a stack trace of the deserialization operation, captured directly from the running code; and a contextual diagram providing the security context of the route being attacked.

A WAF would not stop this attack from reaching the application. The WAF doesn't have visibility into the serialized object and therefore can't tell that the malicious payload is any different from normal traffic from a legitimate user.

In addition, the company's cyber defenses, such as EDR, would only detect the attack if theattacker propagates from the compromised application to the endpoint. These platforms are primarily focused on monitoring endpoints, networks and logs for attack patterns and anomalies. The attack within the serialized object is invisible to these security platforms because it's buried in the serialized data and nothing is logged for this operation.

Conclusion

With application attacks on the rise, organizations need better visibility into the application if they stand a chance at detecting and mitigating these attacks in a timely manner. Contrast ADR, with its deep visibility from inside the application, provides just this level of security. By combining the observability and visibility of Contrast ADR with Splunk, SOC teams are able to quickly and easily get the context and information they need to safeguard mission-critical applications.

Interested in seeing the benefits of Contrast ADR + Splunk for yourself?

Get a demo

6800 Koll Center
Parkway Ste. 235
Pleasanton, CA 94566
Phone: 888.371.1333