Why Contrast ADR?

The application layer leaves you vulnerable

Every month, attackers launch around 26 billion attacks targeted at applications and application programming interfaces (APIs). Although security teams manage to filter out most of the bad traffic, 78% of Security Operations Center (SOC) teams say they have experienced an API security incident in the last 12 months. The troubling part: 70% of critical application incidents take longer than 12 hours to resolve.

The reality is that the SOC struggles to protect applications and APIs effectively because they currently have to rely on network, endpoint or cloud technology to monitor and secure applications.

Why Web Application Firewalls (WAFs) and Endpoint Detection and Response (EDR) don't effectively protect applications

Let's focus on the WAF for an example. Your WAF probably does a great job in filtering out network-layer traffic and is great at protecting you from Distributed-Denial-of-Service (DDoS) attacks. However, intelligently crafted attacks can easily bypass the WAF because of their reliance on static signatures. The main problem here is that a WAF is often your last line of defense against application attacks; when a WAF gets bypassed you lose all visibility to what's happening at the application layer. And let's not even talk about the accuracy of WAF alerts.

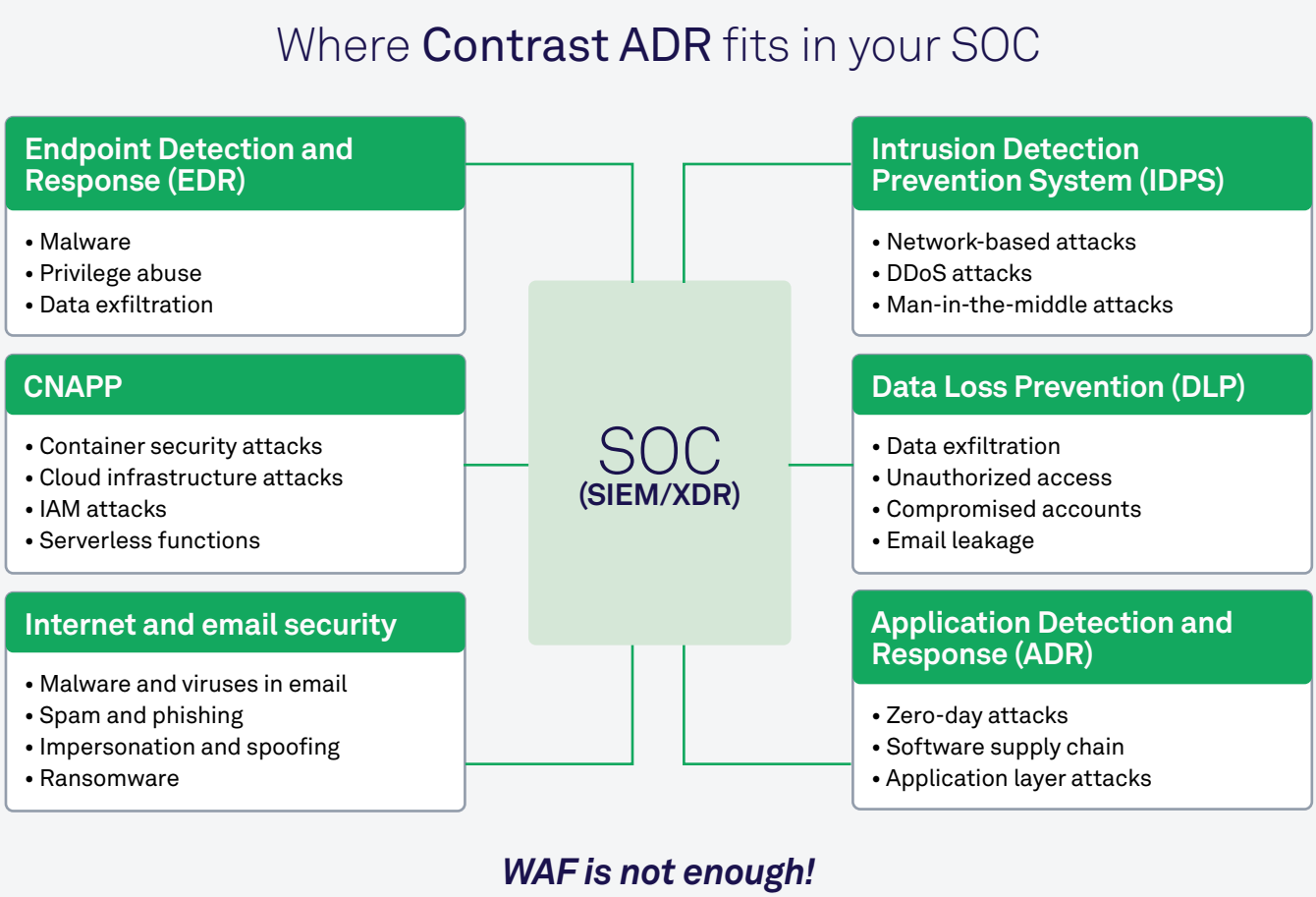
At the same time, your SOC might rely on EDR to detect threats on the servers, but this tooling does not have direct visibility into what is going on inside the application. SOC teams would need to wait for an attacker to execute something on the server endpoint itself in order for EDR to see it. By this point it's often too late to stop a damaging breach. The same logic can apply to other detection and response technologies like Network Detection and Response (NDR) or a Cloud-Native Application Protection Platform (CNAPP). Until now no tool was designed to solve the application layer issue.

HOW ADR HELPS TWO FAMILIAR SOC TOOLS WITH APPLICATION ATTACK DETECTION

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.

Waiting until an application breach has happened before your security team comes into action is not the answer. You need visibility from inside the application layer so you can monitor and protect each application at the code level. By eliminating your application blindspot you can protect your applications and APIs from exploits and zero days.

How Contrast ADR works to effectively safeguard your applications



Contrast ADR eliminates your application blindspot and protects applications and APIs by providing unparalleled visibility, accuracy and protection. By operating from within, the SOC gets real-time visibility that is needed to see application attacks, accelerating detection and enabling them to respond to suspicious activity within the application code itself.

By blocking known and unknown vulnerabilities, including zero days, Contrast ADR empowers organizations to stop application threats before they can cause damage. Continuous vulnerability assessment and seamless integration with SOC tools provide context-rich information about application-level threats, enabling them to secure with confidence, achieving effective security and protection over their exposed application layer.

Contrast ADR takes a fundamentally different approach compared with any other tool in the market. It employs instrumentation inside of the application that becomes part of each application itself. This gives Contrast continuous, real-time visibility into every change in code, every data flow and every potential attack surface.

Because it's inside your application, Contrast ADR sees attacks as they happen, not after the damage is done. Intelligent sensors detect suspicious behavior, analyze it against known attack patterns and flag potential exploits in real time.

When an attack is detected, Contrast ADR doesn't just send an alert. It can automatically block the attack at the application layer, preventing it from causing harm. Contrast ADR also provides the detailed insights an incident response team needs to understand the attack, assess the impact and work with the SecOps team on mitigating the vulnerability, down to the line of code that needs to change to remove the risk.

The result is continuous protection, fewer false positives and faster, more effective incident response on the application layer. That's how Contrast ADR helps you stay ahead of threat actors and keep your applications secure.

For a more detailed overview of Contrast ADR, how it works and how it will benefit your organization, check out this whitepaper, The Case for Application Detection and Response (ADR), written by Contrast CTO Jeff Williams, founder of the OWASP Top 10.

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

Contrast SECURITY