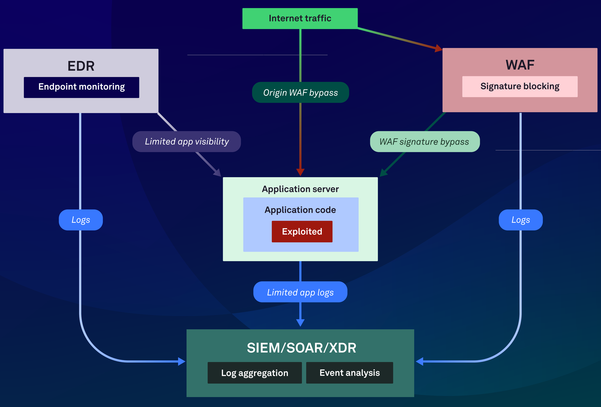
Contrast SECURITY

The limitations of existing Application Security (AppSec) approaches

It's crucial to understand a significant gap in many organizations' security strategies: the lack of robust application-level threat detection.



Common option #1: Web application firewalls (WAFs)

Many organizations rely on WAFs as their primary defense against application-level threats. However, this approach has several critical limitations:

Ineffective SOC integration:
WAFs lack the required context to feed actionable application-level information to their security operations center (SOC).

Network-level focus:
WAFs operate at the network level, analyzing incoming traffic patterns to detect potential threats, but this provides limited visibility into what's happening within the application itself.

False positives:
WAFs often generate a high number of false positives and are hard to tune. This can overwhelm security teams and lead to alert fatigue.

Vulnerability to bypass techniques:
Attackers can often circumvent WAF protections using methods like encoding variations, protocol-level evasion or payload padding.

Common option #2: Endpoint detection and response (EDR)

EDR solutions focus on monitoring and protecting individual endpoints within an organization, but this technology has its own set of limitations when it comes to AppSec:

Focus on endpoint activities:
EDR primarily monitors system-level events and processes, not application-specific behaviors.

Limited visibility inside applications:
EDR solutions don't have insight into the internal workings of applications.

Delayed detection:
EDR may not detect attacks that exfiltrate data directly from the application layer.

Gaps in cloud and web application coverage:
As applications move to cloud-based services, traditional EDR solutions may have gaps.

Want to be better equipped to stop modern application attacks?

Learn how

Contrast SECURITY
All rights reserved. ©2024 Contrast Security, Inc.
contrastsecurity.com