THE CASE FOR APPLICATION SECURITY MONITORING

Improving Application Performance and Resilience with Security Monitoring

More and more companies interact with customers via digital channels, making the digital customer experience they provide a critical component of business success.[1] A crashed or poorly performing application will negatively impact customer confidence and drive up customer churn. Software has to be resilient to a broad range of potential disruptions to avoid these scenarios.

Of course, this places an unprecedented amount of responsibility and pressure on IT Operations and DevOps teams. They have to maintain software availability and functionality, and optimize the performance of customer facing applications – all while deploying faster. The move toward rapid development and deployment models, such as Agile and DevOps, has increased the need for continuous visibility, monitoring and analysis of applications during development and at runtime[2].

RESILIENCE OF SOFTWARE HAS BECOME MORE CRITICAL THAN EVER BEFORE

The need for resilience is therefore at an all-time high and IT Operations teams typically focus on the following key levers to maintain it[3]:

- Application acceleration
- Load balancing
- Overall performance management

WHERE IS SECURITY?

Attacks on live applications are a leading cause of outages, disrupt functionality and affect performance. So, while security is a key component of resilience, it is not on the above list of levers. It is usually an afterthought or perceived to be solely the responsibility of Information Security. One of the main reasons for that is, historically, IT Operations teams were not equipped with tools to continuously monitor application security at a granular level[3].

Monitoring the Security of a Running Application has been a Guessing Game

Until recently, we knew next to nothing about the security state inside a running application – unless developers built in custom logging. Without security visibility, security pros would typically:

- **Hope** the developers wrote secure code
- Harden the platform (e.g., OS, server, container) that the application is running on and **hope** nothing gets through
- Deploy an edge device (e.g., IPS, WAF) and **hope** blocking suspicious traffic is sufficient
- **Hope** your SOC finds the attack in time
- **Hope** that your incident response team can respond effectively
- **Hope** you have talented enough software engineering resources to fix an exploited vulnerability in code

ENTER APPLICATION SECURITY MONITORING

The advent of **Application Security Monitoring (ASM)** provides IT Operations and Security teams unprecedented visibility and control over the security of the application layer.

Operations teams already use similar tools for monitoring performance of the running application: Application Performance Management (APM) solutions such as AppDynamics, Dynatrace or New Relic. These telemetry products use an agent-based technology to instrument the running application and measure performance.

ASM solutions leverage the same technology to monitor security aspects of the application.

> “We were searching for developer-oriented technologies like New Relic and AppDynamics for application for security....Contrast emerged as the most exciting.”
>
> John Monagle, General Catalyst

EXTENDING APM TECHNOLOGY TO MONITOR SECURITY

According to Gartner, Application Security Monitoring (ASM) and APM technologies often have a common architectural approach with respect to how they perform their primary functions[2]. ASM solutions, like Contrast Protect, use agent-based technology to instrument applications and monitor security aspects of applications in production environments. Application Security Monitoring agents that gather security-relevant data and analyze it for indications of breaches are a logical adjacency to APM tools and provide many benefits to Operations teams[2].

ASM solutions fill the visibility gap that current Security & Operations teams experience when monitoring production applications for attacks. Since agents reside inside the application, they provide deep and granular visibility into the running application's security state. Compare that with edge solutions (like an Intrusion Prevention System (IPS) or Web Application Firewall (WAF)) that detect at the perimeter: so there is no visibility into whether the application is truly vulnerable, only "black box" data on application communications.

In Addition to Application Layer Visibility, Application Security Monitoring Offer These Key Advantages Over Legacy Tools:

Cloud-ready: ASM solutions are portable, so applications can be protected anywhere they are deployed. And, they don't require reconfiguration when new code is deployed or application scaled. On the other hand, IPS and WAF products need to be tuned with each new code deployment, which is far from ideal in DevOps environments. In addition, if applications scale, move or infrastructure changes occur, edge solutions need to be re-deployed, or alternate solutions need to be brought online.

Deployment: ASM agents offer rules that are functional out of the box. IPS and WAF products, on the other hand, require setup of rules that need constant adjustment and coordination with network teams to ensure they see the right traffic.

Performance & Stability: Edge solutions fundamentally add latency to applications because of the added network hops and traffic scan time. Well architected Application Security Monitoring agents, however, only add negligible latency even at scale.

Key Questions to Ask When Evaluating ASM Solutions:

- Do you know enough about an attack while it's happening?
- Can you distinguish between an attack or a probe?
- How much time do your teams spend resolving false positives?

If using an edge solution:

- How long did it take you to set up your edge device?
- How often do you update your rules?
- How does your deployment change when your apps scale or move around?
- How much does it cost to add an extra device?

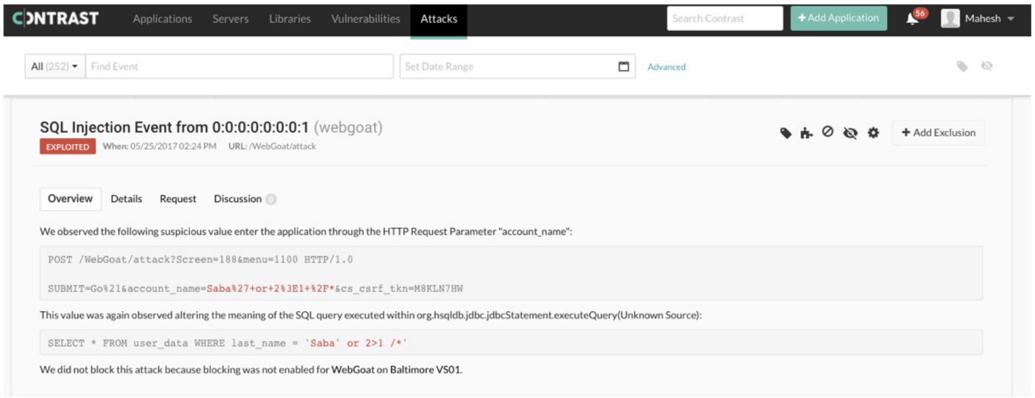
CONTRAST PROTECT – BEST IN CLASS APPLICATION SECURITY MONITORING

With Contrast Protect, You Get Unprecedented Visibility

Contrast Protect's patented deep security instrumentation allows it to go deeper into the application stack. This allows you to (1) protect the full application stack, (2) gather detailed information about an attack as it happens and (3) block the attack instantly. For each attack, Contrast sees:

- Full HTTP request
- Stack trace (including lines of code)
- Targeted web page/folder
- Targeted server
- Attack vector details
- Attacker IP address
- Application account associated with attack
- Attack specific data (not exhaustive):
- XSS: HTTP response data
- SQLi: Full database query
- Path Traversal: Full file path
- Padding Oracle: Exception details
- Command Injection: OS command
- Remediation guidance
- Time of event
- Rate of attack
- Severity of attack

Figure 1. Contrast Protect – Attack Overview



SQL Injection Event from 0:0:0:0:0:0:0:1 (webgoat)

EXPLOITED When: 05/25/2017 02:24 PM URL: /WebGoat/attack

We observed the following suspicious value enter the application through the HTTP Request Parameter "account_name":

```
POST /WebGoat/attack?Screen=188&menu=1100 HTTP/1.0

SUBMIT=Go%21&account_name=Saba%27+or+2%3E1+%2F*&cs_csrf_tkn=M8KLN7HW
```

This value was again observed altering the meaning of the SQL query executed within org.hsqldb.jdbc.jdbcStatement.executeQuery(Unknown Source):

```
SELECT * FROM user_data WHERE last_name = 'Saba' or 2>1 /*'
```

We did not block this attack because blocking was not enabled for WebGoat on Baltimore VS01.

In addition, instrumentation enables Contrast Protect to distinguish between probes and and real attacks / exploitation attempts. These events can be sent to monitoring / SIEM solutions of choice using different syslog levels.

With Contrast Log Enhancement, Monitor Anything Inside the Application

As mentioned above, Contrast Protect monitor mode has standard attack and event logging that provides unprecedented visibility. However, Contrast Protect Log Enhancement extends this capability into the inner workings of application and user behavior. Log Enhancers enable users to log anything in an application and send that data to your log management or SIEM system of choice. Log in failures, privilege escalation, specific database calls and many other aspects of the application environment can be logged and used for correlation to identify indicators of compromise. Contrast seamlessly integrates into any existing monitoring infrastructure. This allows operations teams to leverage this newly available intelligence into their own systems instead of adding another screen or dashboard.

With Contrast Protect, Ensure Best in Class Performance

Contrast Protect provides best in class performance among current solutions. Protect was designed to be fundamentally more efficient (and secure) through deep application level instrumentation. While most edge device vendors typically have per request performance impacts in the 10-100ms range, Protect only adds 0.05ms (50 microseconds).

This performance testing was conducted by Contrast Labs, Contrast Security's research arm, to measure the overhead of Contrast Protect on applications in normal, moderate attack and heavy attack scenarios.

If you are looking to optimize for performance when looking to secure your application production environment, Contrast Protect has demonstrably minimal impact.

CONCLUSION

Application Security Monitoring products are like Application Performance Monitoring solutions: They bring a much-needed level of visibility to the world of continuous integration and continuous deployment of software. They beat out edge technologies like WAF and IPS in delivering insight into the security state of production applications, and also in terms of scalability and cloud-readiness. Application Security Monitoring solutions are destined to be a critical tool in the DevOps toolchain for organizations who need to optimize digital customer experience – which is virtually every organization today.

If your organization is ready to make a change and see ASM in action, then sign up for a personalized demo of Contrast. Visit *www.contrastsecurity.com* and click the "Get Demo" on the top of any page.

[1] https://newrelic.com/resource/digital-customer-experience-best-practices
[2] https://www.gartner.com/doc/3692717/application-performance-monitoring-application-security
[3] http://www.esecurityplanet.com/network-security/application-performance-management-offers-security-benefits.html

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.