Trend Micro

CLOUD ONE™ - APPLICATION SECURITY

Detection and protection for modern applications and APIs built on your container, serverless, and other computing platforms

Businesses are aligning to cloud-native application architectures faster than ever before. Brought on by streamlined operations processes and the flexibility in build pipeline development tools and services, businesses are using application development as a strategic investment in the hopes that they'll achieve improved application delivery and customer satisfaction.

A recent study conducted by research firm ESG indicated that 35 percent of businesses were using a combination of containers and serverless platforms for their application builds, with serverless adoption was quickly on the rise.

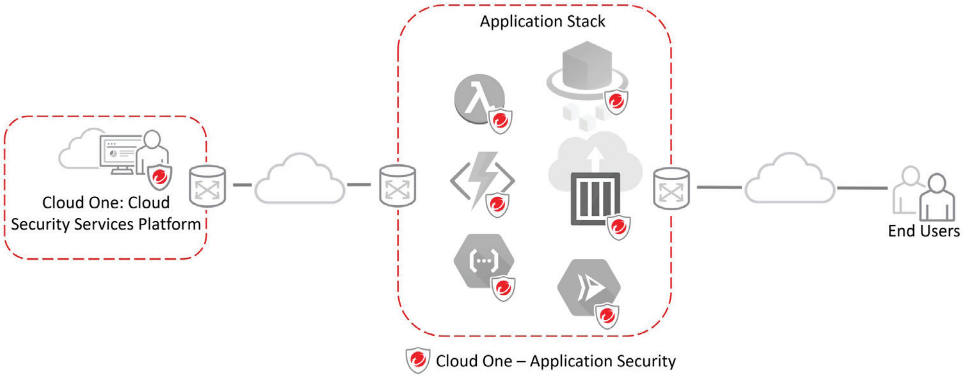
It continues to become easier to make applications for the web, and businesses are using them at ever-increasing rates. Unfortunately, not everyone–including developers and those who must defend their systems–knows how to secure them properly. With the interconnection of most web applications and IT systems, this lack of knowledge exposes enterprises to security risks from hackers who know how to exploit vulnerabilities in order to gain access to systems, software, and sensitive data.

Trend Micro Cloud One™ – Application Security is built for speedy deployment, with minimal impact on development streams and performance. It only takes a minute to add the library to your application, and there is no need to change your development code. Application Security bootstraps itself into your application at runtime, as opposed to an SDK that has to be integrated into the application. You just need to include the Application Security library with your application and activate it with the application keys. This approach simplifies how security is delivered and is a significant shift for application developers who need immediate, real-time protection for their apps and customers.

Application Security minimizes design and deployment risks by protecting against sophisticated hacks from inside the application. Optimized for modern application architectures, Application Security immediately blocks unwanted activity in real time to protect data and business logic. The result is unprecedented protection, keeping web application owners and their users safe from hacks with the highest degree of accuracy.

Application Security's Key Benefits

- Detects and protects against the OWASP Top 10 runtime threats, including SQLi. Remote command execution (RCE) threats are also provided in detection mode.
- Blocks injection and other automated attacks
- Complete coverage and reporting of every attack instance
- Provides full diagnostic details about code vulnerabilities
- Avoids time-wasting false positives and theoretical issues
- Offers insight into an attacker's identity and attack methodology
- Installs in two minutes–no source code changes required


Application Stack
Cloud One: Cloud Security Services Platform
End Users
Cloud One – Application Security

VULNERABILITY DETECTION

Bots, hackers, and other bad actors will find and exploit vulnerabilities in web applications, which are caused by coding errors and weaknesses in dependencies.

NO CODE CHANGES REQUIRED

The self-contained Application Security agent runs inside the process of your application without requiring any code changes in the application itself.

SECURE YOUR CUSTOMERS' DATA

Application Security is designed specifically to secure web assets in the cloud and within local networks, protecting your customers' data and your business.

AUTOMATIC PROTECTION

When your app is exposed to a malicious attack, the agent identifies the attacker, type of attack, and blocks it. User data is protected, and you have the insight you need to fix the coding vulnerabilities.

One of the key differentiators with Application Security is the ability to have malware detection where your web application might accept file uploads, such as attachments, pictures/avatars, or PDFs.

Hackers can take advantage of the this by uploading malicious files, such as excel spreadsheets with malicious macros, images with ImageTragick payloads, or PDFs with malicious scripts. You need to be able to quickly and easily block this threat prior to any destination point without forcing developers to write or modify code.

HOW APPLICATION SECURITY WORKS

Application Security is based on runtime self-protection technology. The Application Security library is self-contained and independently protects its application, even if it becomes disconnected from the Application Security service. User data is never exposed outside the application, ensuring your apps remain compliant with data protection mandates.

Protects

Protects applications with known vulnerabilities until remediation resources are available

Blocks

Blocks sensitive data from being exposed by injection attacks

Secures

Secures hard-to-monitor applications, for example, when hundreds of web apps are running simultaneously on an internal network.

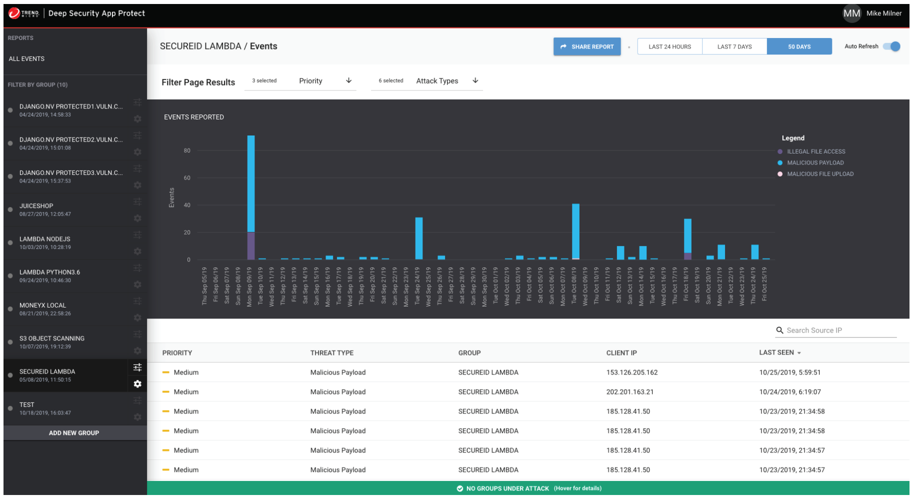
Knowledge is Power

How does Application Security differ from other RASP technologies?

There are three primary differences:

- Code-level visibility into attacks
- Broader coverage of different vulnerabilities
- Breadth of platform support

In addition to securing your customers and applications, Application Security enables development teams to quickly identify and prioritize vulnerability remediation efforts by providing vital information about the identity and severity of attackers.



REPORTS

ALL EVENTS

FILTER BY GROUP (10)

- DJANGO.NV PROTECTED1.VULN.C... 04/24/2019, 14:58:33
- DJANGO.NV PROTECTED2.VULN.C... 04/24/2019, 15:01:08
- DJANGO.NV PROTECTED3.VULN.C... 04/24/2019, 15:37:53
- JUICESHOP 08/27/2019, 12:05:47
- LAMBDA NODEJS 10/03/2019, 10:28:19
- LAMBDA PYTHON3.6 09/24/2019, 10:46:30
- MONEYX LOCAL 08/21/2019, 22:58:26
- S3 OBJECT SCANNING 10/07/2019, 19:12:39
- SECUREID LAMBDA 05/08/2019, 11:50:15
- TEST 10/18/2019, 16:03:47

SECUREID LAMBDA / **Events**

Filter Page Results 3 selected Priority 6 selected Attack Types

PRIORITY	THREAT TYPE	GROUP	CLIENT IP	LAST SEEN
— Medium	Malicious Payload	SECUREID LAMBDA	153.126.205.162	10/25/2019, 5:59:51
— Medium	Malicious Payload	SECUREID LAMBDA	202.201.163.21	10/24/2019, 6:19:07
— Medium	Malicious Payload	SECUREID LAMBDA	185.128.41.50	10/23/2019, 21:34:58
— Medium	Malicious Payload	SECUREID LAMBDA	185.128.41.50	10/23/2019, 21:34:58
— Medium	Malicious Payload	SECUREID LAMBDA	185.128.41.50	10/23/2019, 21:34:57
— Medium	Malicious Payload	SECUREID LAMBDA	185.128.41.50	10/23/2019, 21:34:57

✓ NO GROUPS UNDER ATTACK (Hover for details)

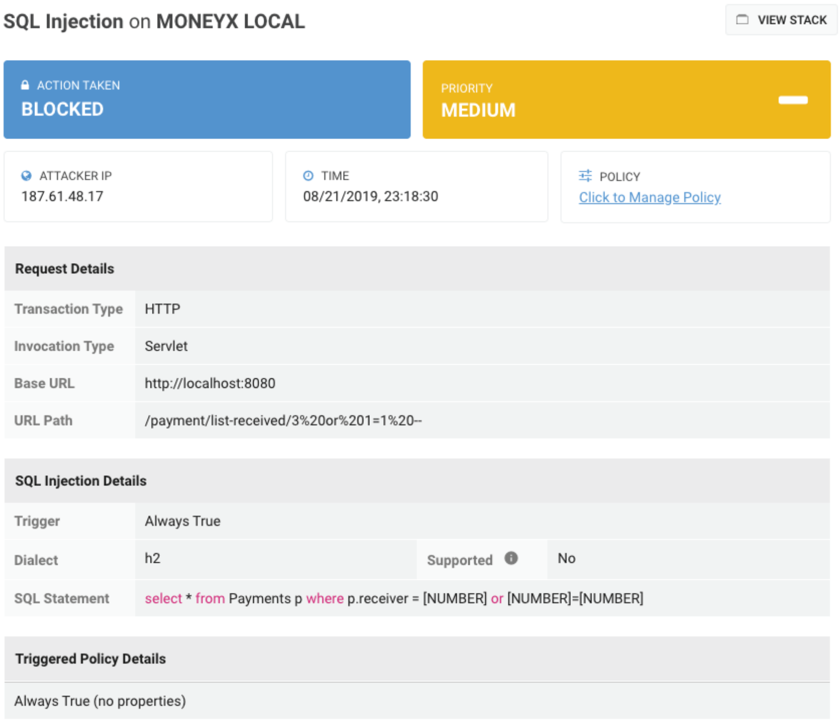
Application Security lets you monitor and review exploitation attempts across an unlimited number of applications. Attack details are propagated across your infrastructure, meaning, if an attack is detected on one application, it is immediately flagged on every app server and for every monitored app in your account.

While the performance experienced by an end user may vary depending on the application type and its overhead, Application Security strives to make sure requests can be handled in under 1 ms.

Application Security delivers information, such as the time, origin, and type, on every attack that occurs on your apps to a central reporting point. Over time, this information builds into a broad profile of the attacks impacting your networks, enabling your web security team to map trends and deploy appropriate resources.

Application Security also gives your developers full visibility into how the vulnerability in your code would have been exploited, including a stack trace down to the line of code (where relevant), reporting of request parameters, and how your app's behavior would have been modified.

.



SQL Injection on **MONEYX LOCAL**

ACTION TAKEN
BLOCKED

PRIORITY
MEDIUM

ATTACKER IP
187.61.48.17

TIME
08/21/2019, 23:18:30

POLICY
Click to Manage Policy

Request Details	
Transaction Type	HTTP
Invocation Type	Servlet
Base URL	http://localhost:8080
URL Path	/payment/list-received/3%20or%201=1%20--

SQL Injection Details			
Trigger	Always True		
Dialect	h2	Supported	No
SQL Statement	select * from Payments p where p.receiver = [NUMBER] or [NUMBER]=[NUMBER]		

Triggered Policy Details

Always True (no properties)

THREAT TYPE	DETECTION	PROTECTION
Open Redirect	✓	✓
Remote Command Execution (RCE)	✓	✓
Illegal File Access	✓	✓
SQL Injection	✓	✓
Antivirus/Anti-Malware Scanning of File Uploads	✓	✓
Malicious Payload	✓	✓

Application Security automatically protects your apps against common web-based attacks and many classes of zero-day vulnerabilities. Additionally, with Application Security's deep instrumentation, API's are protected similar to a web application across a JSON/GraphQL interface. With Application Security working inside the application, you only need one solution to secure both your web application and API's.

Application Security is part of Trend Micro Cloud One™, a cloud security services platform, which also includes:

- **Trend Micro Cloud One™ – Workload Security:**
  Runtime protection for workloads (virtual, physical, cloud, and containers)
- **Trend Micro Cloud One™ – Container Image Security:**
  Image scanning in your build pipeline
- **Trend Micro Cloud One™ – File Storage Security:**
  Security for cloud file and object storage services
- **Trend Micro Cloud One™ – Network Security:**
  Cloud network layer IPS security
- **Trend Micro Cloud One™ – Conformity:**
  Cloud security and compliance posture management

SYSTEM REQUIREMENTS

- Java (8 and newer)
- Python (2.7, 3.4 and newer)
- NodeJS (10 and newer)
- PHP (7.0 and newer)
- .NET coming soon (.NET Framework 4.5.2 and newer, .NET Core 2.0 and newer)
- Ruby coming soon (2.0.0 and newer)

TREND MICRO™

Securing Your Connected World

For details about what personal information we collect and why, please see our Privacy Notice on our website at: https://www.trendmicro.com/privacy
[DS02_Cloud_One_Application_Security_191108US]