5 #TrendTips to Implement Application Security

Application security can be difficult to implement, especially when you don't have access to the compute host in serverless container distribution systems or serverless functions. Perhaps, you are also looking to lift and shift an application to the cloud—maybe a legacy web application that you want to provide runtime-level protection against common web-based attacks for.

We've compiled ***5 #TrendTips*** to help you get started with bolstering your application security posture:

1. **Provide education and training** to help developers learn how to avoid common mistakes. A great resource to start with is OWASP Top 10 application security risks.
2. **Perform automated and human code review processes** to ensure that the code you are releasing is secure as possible. Review and test code frequently against the OWSAP Top 10 threats.
3. **Check that you are running up to date packages** especially open source packages and dependencies. Don't forget older packages as well—they may be more susceptible to exploits in your application.
4. **Provide a runtime application self-protection** (RASP)/Security as Code solution that is easy to setup, install, and monitor to make sure that your application is protected from threats in runtime state. This can also be used to see where bugs may be ending up in your code of your application.
5. **Set up a well-developed process** to alert and remediate the exploited application when a threat event happens.

Trend Micro provides solutions to help with implementing effective application security. As mentioned in #TrendTip #4, you can do that at the runtime level using RASP technology such as Trend Micro Cloud One™ – Application Security. This solution integrates our security libraries into your application stack and with just a single line of code your application is protected.

Since the solution uses Security as Code, your application can reside in a multitude of compute options servers and containers, including both serverless container and serverless functions.

Application Security can also provide additional application insight down to the line of code for that particular threat. Integration is also available with common notification methods such as Amazon Simple Notification Service (SNS), PagerDuty, New Relic, and Slack software.

Want to try it yourself? Start your free trial today to easily and quickly secure your applications with a single line of code, protecting your modern and legacy applications.

Pssst—Trend Micro and Snyk are partnering to release a new Trend Micro Cloud One™ solution that will address open source package vulnerabilities lurking in your code source repository (such as GitHub, GitLab and Atlassian). Stay tuned.

[CSOO_Application_Security_210310US]

TREND MICRO™