MANAGING THE EFFECTS OF IT SECURITY PRACTICES ON APPLICATION PERFORMANCE

THOUGHT LEADERSHIP

Challenge

Minimize aplication performance effects by security-led changes

Products

Eagle-i

Business Summary

System and Application Security continues to rank as one of the top concerns for IT leaders. The implementation of updates or patches that can eliminate a threat must therefore be prioritized. However, businesses must ensure that they can measure the performance impact of updates on an application and how the end user experience is affected. Remasys' Eagle-i monitoring service offers a unique solution to this issue, with an agentless monitoring approach that is not impacted by security patches, providing a consistent benchmark for application performance before and after.

Intro

A single data breach or high-profile incident can erode public trust in a business, making cybersecurity a leading, persistent concern. CIOs and IT leaders increasingly look to mitigate the business risks arising from the ever-growing reliance of enterprises on IT systems and infrastructure.

The increasing number of security protocols and patches encountered by businesses are often rushed through to reduce risk. Unfortunately, consideration of the ways in which change affects system performance and availability are often measured after implementation. Although businesses must ensure security is a top priority, they must also consider how security-led changes, patches and updates affect application performance. This basic requirement necessitates appropriate monitoring tools to be in place.

Maintaining optimum balance between security levels and monitoring insight

When new threats are identified, such as the recent Spectre & Meltdown vulnerabilities, initial actions are correctly concentrated on how to eliminate the threat and maintain systems integrity. Patches are designed and installed to mitigate risks, before considering the effect on the end user. In the case of non-urgent security upgrades, trade-offs can be analysed and balanced before taking action. However, businesses often lack the tools to measure the end user impact of such changes.

In addition, most application performance monitoring tools require the insertion of a code agent inside internal business systems and applications. For many security teams, the resulting threat scenario is unacceptable. These agents can also prove troublesome when managing patches, as the effect of changes on the agent could trigger a loss of monitoring insight. This creates additional complexity for IT teams managing change.

Security, of course, is a crucial factor for any business. However, a loss of focus on end user experience – with resulting key application failure – can be equally as damaging as a security breach. IT teams need a tool that enables them to quickly understand and measure the performance impact of security measures, without adding additional vulnerabilities or configuration changes. This will lead to reduced workload, boosted efficiency and preservation of the valuable insights obtained from monitoring.

Solution

Businesses looking to measure application performance before, during and after security patch implementations require a unique approach. Remasys' eaglei monitoring service uses synthetic monitoring to proactively test key user journeys, using automated scripts that engage with a platform as a user would. This approach removes the need for configuration changes due to back-end updates. To isolate the effect of security patches, eaglei is designed to measure performance from a consistent benchmark, evading misleading results that can be caused by external factors such as network strength or device issues. In addition, unlike other monitoring solutions, eaglei is technology agnostic, and does not require the insertion of code agents, which can create a security risk to businesses.

Remasys' monitoring experts work with businesses to understand their critical user journeys before automating these journeys using eaglei. These journeys are then run 24/7 at scheduled intervals, collecting vital performance and availability metrics that are of high value to businesses. This active monitoring approach also means that issues can potentially be identified before they affect the end user, giving support teams valuable time to resolve issues before impact. In addition, EAGLE-i records a video of the user journey to provide a visual record to support analysis.

Rapid, Secure Deployment process

Eaglei's agentless methodology requires no code integration into core applications. Set up of a typical Eagle-i monitoring involves:

- Automation of selected end-user journeys that utilise core organisational applications, such as accessing ERP applications
- Completion of testing 24/7 at 5 minute intervals, monitoring performance and availability of systems
- Results are delivered in a centralised, web-based GUI
- Managed Service

About Us

Remasys develop and deliver software solutions that enable our customers to achieve success. Over two decades, Remasys has supported businesses in achieving their goals with our unique capabilities, all delivered by our expert Melbourne team as a managed service. Customers utilising Remasys solutions receive true operational flexibility, as our agentless systems architecture imposes no changes to a managed IT environment. At Remasys we understand that success is built on confidence in your systems – be sure.

Contact Us

Level 8, 278 Collins Street, Melbourne VIC 3000, Tel. (03) 9804 4100, info@remasys.com

Remasys
Be sure