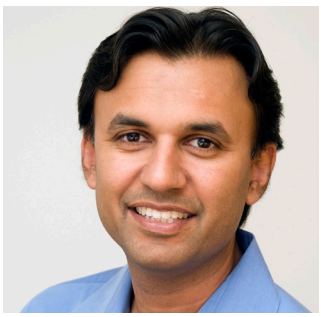
SolarWinds on Continuous Monitoring



Sanjay Castelino, VP and Market Leader, SolarWinds

Continuous monitoring is recognized as a powerful tool for identifying and mitigating potential threats to an agency's infrastructure. But that's just one aspect of its value, says Sanjay Castelino, vice president and market leader at SolarWinds. Continuous monitoring also can provide information technology professionals with invaluable insight into the health of that infrastructure. It's all about dual use.

Q What is continuous monitoring and why is it important? How is it different from the "checklist compliance" approach originally required by FISMA?

A Continuous monitoring is the ability to automatically collect data and report on the performance, availability and security posture of your IT infrastructure and applications.

The "checklist compliance" approach originally required by FISMA looks at risk and compliance at the time of implementation or audit. Reporting on a quarterly or monthly schedule is no longer adequate, driving FISMA's additional requirement of "automated and continuous monitoring." The consequences of a successful cyberattack can be catastrophic and a vulnerability that becomes apparent only in a monthly report could have already been exploited.

The need for continuous monitoring comes from an increase in both old and new security threats and from the constant – but necessary - change of IT infrastructure.

Q What are the essential components of a continuous monitoring solution – and to what extent can agencies tailor a solution to their specific environment?

A Several things are essential in an agency's continuous monitoring solution, including how often it monitors (hourly, weekly, daily, etc.), what it monitors, how often the automated checks are updated and how often someone looks at the data to initiate a response, track the response activities and validate that the issues are fixed. A solution of course needs to run continuously, results need to be stored for analysis and trending, and alerts need to be generated with appropriate priority for critical items. As part of its solution, an agency also needs a process to ensure that alerts are reviewed and that appropriate actions are taken.

Agencies must be able to tailor a solution to their specific environment. IT infrastructure and missions vary from agency to agency and are constantly changing. The implementation of security controls will vary according to an agency's IT environment, its mission criticality, as well as the varying criticality of each application and its data. And each agency might need to mitigate vulnerabilities in different ways depending on their implementation and infrastructure. If the solution cannot be tailored, problems

can occur. For example, an agency might be running a legacy application for which source code access is outside their control and so special firewall rules might need to be configured to avoid constant alerts for something that is a known and accepted vulnerability. The same vulnerability could be mitigated different ways in different environments depending on who is doing the mitigation at the agency.

Finally, agencies should move away from having separate network operations and security operations centers and instead have an integrated network and security operations center.

Q How does continuous monitoring fit into an agency's larger cybersecurity strategy?

A First, we need to understand that the functions of IT operations and information security, which traditionally have been seen as separate, are no longer different at all. The health of networks and systems and the security of networks and systems are now one and the same concern.

Continuous monitoring has been almost universally adopted by IT operations teams for years to identify problems and to "keep the lights on." Now that Information Assurance (IA) is rapidly adopting continuous monitoring to help achieve their goal of protecting the same IT infrastructure from intrusions and other exploitations they are seeing the same need. For both groups, weekly or monthly reports are great for trending and analysis, but real-time continuous monitoring for known vulnerabilities and known attack patterns is critical for keeping ahead of threats.

Because of the significant overlap between what information IT operational professionals and information security professionals need to track for continuous monitoring, it makes sense to look at combining some of these monitoring functions, adopting continuous monitoring tools that can provide value to both groups at the same time. It's all about dual use.

Dual use means that the same raw technical data that is gathered can provide both an ops view and an IA view. "Monitor once, report many" is the new way to cost effectively implement continuous monitoring. Getting dual-use value out of continuous monitoring tools should be part of every agency's cybersecurity strategy.

Q Given the shrinking budgets that agencies now face, what is the business case for investing in a comprehensive continuous monitoring solution?

A The short answer is "dual use." Best practices for IT management in the federal market today involve continuously monitoring the IT infrastructure, then generating different views of the data based on different needs. The IT operations team is looking at the data for insights into performance, availability and reliability, while the cybersecurity team is looking at the data for information on security, compliance and vulnerability. The best way to build a business case for investing in a comprehensive solution is to find tools that can produce both. Not only will the agency save money, by purchasing one tool instead of two, but it will provide operational efficiencies, as both teams will be working from the same data. In summary: Collect once, report many.

One of the most significant unplanned costs of implementing IT tools is the ongoing labor costs of keeping them operationally relevant in a constantly changing IT infrastructure. If IA can leverage tools that ops is already maintaining for its own benefit, then IA can save significant operational costs in keeping the tool configured to monitor the changing IT infrastructure. And of course, IT management tools that are easier to keep up to date in today's changing IT environments provide significant operational cost savings.

I also recommend that agencies look for affordable solutions that they can try before purchasing and that are easy to use, which can significantly reduce training costs. By using tools that "collect once, report many," and that can be tried out at no cost, agencies can put together a solid business case that documents both cost savings and resource savings and a low risk of failure. Try before you buy, and see just how different tools work in your environment.

Q When it comes to aggregating and analyzing security data, how do agencies strike the right balance between being

comprehensive and not getting overwhelmed?

A I rarely hear complaints from staff that they are monitoring "too much" data. The complaints are more about "too many reports" being sent to too many people and becoming noise. "Too many reports" complaints generally come from not tailoring reports and views to the different roles that people have. Collecting lots of data is valuable to the IT professionals who need access to lots of data for their jobs.

To be comprehensive without overwhelming staff it's essential to select tools that can collect all the necessary information but display different views to different people with easy to set up role-based reports, dashboards and alerts. The right tools can be set up to collect once, report many – and deliver the right reports and alerts to the right person, with links to additional details provided.

Selecting tools that are easy to use and require very little training is also essential to striking this balance and to avoid overwhelming staff with in depth training.

Q Given the on-going evolution of the federal IT enterprise, how can agencies ensure that their continuous monitoring plan keeps pace?

A Again, the best way for your continuous monitoring plan to keep pace with the ever-changing IT infrastructure is to select and implement dual-use tools that provide value to both ops and IA. The labor saved by operating a single tool instead of two can be leveraged to produce more customized role-based reports, keep the vulnerability detections updated, customize data collection as needed for your specific infrastructure and establish a remediation workflow. By providing useful and timely detection of vulnerabilities and having a process to drive them to remediation, your continuous monitoring technologies will become a vital part of the IT operations process. And frankly, that is the goal: to make information assurance just another part of the routine IT operations process, which will enable you to ensure your plan keeps pace as well.

Q In what ways does continuous monitoring support a risk management approach to cybersecurity? And how can a risk management approach shape a continuous monitoring strategy?

A Continuous monitoring is an essential component of a risk management approach to cybersecurity in two ways. First, new threats are constantly being discovered and what is 100 percent covered today might not be covered tomorrow. Understanding your current risk is critical. By continuously monitoring your infrastructure for known vulnerabilities you are able to detect new vulnerabilities quickly and find a way to mitigate them and keep up with this new, rapid pace of constant cyberattacks.

Second, no IT system is ever left unchanged. As users and IT operations make changes they can inadvertently or deliberately expose well-known vulnerabilities that had been previously patched, fixed or mitigated. With continuous monitoring you can uncover these issues quickly.

Risk management has an additional set of requirements beyond those covered by continuous monitoring strategy to consider–to report on security issues when they happen so they can be immediately addressed. The continuous monitoring tools ideally need to address more than just operational concerns, but also some amount of risk management and vulnerability detection. And the requirements of risk management should be factored into continuous monitoring process development and tool selection.

Q What are some common pitfalls that agencies should look out for when developing their continuous monitoring strategy?

A Hidden operations costs are probably the biggest. Operations costs are higher for tools that can't provide dual-use functionality because you will need to implement two tools to collect the same raw data. Another hidden operations cost is that some tools are just plain "expert friendly," which is a nice term for "complicated to maintain and operate." The expert friendly tools are ones that can only be implemented and operated by a very senior IT professional and that cannot be successfully maintained in the constantly changing IT infrastructure of today's agencies.

Another common pitfall is IA expecting the operations team to maintain and operate tools that are single purpose. If ops receives no direct benefit from

the tool, they're less likely to maintain it properly. In complex, ever-changing infrastructures, tools that seemed like good ideas on paper fail all the time for the simple reason that they are too complex to keep operationally relevant.

For that reason, the best security solutions are not those that create additional steps and limits on IT operations, but those that make their jobs easier. The best solutions are those that are useful to the operations team and enhance security at the same time.

For example, a log management tool designed to alert on operations issues, such as application errors, could also provide alerts that possible security threats, such as malware, might be the cause. Tools pushed from one team to another, or pushed down from above, often don't become a part of the daily workflow as easily as those that both streamline daily operations and enhance security.

Dual-use tools that benefit both priorities will win advocates from the bottom of the organization on up, as employees use the things that make them more productive. When continuous monitoring is built into your solutions — and when those solutions are easy to use and make everyone's job easier — security and performance are not conflicting goals.

Q A high-ranking federal official once argued that even with continuous monitoring, "total" security was impossible. What are the practical limitations of the continuous monitoring approach? And how can agencies address those limitations?

A The only totally secure system is one that is turned off, disconnected from the network and physically protected from tampering. If systems are to be useful, some risk has to be accepted.

Continuous monitoring success depends on multiple success criteria. One is that identified vulnerabilities must be continuously updated. But even with constant updating, there are still zero-day threats out there that have not been identified yet.

Incomplete coverage of the IT infrastructure is another risk. Rogue devices can introduce tremendous risk. For example, there might be a closet that has several servers running in it that operations was not aware of, so they are not being monitored. Or perhaps someone put the servers behind a firewall that hides their IP addresses so they were never discovered.

Using tools that automatically identify rogue devices and that do automatic discovery of what is on the network help agencies understand the ever-changing infrastructure they have. Keeping up to date with the latest known vulnerabilities, and configuring your tools to identify them, is a never ending battle, but must be done to keep your continuous monitoring tools relevant and useful.

Q To what extent can continuous monitoring help agencies go beyond simply responding to problems and actually help them anticipate and mitigate future threats?

A Ops has leveraged continuous monitoring tools for years to help them proactively identify problems before they impact users. IA can leverage the significant experience and investment that ops typically has in monitoring by identifying dual-use capabilities and using them appropriately to be proactive. When IA is able to identify vulnerabilities on a daily basis through continuous monitoring, they can prioritize the problems and drive resolution on the most important issues, as well as detect and mitigate critical vulnerabilities much earlier.

Additionally, IT operations needs to maintain an accurate and up-to-date change management system for optimal efficiency and to make it possible to revert easily to prior configurations when necessary. If information security isn't part of that process, evaluating each change for its impact on security posture, new vulnerabilities can go undetected.

Dual-use tools that collect information for both performance and security needs eliminate the potential for communications errors, and speeds network threat detection. •