As the cyber threat landscape evolves, security methods and tools need to change, too. Gone are the days of defining an information technology system by identifying its boundaries and drawing a fence around it, said Ken Durbin, manager of the Continuous Monitoring Practice at Symantec Corp., during a June 10 webcast titled “Continuous Monitoring: Elevating Cybersecurity in State and Local Government.”

“Mobile devices and the cloud itself are making it a lot harder to define what the boundary of a particular IT system, so then how am I supposed to protect that?” Durbin said. “We should be moving away from checkbox compliance and actually using appliance mandates to actually improve your cybersecurity posture.”

To that end, continuous monitoring is a positive step. A continuous monitoring solution involves deploying sensors to parts of your infrastructure that send status data back so information technology managers can spot suspicious activity.

Symantec’s products go a step further, however, by aggregating the collected data and making it useful.

Parallel transformations
Symantec has been transforming itself in line with what’s happening in cybersecurity at large. Traditionally the company has developed and acquired state-of-the-art products. Over time, the need has arisen to integrate individual products using key functions. As a result, Symantec now focuses on two major areas: security, through its Unified Security Ecosystem, and information management, through Unified Information Management.

“If you look at the federal government and what they’re doing with continuous diagnostics and mitigation, it’s very much an attempt to break down the silos between the

NIST’s Cybersecurity Framework, released in February, aims to help organizations improve or start cybersecurity efforts. It breaks down cybersecurity into five areas—identify, protect, detect, respond and recover—with subcategories and a list of the controls that apply to them. For example, if your agency is NIST 800-53-compliant, managers can see in the Informative Resources section the controls that satisfy that for a given category.

“The goal was—and they achieved this goal—they didn’t want to create a single new control as part of the Cybersecurity Framework,” said Ken Durbin, manager of the Continuous Monitoring Practice at Symantec Corp. “Because of that, it’s a tool that truly helps organizations.”

Symantec’s solution includes the framework in its controls library for additional ease of use and as a way for organizations to see how they’re stacking up against the guidelines.

“We’ve also indicated where we don’t have a framework that fits that individual framework control,” Durbin added.

If all continuous monitoring means to you is deploying sensors to eliminate top causes of suspicious activity, you’re on the right track, he said. But to really stay ahead of threats in an ever-evolving environment and be ready to respond to breaches, Symantec’s aggregation layer is a differentiator to consider.”

LISTEN/LEARN:
For a replay of the webcast, go to: GCN.com/2014ContinuousMonitoring
organization that they’re all concerned about … and taking that information and marrying it with information from another silo, like asset management, so that if you integrate that data, you get a better view of what’s going on in your IT system, better situational awareness, and it allows you to take action on what you’re seeing,” Durbin said.

Symantec also added user productivity and protection to the technology because if users aren’t productive and protected, it will be hard to accomplish the other two goals, he added.

The new offerings in the user productivity and protection segment incorporate Norton 360, Mobile Security and Data Services; endpoint protection and encryption; enterprise mobility; and user authentication.

Under information security, it provides managed security services by monitoring the logs of a multitude of companies and entities to alert them to potential events. Also part of this is the Control Compliance Suite, products that capture data from the sensor network and use it to show compliance or initiate action on noncompliant pieces. This focus area also addresses insider threats through, for instance, data-loss prevention, and critical system protection by locking down the system and hardening it so managers know what it can and can’t do.

“When people think of continuous monitoring and cybersecurity, I think most of the press goes to information security, and I think that’s kind of a misplaced belief because we all know that it’s a matter of when, not if, that a security event is going to take place,” Durbin said. “If we believe that that’s the case, then we need to be prepared to recover from that event.”

That’s where information management comes in. It involves storage to keep access to data highly available. It uses Symantec NetBackup, Backup Exec and Enterprise Vault, which archives data off the system but still allows access to it.

“The secret sauce, if you will, to Symantec is what we call our threat intelligence or our global information network,” Durbin said. The company monitors 13.8 billion files, 21.3 billion URLs data from sensors worldwide. Its products work with Symantec sensors and those from other manufacturers as well.

“We are gathering an unsurpassed amount of unique threat intelligence,” he said. “Nobody has access to the same threat intelligence Symantec has because it’s our data coming from our sensors in our networks. This information is culled together and analyzed by very smart people on our team and others to develop patterns and to be able to feed and fuel and inform our other Symantec products.”

‘Scan Once, Assess Many’

A 2011 mandate related to the Federal Information Security Management Act of 2002 requires all federal agencies to perform continuous monitoring, but continuous monitoring is not happening only at the federal level. Many states have adopted the National Institute of Standards and Technology 800-53 risk level in addition to risk management framework processes, law enforcement monitors to FBI’s Criminal Justice Information Services, health monitors to the Health Insurance Portability and Accountability Act, and retailers monitor to PCI.

To further clutter compliance, entities could be monitoring according to multiple standards. For instance, a government agency that does transactions by credit cards could also be using PCI. Symantec’s solution includes the Control Compliance suite, which is mapped to all of these standards so that sensor-collected data can be automatically checked against them.

“We have a process we like to call ‘Scan Once, Assess Many’ especially in environments like the states where they do have multiple frameworks and multiple control sets that they have to comply and report against,” Durbin said.

“We should be moving away from checkbox compliance.”
— Ken Durbin, manager of the Continuous Monitoring Practice at Symantec