Enhancing Security While Achieving Unparalleled Application Performance

An interview with Peter Graupp, Solutions Engineering Manager at Riverbed, and Ken Bradley, Senior Solutions Engineer at Merlin International

Agencies continue to rapidly implement new security monitoring tools with the goal of identifying actions impacting security within each layer of their environment. This growth of management and monitoring tools has negatively impacted systems and application performance due to the additional overhead placed on the network.

Is this plethora of tools really meeting the agency goals of protecting these critical assets while meeting service level agreement guidelines around application performance? According to Peter Graupp from Riverbed, a leader in application performance infrastructure and Ken Bradley from Merlin International, an information technology solutions provider, the answer is not always.

In many cases, agencies are overprotecting some resources, to the detriment of more critical assets' security and performance. "Would you place the same level of value on the assets of Fort Knox that you would your refrigerator? Probably not," said Bradley. "Instead, fit a security posture around your known assets. The value of these assets should dictate what security position to deploy and what policies should be defined based on the amount of risk the organization is willing to assume with each asset."

Graupp said it's critical for agencies to identify individual applications and evaluate them within the larger network context. "It's imperative to understand the application," he said. "Is it available? Is it the network performance that's impacting it? How is the application performing, versus the server response times, the peak loads, the latency, and the metrics?"

Unfortunately, many agencies lack true visibility into their network and the applications that perform within it. That has negative impacts on performance, but also security. "The application layer continues to hamper ITs ability to identify and proactively prevent threats," Bradley said.

Without a clear view of the application landscape, it's nearly impossible for security personnel to pinpoint potential security and performance vulnerabilities. Instead, they require end-to-end visibility for all applications across an organization's network and insight into metrics and forensic data.

"Riverbed's SteelCentral solutions can identify what systems are on the network, who is talking to whom, over what ports or protocols and where the traffic is flowing are key to having full visibility over one's network," Graupp explained.

This end-to-end approach also has an added benefit for government organizations. "Not only is this kind of visibility into the network beneficial for understanding what needs to be secure and protected, but it is also a common platform across most information security regulatory requirements," Bradley said.

But how does an agency achieve this end-to-end visibility of its applications and network? According to Graupp and Bradley, the key is consolidating the points of risk. That's easier said than done in a time when most agencies are expanding their networks to accommodate remote employees and virtualized work environments. However, some solutions can centralize the view of an agency's network, even as the network expands.

"Solutions like Riverbed's SteelFusion enables agencies to centralize data back into the data center, consolidating and securing that data allowing policy to be enforced in the data center where it has a containerized view from a centralized point of control," Graupp said. That data can provide a full view of the agency's applications, where they reside on the network, and how they're performing.

Additionally, this strategy insures integrity of intellectual property, mission continuity and it provides for recovery after interruptions and disasters. Even in places where it's safe to maintain local copies of data, branches and remote offices generally lack the continuous protection mechanisms typically employed by data centers to safeguard data from risks and provide non-stop data access and availability.

This consolidated data strategy offers operationally feasible ways to get the data out of the branch and into a more secure setting, even while employees use applications onsite. "Collapsing all data back to the central datacenter provides an immediate improvement in an organization's security posture and enables staff to dedicate their limited resources to fewer locations," Graupp said.

"What we are advocating is a strategy that enables organizations to drive workflows into daily operation, automatically mapping their networks so they can manage change, track compliance, conduct robust survivability analysis, and execute threat modeling for common attacks," Bradley continued. "This, along with the ability to provide immediate reporting, provide management and IT personnel insight into situational awareness across the enterprise."

Agencies are looking for technology platforms and strategies that offer the ability to deliver services in a repeatable and predictable manner. In order to achieve that goal, data and applications have to be available for the disparate number of platforms and environments, without sacrificing performance or security. That requires an end-to-end understanding of your network, as well as the applications living within it.