APAC Police Force Turns to Radware to Safeguard Sensitive Law Enforcement Data in New Data Center

THE CHALLENGES

Design a new data center that incorporated a segmented network infrastructure, so a cyberattack on one department wouldn't compromise the data of other departments.

THE SOLUTION

The law enforcement agency implemented Radware's application delivery controller (ADC), Alteon, and its web application firewall (WAF), AppWall®. To manage the ADC/WAF services and monitor application service-level agreements (SLAs), it implemented APSolute Vision.

WHY RADWARE

Radware's virtualized ADC/WAF solution guaranteed that each department would receive its own security policy for the set of applications it protects.

BENEFITS

The virtualized solution increased network flexibility and lowered the total cost of ownership (TCO) of the new data center by avoiding the implementation of a complex physical network infrastructure.

This national police department employs approximately 230,000 officers, roughly 17% of all civil servants within this APAC country. Since officer cadets are required to graduate from an armed forces preparatory school, this department is considered to be part of the military.

THE CHALLENGES

This national law enforcement agency needed to construct a new data center that potentially required a very complex network infrastructure design based on the agency's security needs. The network design was complex because the organization's security policy required separate subsegments for each of its five departments, so a cyberattack on one department's data would not compromise the data of another department. This complexity would have made it difficult for the agency's IT team to manage and update the various subsegments with its current resources.

The agency managed confidential data from an array of other law enforcement organizations, including narcotics, immigration and criminal justice. The agency was also concerned about the security and availability of its website and applications, including its database, from downloads and video streaming.

THE SOLUTION

To meet the customer's requirement of separate subsegments and avoid the cost of building a segmented network infrastructure, Radware proposed segregation of each department's applications by virtualizing its ADC and WAF functions.

Each department would have its own virtual ADC reserved with its own dedicated resources, including its own network interfaces, CPU and network capacity, and SSL encryption. Each virtual ADC would also get its own WAF instance with separated WAF resources (e.g., CPU power, memory, etc.) to ensure predictable performance of the WAF and ADC functions. By allocating a dedicated WAF instance per department, each department would receive its own security policy for the set of applications it protects — a key consideration when managing complex security policies for multiple applications.

Although F5, the incumbent ADC provider, recommended a similar solution, it couldn't ensure the availability of its ADC and WAF services. F5 could not guarantee that its virtual ADC and WAF, or each function, would have the necessary resources to provide proper operation with minimal latency.

The agency implemented Radware's ADC, Alteon, and its WAF, AppWall. To manage the life cycles of ADC and WAF services per department, Radware proposed two management and monitoring solutions, APSolute Vision and Operator Toolbox (OTB), to provide SLA monitoring of applications and automation of the launching and maintenance of the ADC services.

BENEFITS

- A virtualized solution that increased flexibility and lowered the TCO of the new data center by avoiding the implementation of a complex physical network infrastructure
- Ability to scale delivery services without the need to add licenses or swap hardware
- Virtual segregation between departments so sensitive law enforcement data is not breached if one department is cyberattacked
- An integrated WAF that provides bot management capabilities and device fingerprinting to block Dynamic IP attacks, protecting Layers 3–7
- No added latency or single points of failure
- Support of dynamic, real-life requirements with varying application capacity prerequisites