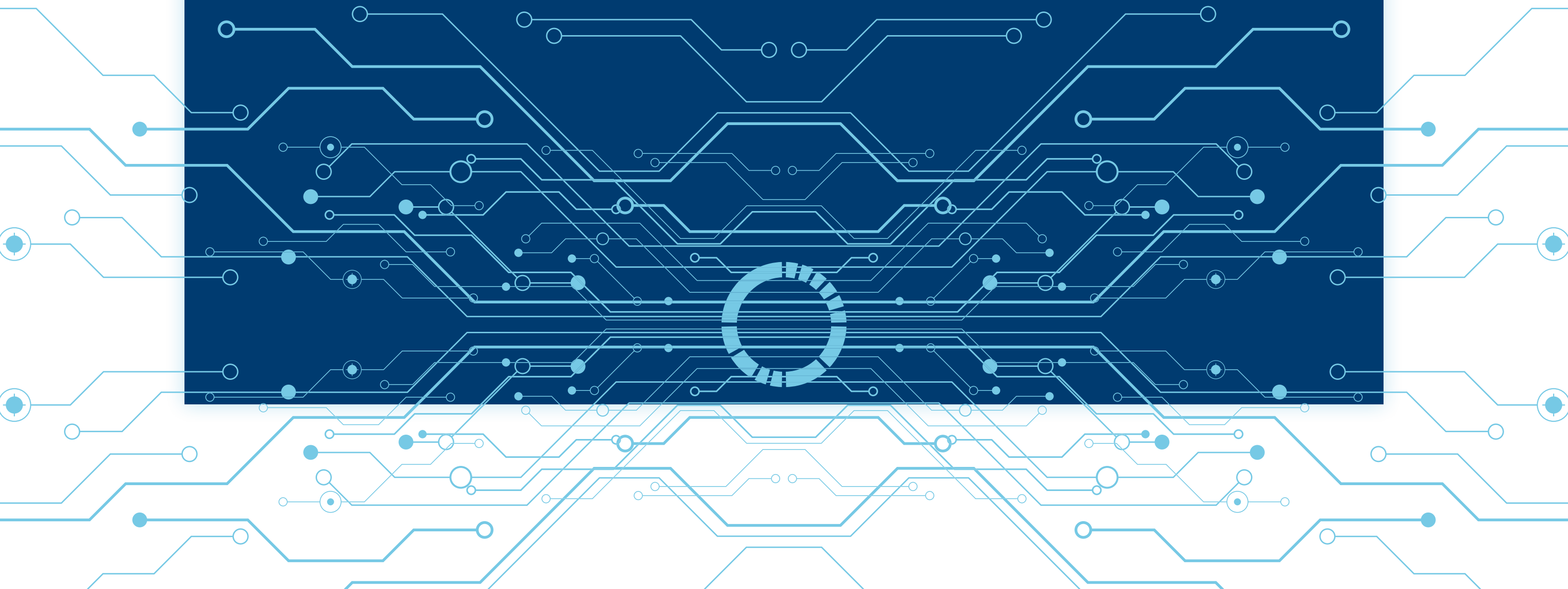
GTA

Georgia Technology Authority

NASCIO 2015 State IT Recognition Awards

Title:	State of Georgia Private Security Cloud Implementation
Category:	Cybersecurity
Contact:	Mr. Calvin Rhodes CIO, State of Georgia Executive Director, GTA calvin.rhodes@gta.ga.gov 404.463.2340
State:	Georgia
Project Initiation Date:	March 2011
Project Completion Date:	July 2014



EXECUTIVE SUMMARY

The Georgia Technology Authority (GTA) and its network security partner, AT&T, completed a three-year program in 2014 to move most of its local firewalls and network security services to a centralized Private Security Cloud platform. The program successfully transitioned more than 800 local firewalls at agency locations to create a centralized solution, which significantly enhanced the state's security posture. This new platform will also enhance security services that can be provided on premise by including such features as virtual firewall, intrusion prevention, distributed denial of service defense, web-based malware protection, application analysis, network encryption, forensics and URL filtering services. It would have been exponentially more expensive to replicate this functionality at each site with local firewalls and security devices throughout the network. Georgia's state government is also benefiting from using the best-in-breed security tools, and executing better security processes that quickly help address malicious attacks against the state's network.

Centralizing these network security services has saved the state of Georgia millions of dollars in equipment, maintenance and management costs, and has greatly enhanced the security and business continuity posture of Georgia's state government. The solution provided a platform that reduced the footprint of appliances in the network, which in turn reduced the complexity of the network. Lastly, the Private Security Cloud is a focal point in the network, which is continuously augmented and upgraded over time to keep ahead of increasing security threats.

> The program successfully transitioned more than 800 local firewalls at agency locations to create a centralized solution.

BUSINESS PROBLEM AND SOLUTION DESCRIPTION

Fifteen of Georgia's state executive branch agencies previously managed their own network security infrastructure, policies and processes. Personnel at the agency level did their best to keep pace with the increasingly complex security environment, but agencies found it hard to hire and retain skilled security personnel. Firewalls and other network security technologies became out-of-date, and the implementation of security technology became less effective over time. In addition, troubleshooting network connectivity issues and security events required multiple agency and vendor personnel to review device logs and remediate problems.

Another problem becoming more prevalent in government networks is providing secure connectivity to cloud computing and software-as-a-service vendors who support state agencies. Agencies are now much more reliant on the public Internet for software-as-a-service and cloud computing environments. GTA contracted with AT&T to drive the implementation of the Private Security Cloud to address many of these issues.

The Private Security Cloud service was built by GTA and AT&T as a way to better serve the security needs of state agencies as they move more services to the cloud. AT&T teams began moving Internet traffic out of the state's data center (the primary hub location) and closer to the Internet cloud for agency locations. The result is a reduction in latency to access resources, and a central location for enforcement of security policy, network encryption mechanisms and application analysis.

The Private Security Cloud provides:

- A central point for business partners to connect to the state network.
- A perimeter security platform between business partners and state agencies.
- Network encryption capabilities, to ensure communications traversing public networks are further secured to agency locations, where necessary.

The new Private Security Cloud also provides virtual firewall and intrusion prevention, which allows each agency to employ custom policies on a common platform. The improvements include:

- Policy management, event management and logging and reporting are centralized in one location.
- Firewall changes are performed by a centralized group of highly skilled security analysts, who ensure best practices and standards are followed.
- Change management and incident management are simplified, since fewer firewall devices are in the path of traffic and applications are allowed to flow properly throughout the network.
- Security changes now go through standards-based processes to ensure they are reviewed, vetted and approved before implementation.

By consolidating firewall platforms and centralizing policy management, a new set of capabilities is available for functions such as firewall policy tuning, geographic protection and global policy enforcement across multiple virtual firewalls. As part of the effort to consolidate firewalls, AT&T performed a highly structured analysis of the existing firewall policy to standardize configuration, remove unused firewall procedures and implement security best practices within the updated policy. Firewall tuning software was deployed to assess firewall policies within the centralized Private Security Cloud platform to help automate remediation efforts.

Successful Solutions To Real Life Threats

Defense against Denial of Service Attacks

Georgia's state network came under a distributed denial of service attack on December 7, 2012, which prevented thousands of agency users from accessing the Internet. Agency users could not load Internet-based websites, and constituents could not enter state government websites. GTA quickly gained access inside the Private Security Cloud environment to identify a large volume of domain name service (DNS) server traffic overrunning the state's ability to resolve website addresses. GTA and AT&T implemented an emergency distributed denial of service defense that re-routed the attack through network "scrubbers" and eliminated a majority of the attack traffic. The attackers eventually stopped and the event was mitigated. The distributed denial of service defense is now an integral, permanent part of the Private Security Cloud solution for the state of Georgia.

Exploits of Vulnerable Systems

New exploits commandeering the Internet have tested the capabilities of the Private Security Cloud. Two examples include the recent "Shellshock" set of security bugs and an Internet Explorer vulnerability that could allow remote code to be executed on users' computers. In both cases, GTA worked with AT&T to implement newly released intrusion prevention signature files within the Private Security Cloud platform to block this activity to and from Georgia's state network. The intrusion prevention tools proactively blocked the attacks and greatly reduced exposure to these vulnerabilities. The quick application of the proactive blocking capabilities greatly reduced the risk of information being stolen from state agencies and services being degraded for constituents needing to access state websites.

Overseas Threats and Global Policy

The centralized Private Security Cloud platform greatly reduces the complexity of pushing policy across all firewalls simultaneously, with one click of a button. In the past, keeping up with concerns—like geographic protection against embargoed countries that were hacking into government systems—was very difficult to implement and maintain. Now that the policy is centralized, GTA can have a global policy pushed across all the unique state agency virtual firewalls to block very specific attack vectors. For example, using AT&T's capabilities, the state recently blocked traffic from embargoed countries—which should have no business dealings with the U.S.—trying to enter Georgia's network.

SIGNIFICANCE

Georgia’s state government operations benefit from the Private Security Cloud platform in terms of reduced costs, due to a smaller footprint of remote security devices, enhanced security from better tools and personnel, and faster restoral times for application issues using centralized platforms. In addition, Georgia state agencies have strengthened business continuity by moving the security perimeter out of a single, centralized data center to dual, geographically redundant security cloud nodes. The agencies now also have access to skilled security personnel at AT&T to help drive best practices and address security events as they arise. Furthermore, the reduction in firewall devices has greatly improved restoral times and implementation timeframes for new applications.

Security is an ever-evolving and rapidly changing concern that government entities need to constantly enhance to keep up with attackers. The Private Security Cloud is a beachhead for the state to allow more rapid deployment of security tools and connectivity to the cloud. The Private Security Cloud provides a central location to augment security as the threat increases over time. Additionally, the Private Security Cloud platform provides a secure, central hub for cloud connections from state agency networks to cloud providers. The platform offers a central connection point and a security perimeter to help ensure traffic coming from external service providers will not compromise state agency systems.

BENEFITS OF THE PROJECT

The centralization and consolidation of information technology is a difficult and lengthy endeavor for all entities involved. GTA drove disparate state agencies to embrace centralization of network security, which is crucial to state operations, and ultimately its reputation to constituents. Implementing security solutions for government entities helps build confidence in utilizing government services. Management teams in state agencies gain greater confidence that their services will not be compromised, due to the enhanced security posture the Private Security Cloud provides.