



United States Government

A top Systems Integrator manages endpoint security for this U.S. Government department using Bit9 Parity Application Whitelisting



Summary

This agency maintains the highest standards for ensuring the safety, soundness and security of its U.S. and international systems. The agency serves the American people and strengthens national security. Its mission is to manage the U.S. Government's finances effectively, promoting economic growth and stability, and ensuring the safety, soundness, and security of the U.S. and international financial systems. Within this agency, a communications systems group maintains the private data network infrastructure and all of its bureaus. As a high-profile division of the United States government, this agency not only handles extremely sensitive information, it is a target for malicious attacks. As the manager of system security for multiple department bureaus, their Systems Integrator needed a new level of security to prevent unknown and targeted malicious attacks for which no antivirus signatures exist. To reduce risk and demonstrate compliance, they also needed a way to control unauthorized applications—whether they were malicious or not—from running on the governments' critical machines. The contractor chose Bit9 Parity Application Whitelisting to prevent any unauthorized applications from executing on the department's critical systems.

INDUSTRY

Government

ENVIRONMENT

Endpoints in highly targeted bureaus of a major U.S. government department

BUSINESS CHALLENGE

Protect the systems that run applications and maintain data for department bureaus

SOLUTION

Bit9 Parity™

BENEFITS

- Allows IT staff to monitor and control all software running on system endpoints
- Blocks viruses and malware for which no antivirus signature exists before they breach network systems
- Prevents zero-day and targeted attacks
- Reduced time and money spent on technical support by controlling applications

The Challenge

The department's system group enables the many applications that assist in carrying out department functions. As the manager of this large private, wide-area network, the Systems Integrator needed to reduce the likelihood of unauthorized software getting onto department systems—whether by download or USB device. They needed the ability to halt introduction and propagation of any unauthorized software before it could execute and spread across the network. The integrator was concerned that the “blacklisting” solution provided by their existing endpoint security vendor was stopping only 50% of threats and that significant cleanup after breaches were occurring. While the existing solution prevented known attacks from executing on the systems, it was not preventing the unknown attacks for which no antivirus signature existed.

The security of these bureaus is paramount, as they are responsible for important highly sensitive data and functional applications for agencies that serve the United States public, and are essentially the first line of defense between the department and the outside world. The integrator realized that they needed to implement another level of security and control to allow only authorized software to run on the department's network.

The Solution

After testing and evaluating Bit9 Parity Application Whitelisting, the integrator deployed Bit9 Parity on the departments' systems. They gained greater visibility into all the applications that were running on the endpoints (laptops, PCs, servers) in the bureau, as well as definitive control over what approved applications would be allowed to execute. Bit9 Parity was able to identify and stop 100% of unauthorized software during the trial period without interrupting the administrative rights of the teams' 300 technicians and system management experts. The Bit9 Parity whitelisting solution also proved to be flexible, allowing custom applications to run unhindered. Technicians realized a greater level of visibility and control over their endpoints.

Bit9 Parity now allows IT staff to monitor and control all software running on system endpoints, blocking any unauthorized software, whether it is malicious malware or software that is not approved such as Skype or games. The government is able to protect against viruses and malware for which no antivirus signature exists before they can breach network systems, thereby preventing zero-day and targeted attacks.

With Bit9 Parity, the system integrator continues to define the direction and standards of security for this major department of the United States government. The Bit9 solution has made it safer and easier for the IT group to analyze software applications that are introduced to the systems. With Bit9, they can focus their efforts on bettering IT functions within the department without worrying about the ever-developing malware environment targeting and threatening the security of their systems.

