

An Inventory of Authorized and Unauthorized Devices

How Great Bay Software is helping United States Federal organizations address the #1 item in the Consensus Audit Group's list of the 20 Critical Security Controls

Great Bay software's Beacon Endpoint Profiler™ is being deployed by numerous federal agencies to address the FISMA requirement to develop and maintain a comprehensive inventory of all authorized and unauthorized network devices. Beacon's Endpoint Profiling technology allows organizations of all sizes to rapidly, and unobtrusively, gather and maintain this foundational component of modern-day IT security.

Beacon's unique approach to automatically discovering, identifying and monitoring all enterprise endpoints is specifically targeted at providing endpoint identity and in providing numerous attributes such as location, behavior, and addressing, all critical elements in a comprehensive IT security strategy. Beacon's identity based database includes both real-time and historical information, lending itself to troubleshooting and incident response scenarios, and contributing to reducing both mean time to repair and the cost of managing the enterprise network.

Beacon's discovery methods do not employ vulnerability scanning, which can cause undesirable results for network devices not designed to withstand such aggressive discovery techniques. Vulnerability scanners serve an important role in IT security to detect the state of user-based devices and certain operating systems, but the use of a VA tool to discover the identity of devices such as patient care systems, SCADA systems, legacy devices, or purpose built devices like HVAC and door access systems is a mismatch in technology and application. These devices must be discovered using methods that can unearth their function, or role, within the enterprise and not just their Operating System.

Importantly, Beacon can be deployed in either a centralized or distributed way eliminating the need to deploy costly systems to remote sites or distribution layers throughout the network in order to gather the required inventory.

By deploying Great Bay's Beacon Endpoint Profiler, United States Federal organizations will be laying a strong foundation for addressing FISMA's requirements, achieving more efficient incident response, and increasing the overall operational efficiency.

Beacon Endpoint Profiler:

- Automatically discovers and identifies all network attached endpoints
- Frequently deployed to address FISMA requirements for device inventory
- Scalability to support the largest enterprises
- Enables more efficient incident response process
- Serves as an enabling technology for 802.1X and NAC deployments
- Automated new endpoint Discovery and Profiling
- Graceful aging of retired endpoints

Have questions?
Feel free to contact us at:

sales@greatbaysoftware.com

or

support@greatbaysoftware.com

Beacon Endpoint Profiler FAQ:

Q. How is Beacon different than patch management systems such as BigFix or Altiris?

A. The focus of endpoint management products is on managing the fine details of the managed hosts in an environment, whereas Beacon is providing a comprehensive identity-based inventory of all network endpoints. Beacon provides this granular discovery and monitoring of all network endpoints without the use of an agent or a scanner. This discovery is specifically designed to unearth the unique identity of devices such as HVAC systems, VOIP phones, security cameras, WLAN Access points, patient care systems, etc.

Q. How is Beacon different than asset management tools?

A. When compared with an Asset Management system, Beacon provides greater contextual information about the endpoints such as behavior, addressing, and location and also provides a more robust real time view of this information. This real-time view is a function of Beacon's continuous operation, which is in contrast with the comparative or scheduled approach taken by most asset management tools. Beacon does not, however, provide information such as serial number or asset tag, which are commonly provided by an Asset Management system.

Q. How is Beacon different than vulnerability scanners?

A. Beacon does not "scan" networks the way a VA tool does. Instead, Beacon is designed to exclusively gather information about endpoint identity and is generally deployed in more passive configurations. Beacon's database of information provides a wealth of information about the endpoint landscape, but does not report on vulnerabilities on the part of the endpoints like a VA tool would do.

Q. What benefits does Beacon's real-time Identity Monitoring provide?

A. Beacon's continuous and real-time identity monitoring is in contrast with scheduled or comparative systems in that Beacon is continuously in operation and ingesting information about the enterprise endpoints. The constant operation allows contextual attributes about the endpoints to be updated and presented to the user as a real time view of the location, addressing, behavior, and identity of network endpoints.

Q. How is Beacon used for incident response?

A. Beacon's historical data allows the IT security operator to quickly retrieve historical information about an endpoint of interest such as address assignment, location data, and identity assignment. This historical information can be used to align endpoint information in an event coming from a SIEM, Firewall, or IDS/IPS and to accurately track that endpoint given that its address, location, and maybe even assigned identity may have changed since the time of the event.

Q. What are the other applications for Beacon?

A. In addition to its role as an Endpoint Profiling system and a foundational component of 802.1X enabled networks, Beacon is frequently leveraged in numerous IT and IT security applications ranging from day to day tasks such as locating endpoint quickly to contributing to organizations Identity Management initiatives.