



Managing the Endpoint Lifecycle with the Beacon Endpoint Profiler™

Introduction and Background

For several years, enterprises have placed a great deal of focus on securing the perimeter of their networks from external threats in efforts to improve security and availability of the network infrastructure. The features and functionality of network infrastructure and security products, the discipline of network design to include numerous high-availability and improved security measures, as well as advancements in enterprise network management practice have evolved to the point that the network infrastructure itself has become quite reliable, resilient and increasingly secure. For external threats in particular, most enterprises have deployed effective technology and policy measures to protect the enterprise against attacks from outside the bounds of the networks under direct control and management.

For many large enterprises today, several different initiatives are either under consideration or evaluation to address internal threats to network availability posed by and via the devices connecting to the network from within the enterprise. Many enterprises are finding that managing the organization's endpoints across their lifecycle is the next logical step toward realizing continued gains in network reliability and availability. "Endpoint" in this context includes all the devices that connect to the network including user devices such as desktop and laptop computers, as well as the increasingly diverse set of other IP-enabled devices that are using network services. The "endpoint lifecycle" as it used here refers to all phases of the useful life of all network-attached devices, regardless of type or function. It begins when a new endpoint is first connected to the infrastructure and terminates with the retirement of that endpoint.

Throughout the lifecycle of any network endpoint it may be involved in an incident that requires a response from network management, preferably at the access port level. These incidents can range from simple moves and changes, to common troubleshooting scenarios; a user unable to connect to network resources for instance, to security events that require rapid location of an infected, disruptive, improperly configured or non-compliant device so it can be isolated from the network. Large-scale network migrations are yet another example of how endpoint-level visibility can be advantageous. It is highly desirable in these migrations to have a working knowledge of the progress of the migration so that it can be continuously monitored and measured.

Traditionally the field-of-view of enterprise network management has been limited to the network edge, to the devices providing endpoint connectivity and not extended out to the end nodes that are utilizing the network, This "blind spot" of not being able to detect, locate, and track endpoints both in real time and historically significantly adds to the

difficulty and complexity of maintaining the availability and security of the increasingly complex enterprise networks common today.

In recent years a myriad of non-user “IP-enabled” devices ranging from security cameras, badge readers, and facility control systems to medical imaging devices have been added to the network and their functionality dependent on the interconnectivity provided. Often times these devices provide mission-critical services to the enterprise and are dependent upon reliable access to the network infrastructure. With the ubiquity of dynamic endpoint configuration via DHCP and the wide availability of “zero configuration” home networking products, endpoints as well as infrastructure devices such as SOHO switches and access points can be added to the enterprise network with little or no assistance from, or the knowledge of the IT staff. These factors contribute to a growing undocumented endpoint problem for the large enterprise as more, and increasingly disparate devices are added to the network significantly complicating endpoint lifecycle management. It is proving increasingly problematic for the IT staff trying to maintain availability and security of the network infrastructure serving a heterogeneous and ever increasing inventory of endpoints, many of which are providing critical services to the enterprise but are not necessarily IT assets.

The start of any initiative to expand network management into including the endpoint lifecycle is developing an accurate and dynamic inventory of 100% of the endpoints that are attached to the network and then maintaining that inventory over time as new devices are added, and existing devices are moved or retired. This is typically the approach of a number of IT asset inventory and management solutions that are currently in use. However the challenge associated with these solutions is that many of them operate on a “snap shot” basis and most provide limited views or information about the devices connected to the network, their precise location and capabilities and other required contextual information. That is, they utilize technologies and techniques to discover the endpoints connected at a single point in time and provide limited device descriptions and little supporting contextual information particularly for devices other than desktop and laptop computers. Enterprise networks today are constantly changing and evolving however. Endpoints are moved, new endpoints are added to the network and others are retired from service on a daily basis. Like physical sight-inventories, many of the asset management and inventory solutions available today do not detect changes occurring on the network on a real time basis. In addition, many of these solutions have been designed to identify devices such as laptop and desktop computers and in some cases printers and IP phones, but these solutions typically do not have the capability to identify the ever expanding list of devices that are becoming IP-enabled.

Lastly, many of the traditional IT inventory and asset management solutions do not provide a bridge between having an inventory and putting it to use in the manner required for the purposes of improving network availability. As outlined earlier, managing the endpoint lifecycle often requires locating an endpoint to the network device to which it attaches to the network. This is imperative for effective and efficient incident response as will be outlined later in this document. Understanding that most of the asset management and inventory solutions were primarily designed to address compliance and financial

management requirements associated with IT assets, their utility for network management purposes can be somewhat limited. They simply were not purpose-built for supporting incident response and therefore may not provide the tools required for improving network availability through endpoint lifecycle management.

Systems management solutions have become widely deployed in the enterprise, but their functionality is typically limited to devices supporting end users such as desktops and laptop computers. Although systems management solutions have significantly improved the visibility and management of the user-centric devices throughout their respective lifecycles, they provide no capability to discover, locate and continually monitor the myriad other devices that are currently utilizing the IP network. Accordingly their utility for the endpoint lifecycle management purpose for devices other than desktop and laptop computers is limited.

A New Solution: The Beacon Endpoint Profiler™

The Beacon Endpoint Profiler from Great Bay Software has been designed to provide endpoint discovery, location and monitoring in order to deliver endpoint lifecycle management for enterprise networks. Through the Endpoint Profiling and Behavior Monitoring functions provided by Beacon, enterprises are able to maintain a real-time and historical contextual inventory of 100% of the endpoints connected to the network, throughout their respective lifecycles. Beacon utilizes a number of technologies and techniques for Endpoint Profiling and Behavior Monitoring that are inherently scalable, and do not impact the network or the endpoints themselves. Beacon utilizes a completely agent-less approach to endpoint profiling, relying instead on direct observation of selected attributes of endpoint behavior and attributes of the system to perform the Endpoint Profiling function. Beacon utilizes standard network management protocols to perform the endpoint location process, and all data is maintained in a standards-based and extensible database. The Endpoint Profiling and Behavior Monitoring data can be utilized by the existing enterprise network and security management software products such that the functionality of these platforms can be enhanced to include endpoint lifecycle management for the enterprise.

As outlined earlier in this paper, the requirement for endpoint lifecycle management cannot be addressed by simply generating a list of MAC or IP addresses of the devices connected to the network at a point in time (e.g. at the time a “scan” or inventory process is performed), with a one time assessment of what type the device is likely to be. The Beacon Endpoint Profiling functionality is an inherently dynamic function that is continually collecting information about all the network-attached endpoints in the network to maintain an up-to-date contextual inventory of all the connected endpoints.

The Beacon Endpoint Profiler system collects identifying behavioral information about endpoints primarily in a passive mode, potentially using observable endpoint behavior at multiple layers of the OSI model. Beacon also provides the ability to utilize other data

collection systems such as NetFlow for use in the Endpoint Profiling process. For endpoints that are difficult to profile via passive techniques, the passive profiling techniques can be augmented by an active profiling mechanism. The Beacon active profiling mechanism is very precise and limited in scope to actively query only designated endpoints for the purposes of generating endpoint behavioral data and not to simply probe or scan all possible ports. In contrast to other solutions that take a broad brush approach to active endpoint discovery that have proven problematic for special purpose devices with limited resources, Beacon's active profiling capability is more of a tightly focused approach. This enables the ability to discover and locate all endpoints without disrupting either the endpoints themselves or adversely impacting the network.

In addition, the Beacon Endpoint Profiler was purpose-built for providing all the necessary functionality required to address improving availability through endpoint lifecycle management, including the precise location of any endpoint in the environment. Beacon enables the location of each endpoint to the device and port that the endpoint is currently connected, and provides the current status of several port parameters required for incident response.

Beacon provides the current location of an endpoint maintained in real-time, while maintaining a historical database of information about each endpoint as well. The historical information enables the tracking of each endpoint, the profile or profiles it was classified into by Beacon, the IP address or addresses that it used, and where it was gaining connectivity to the network from across its lifecycle. This can be extremely important in today's enterprise networks that often have multiple sources of information such as SYSLOG servers, IDS or SEMs that are continually providing voluminous information about events occurring in the network. Network administrators often find themselves well informed about what happened in the past without any ability to marry that information to the present. Beacon provides that capability which again is critical to endpoint lifecycle management, and to date very difficult to achieve through a unified, commercially available solution for endpoint lifecycle management.

The day to day applications for a system that manages the endpoint lifecycle are countless, and include reducing the Mean Time to Repair for help desk calls, being able to detect all new devices added to the network, or simply using the data in the system for capacity planning. In addition, there are a number of use cases that are particularly compelling in today's IT landscape. Listed below are some challenges that network and IT security administrators are grappling with at present that can be greatly benefited by the usage of the Beacon system.

Audit and Compliance Initiatives

Given the recent focus on compliance and regulatory adherence, companies are increasingly looking to find a system that allows the network administrator to know exactly what devices are connected to the network and where. Auditors have recently made the transition from verifying external connectivity considerations to being more focused on the aspects of internal communications. This discussion typically revolves around what level of internal network access a non-enterprise asset can get by simply

plugging into a LAN port or attaching a hub or Wireless Access Point to the network from inside the enterprise. The nuance here compared to previous areas of focus is two fold; one being that the organization's local area network, and not external network connectivity is being focused on and the second is that the target of the analysis is not whether the network can be used to achieve connectivity to the internet, but rather what sort of internal services and data can be accessed from the enterprise's internal LANs. Defense mechanisms such as Proxy, Firewall, and IPS systems do an effective job of defending attacks on the enterprise IT infrastructure from outside the enterprise; the questions on auditors minds today are increasingly more focused toward these questions about connectivity coming from within: "does the organization know what is attached the LAN?", "Can changes to the endpoint landscape be detected and localized easily?", and "What level of access to internal resources can be achieved by connecting a laptop computer into a network jack from within the walls of the enterprise?"

Incident Response

Among the most compelling challenges in IT security incident response scenarios are those of timing and location. When the IT Administrator is looking into an event such as a virus, malicious behavior, or incorrectly configured endpoint, the event itself almost certainly occurred at some point in the recent past, either earlier that day, or the day or days previous. These events are most commonly indexed by the IP address of the endpoint in question, a value that is not terribly helpful given that a) the vast majority of Enterprise networks utilize DHCP and b) the IP address of an endpoint is incredibly easy to change. This means that whether the endpoint, and the person using it, where acting maliciously or not, there is a percentage chance that the IP address on that endpoint will have changed by the time the event is being analyzed.

Beacon solves these two challenges, timing and location, by providing the network administrator with the capability to identify the endpoints address information in the past (at the time of the event), and the ability to marry it with that endpoint's current address information. This understanding of the chronology of endpoints network address information is a critical enabler for addressing the second challenge. By understanding the addressing information across the lifecycle of the endpoint, Beacon can associate the location and address information from the time of the event with the current location of that station. This allows the IT administrator to close the loop on that incident by knowing the exact location of the endpoint at present, regardless of where it may have been at the time of the event.

Change Control and Endpoint Management Systems

Perhaps the biggest shortcoming of inventory and asset management systems is the continuous fluidity of the Enterprise network. Snapshot or manual approaches to gathering an inventory of all network attached endpoints can quickly become outdated and invalid. Beacon's continuous discovery and profiling of all network attached endpoints provides a continuously up-to-date view of the network edge. In addition, management packages that monitor and update devices such as Windows hosts, or VOIP phones can also be augmented by the data stored in Beacon. In this case Beacon provides a view into the subscriber rates for devices that should be managed by systems such as

SMS, Anti-Virus, and HP JetDirect by differentiating between devices that have spoken to the managing system and those that have not. As an example, this would provide an immediate view of the fact that 98% of the Windows devices had communicated with the AV update server in the past 30 days, while the 2% that had not could be quickly located and remediation performed to ensure that the correct software was installed and running.

Augmenting Asset Management systems

Existing asset management systems tend to provide visibility of either the Layer 2 MAC address or the layer three IP address. These systems provide an incomplete view of the endpoint landscape that can be augmented by the data available in Beacon. Using the Endpoint Profiling data in Beacon the complete picture regarding an endpoints location, MAC, IP, and behavioral attributes can be ascertained both in real-time as well as historically.

Enabling and Extending Network-based Authentication and Network Admission Control

Beacon provides a solution to the most compelling challenge to deploying and managing the authenticated or NAC-enabled network; that of discovering, provisioning, and securing the non-NAC or non-authenticating hosts. By automatically generating a working inventory of these endpoints and providing mechanism for configuring the network and monitoring the connectivity of these endpoints, Beacon dramatically decreases the cost and risk associated with a NAC deployment and completes the solution by providing NAC-like functionality for non-NAC endpoints

In addition, as port-based authentication (802.1X) or Network Admission Control (NAC) continue to gain momentum as approaches to control the network admission of devices owned by the enterprise as well as authorized guest devices, the criticality of endpoint lifecycle management as a prerequisite to successful deployments becomes more compelling. Having a functional contextual inventory of all endpoints in place at the front-end of an authentication or NAC deployment is often a must-have requirement particularly in the large enterprise. Beacon was architected and designed with authentication and network admission control in mind, and, as a result, has already implemented tight integration with market-leading solutions in this space. Beacon complements these systems by identifying, locating and provisioning access for the devices that cannot interact directly with the authentication and admission control mechanism. For many of the same reasons Beacon is particularly effective for addressing the discreet challenge of endpoint lifecycle management as described in this paper, it is also very well suited for integration with authentication and NAC at such time the enterprise chooses to pursue this enhanced level of internal endpoint security.

Conclusion

To maintain the availability and security of the enterprise network infrastructure today it is no longer sufficient to manage only to the edge infrastructure devices providing endpoint connectivity. Increasingly organizations require a contextual inventory of all endpoints in order to be able to maintain the availability and security of the network and unequivocally answer the question, “what is on the network, and where is it connected?” What is needed is an effective and efficient solution for endpoint lifecycle management. Endpoint lifecycle management is different in many respects to IT asset inventory and management solutions, and requires a purpose-built approach particularly in the ability to provide the functionality required for the use cases listed herein.

Beacon is the first product to unify the disciplines, tools, and techniques from network administration, management and security and apply them specifically to the problem space of endpoint lifecycle management. Beacon was designed to integrate with the leading enterprise network and security management platforms in order to leverage existing infrastructures rather than create yet another management console. In providing a unified solution for discovering and locating all endpoints both real-time and historically, the Beacon Endpoint Profiler system can help enterprises address endpoint lifecycle management and can help many enterprises achieve previously unattainable levels of network availability.