Understanding Your Attack Surface

Most enterprise IT organizations have a very limited understanding of their attack surface because they are unable to understand the full range of devices that are on the network. SANS recommends that the number one task in creating effective Cyber Security Controls is to develop an inventory of authorized and unauthorized devices.

Unfortunately, understanding the device inventory has become even more challenging with the advent of dynamic virtual networks, bring your own device (BYOD) policies, and Internet of things (IoT) devices appearing at the office. It is imperative organizations quickly discover every connected device: laptops, desktops, workstations, BYOD, mobile devices, data center and cloud virtual machines (VM), orphaned VM’s, network routers, WiFi access points, printers, smart appliances, wearable devices, and rogue devices. Eliminating or controlling these unmanaged assets on the network — which are far more likely to be compromised — greatly reduces an organization’s attack surface and overall risk.

Traditionally, network monitoring products have been used to help them perform regular SNMP or TCP/IP based network scans, in efforts to build an effective map of the network. While sometimes effective, monitoring solutions often fail to form a complete map as scan attempts are only successful if devices have enough networking capabilities enabled to respond. Further, device scans are often confused with malicious network scans, as they are similar to device scans performed by some flavors of malware, and are often blocked by deployed security defenses. Device detection that depends on point in time scanning technologies often create issues for IT departments, and don’t provide a complete view of all the devices in the network.

http://www.prweb.net/Redirect.aspx?id=aHR0cHM6Ly93d3cuc2Fucy5vcmcvY3JpdGljYWwtc2VjdXJpdHktY29udHJvbHM=

Unmanaged IT Asset Discovery

Challenge

IT security teams need to identify:

- Unapproved routers and network access points.
- Unmanaged virtual machines.
- Unmanaged IoT and business devices.
- Hosts without required management software.

Benefits

- Eliminate uncontrolled network access points.
- Ensure that all hosts have the required management software.
- Control network access for unmanaged IoT and business devices.
- Understand and manage their virtual host landscape.
- Fully evaluate the network’s attack surface.

© Copyright 2017 Ziften Technologies, Inc. All rights reserved. | Solution Brief
Continuous and Quiet Discovery

As a key aspect of understanding an organization’s security posture, Ziften Zenith includes passive and continuous unmanaged asset discovery.

Every Ziften Zenith agent in the network takes on the task of passively monitoring for Ethernet announcements that are required for any network device to operate in the same network. This information is constantly evaluated and any changes in the list of connected devices are delivered to the Ziften Zenith server. For each discovered device, Ziften can determine whether the device is under management by IT, and if the device is not managed, Ziften provides product details on the connected device.

As the Zenith solution discovers network devices passively, obtrusive network scans are not required, avoiding unwanted network traffic and device impacts. This eliminates unwanted security tool alerts from the asset discovery process. Since the agent is constantly assessing the device health and monitoring for new devices, the Ziften console always provides a current view of any devices that have accessed the protected network.

Tracking Over Time

In addition to continuous asset discovery, Ziften tracks asset connectivity over time storing the historical data for analysis. Not only can organizations identify unmanaged and or rogue devices in real-time, but they can evaluate the connectivity behavior of each device over any time period. This historical connectivity view allows IT to determine when a device first connected to the network, when it last appeared, and how often it reconnects.

Improve Your Security Posture

Full knowledge of the devices on a network is the first step to improving the security posture of an enterprise. Ziften finds that as many as 30 percent of all connected devices can be unmanaged or unknown in today’s enterprise networks, exposing organizations to dramatically increased risks. Once detected, IT organizations can take steps to eliminate unnecessary risks and bring unprotected devices into compliance with IT security policies. Once a host is identified, the Ziften Zenith agent can be deployed, allowing for deep visibility into the device health and security state.

“Device detection that depends on point in time scanning technologies often create issues for IT departments, and don’t provide a complete view of all the devices in the network.”
Ziften’s discovery of unmanaged assets also helps organizations maintain regulatory compliance. Compliance mandates require regular asset discovery efforts. Ziften provides continuous views of all connected devices, not just point-in-time checks. This capability prevents missing rogue devices that may only connect to the network intermittently, and greatly increases the ability of security operation teams to ensure unmanaged connected devices are either removed from the network or brought into compliance with internal or external security requirements.

For enterprises, Ziften’s asset discovery improves security team efficiency. With detailed intelligence on each connected device including the manufacturer, hostname, and the device type, operation teams can quickly clean up their environments eliminating rogue and unmanaged devices — even VM proliferation. The removal of these at-risk devices reduces security alerts, reduces alert fatigue, and increases time operation teams spend on productive endeavors.

Contact Ziften for more information on how to improve your organizations security posture.

“As many as 30 percent of all connected devices can be unmanaged or unknown in today’s enterprise networks, exposing organizations to dramatically increased risks.”