## Contents

- **Introduction** ..................................................................................................................................................................................... 3
- **The ForeScout Approach** .......................................................................................................................................................... 3
- **Discovery Methodologies** ........................................................................................................................................................ 4
  - **Passive Monitoring** ...................................................................................................................................................................... 4
    - Passive Authentication ................................................................................................................................................................. 4
    - Passive NMAP (Universal) ............................................................................................................................................................ 4
    - DHCP & ARP Request Monitoring .......................................................................................................................................... 4
    - IPS Monitoring ........................................................................................................................................................................... 4
    - Spoof Detection (L2 and L3) ....................................................................................................................................................... 4
  - **Active Interrogation** ..................................................................................................................................................................... 5
    - External Scan ........................................................................................................................................................... 5
    - Internal Scan (Windows, MAC, Linux) ............................................................................................................................... 5
    - Internal Scan (SNMP & CLI) ................................................................................................................................................ 5
  - **Network Integration** .................................................................................................................................................................... 5
    - LDAP, RADIUS & 802.1X .......................................................................................................................................................... 5
    - Patch Management & Helpdesk ............................................................................................................................................... 5
    - Firewalls, Routers, Switches, Remote Access VPN .............................................................................................................. 6
- **Deployment & Discovery Capabilities** ................................................................................................................................................ 6
  - Layer 2 Deployment & Discovery ................................................................................................................................................ 6
  - Layer 3 Deployment & Discovery ................................................................................................................................................ 6
  - Hybrid Deployment & Discovery ............................................................................................................................................... 6
  - The Response Port ........................................................................................................................................................................ 6
- **Network Device Detection (Wireless Access Device)** .................................................................................................................. 8
  - Passive & Active Interrogation ....................................................................................................................................................... 8
  - Multiple MAC Address (Switch Port) ....................................................................................................................................... 8
  - NAT Device Detection................................................................................................................................................................. 8
Introduction

This document has been created to explain the mechanisms used by ForeScout CounterACT to detect devices and hosts, as they are connected to a network, in addition to looking at how CounterACT can help identify unauthorised network devices, such as switches, routers and rouge access points, including the policies that can be implemented to disable any such devices.

The ForeScout Approach

ForeScout CounterACT is an integrated network security appliance that delivers real-time visibility and control of all devices on your network. CounterACT is deployed out-of-band on your network by receiving mirrored traffic or by integrating with network layer devices such as routers, switches, wireless controllers, and authentication services. ForeScout CounterACT automatically identifies who and what is on your network and controls access to your network resources from any host or segment, measuring compliance with your security policies and remediating or mitigating endpoint security and policy violations when they occur.

ForeScout CounterACT employs a proven approach for IT risk management, as shown in the diagram below. Every device that accesses the network is identified, inspected, remediated (if you wish), and continuously monitored.

ForeScout CounterACT revolutionizes Network Access Control (NAC) technology by eliminating deployment obstacles of typical solutions, such as costly hardware upgrades and lack of interoperability with existing infrastructure. Unlike other solutions, ForeScout CounterACT installs quickly and easily. It seamlessly integrates with any network environment. No software to install. No hardware upgrades.

CounterACT is 100% agentless, which means there is no software to install on endpoints. It works with all of your existing endpoints – managed and unmanaged, known and unknown. And CounterACT can control access to your network with or without 802.1X.
Discovery Methodologies

ForeScout CounterACT can discover devices as soon as they connect to the network, in both centralised and distributed network architectures. Through a combination of effective techniques, CounterACT provides the highest detection accuracy possible, allowing administrators to create effective reporting and remediation policies, based upon the types of devices connecting to the network and their activity whilst connected.

Passive Monitoring

Passive monitoring allows CounterACT to accurately detect the hosts and devices communicating across your network, without the need to be connected inline of critical data-flow paths. With passive monitoring CounterACT simply receives a mirror (or SPAN) of the data-flow (either port based or VLAN), and from there CounterACT is able to perform the following functions to enumerate the hosts and devices connected:

Passive Authentication
ForeScout CounterACT can monitor traffic to an existing server (or group of servers) and passively monitor the authentication of those devices. From the conversation, CounterACT can identify the user, the authentication status, and identify the device they have authenticated from. New events will be stored, and the source device (IP and/or MAC address) will be shown in the CounterACT management GUI.

Passive NMAP (Universal)
ForeScout CounterACT can analyse the L3/L4 data within a packet and by comparing the output of this data to a detailed database of known operating system and application traces, CounterACT can accurately determine (in most cases) the operating system and services being run on the remote host, as the data traverses the network and is mirrored to CounterACT.

DHCP & ARP Request Monitoring
By monitoring the DHCP and ARP requests across the network, CounterACT is able to identify when new hosts or network devices connect to the network, by analysing the source and destination of these requests. Through correlation of these events in the CounterACT database, we are then able to build up a real-time picture of where new devices or hosts are connecting and what network segments they are connecting to.

IPS Monitoring
As CounterACT begins to build a database of know hosts and network devices through passive monitoring techniques, we then further analyse the traffic flows and consistency between those hosts and devices. Through our own threat detection engine, CounterACT is able to detect hosts performing malicious actions such as port scans, attempted infections, service scans, etc. and immediately report and/or remediate such hosts or devices on the network.

Spoof Detection (L2 and L3)
ForeScout CounterACT provides the capability to detect hosts that attempt to spoof either their IP or MAC addresses when attempting to connect to other hosts across the monitored network segments.
Active Interrogation

ForeScout CounterACT can also employ active interrogation techniques to provide further detailed information on hosts and devices that are connected to the network. With active interrogation, CounterACT can be configured to run further detailed scans and report back the information collected, to allow administrators to define more granular response and control policies. Active interrogation is performed in one of the following ways:

**External Scan**
ForeScout CounterACT can run an active external scan against hosts and devices to gather more detailed information with respect to the operating system, vendor, services, applications, processes, and available files (where applicable). This data is then revealed within the CounterACT management GUI, providing administrators with a real-time view and further detail on the exact device type or state of the host that has connected to the network.

**Internal Scan (Windows, MAC, Linux)**
Perhaps the most detailed information is achieved through an internal scan of the host devices on the network. Through either service level account access to domain machines, or through the installation of an 800kb thin-client connector (called SecureConnector), ForeScout CounterACT is able to query the device in detail to discover almost any piece of information available about the host. In environments with guest users or non-manageable hosts, the CounterACT SecureConnector can be installed so that it dissolves, when the user/host disconnects from the network, so that no changes ever need to be persistent on non-corporate host devices.

**Internal Scan (SNMP & CLI)**
With respect to network devices such as printers, manageable switches, routers and wireless access points, CounterACT can be configured to use SNMP or CLI read of the devices, to retrieve further detailed information from the device on OS type, device type, connected host devices and much more. All this information is revealed within the CounterACT management GUI to help administrators check on compliance levels.

Network Integration

The network integration part of ForeScout CounterACT provides a wealth of additional detail on the state of the network, hosts connected and their level of compliance against policies such as PCI, anti-virus, windows patch, software versions and much more. ForeScout Counteract can integrate with the following:

**LDAP, RADIUS & 802.1X**
CounterACT can integrate into multiple authentication services, to actively or transparently authenticate those devices that connect to the network, before permitting them authorised access to network resources.

**Patch Management & Helpdesk**
CounterACT can integrate with existing patch management & helpdesk solutions to automate remediation, logging and reporting tasks of any non-compliant hosts or devices.

**Firewalls, Routers, Switches, Remote Access VPN**
CounterACT can integrate with other network layer devices to gain further information on connected host devices and users. In the case of remote access VPN solutions, CounterACT can integrate with the VPN gateway server to monitor and interact directly with the connected hosts, for compliance checking and enforcement of those hosts before they gain access to the core and critical network resources.
Deployment & Discovery Capabilities

Discover of devices, hosts and users across a corporate LAN/WAN environment is achieved through the integrated approach of passive interrogation, active interrogation and network integration techniques as described previously. It’s important to note that the accuracy of detection will vary and is directly dependant on which of the discovery techniques can be used; this also depends on the deployment method of the CounterACT appliance itself. CounterACT can be deployed in any one of following modes:

**Layer 2 Deployment & Discovery**
In a Layer 2 deployment topology, CounterACT is configured to receive the mirrored (or SPANNED) data flows from a particular point (or multiple points) on the network. In most cases CounterACT is deployed at the core or distribution layers of a corporate network, monitoring access to and from centralised resources, such as authentication, DHCP, and file or print services. When deployed in this mode, CounterACT can be configured to receive VLAN tagged traffic from thousands of VLANs.

**Layer 3 Deployment & Discovery**
In a Layer 3 deployment topology, CounterACT is configured to integrate directly with network layer devices, either at the core, distribution or access points of a network and can also be configured to integrate with remote site network layer devices. In this deployment mode, CounterACT relies on a connection to the network layer devices and remote sites to be able to enumerate newly connected devices on the network, before further interrogation can be performed in addition to a L2 SPAN of core network traffic (dependant on where the CounterACT is deployed in the network) to ensure great visibility capabilities.

**Hybrid Deployment & Discovery**
In a hybrid deployment topology, CounterACT is configured to monitor traffic at L2 either at the core, distribution or access points in the corporate network. Additionally CounterACT is also configured to integrate directly with the network layer devices across the corporate network to provide further information on host location, as well as being able to discover network activity on remote sites across the WAN, through integration with those network devices also.

**The Response Port**
One of the most important elements of the CounterACT solution is a correctly connected and configured response port so that the CounterACT appliance can respond to events (discovery, threat, end-point alerting, compliance enforcement & remediation, etc.) CounterACT has the ability respond at both Layer-2 and Layer-3 to any such events, and the switch/router port must be configured correctly to allow the desired response capability. CounterACT can be configured to respond at Layer-2 (on each VLAN) or Layer-3 (IP Layer) simultaneously, where required.
Deployment Scenarios

Given the several options available for deployment of ForeScout CounterACT, let’s take a look at the typical network topologies supporting each deployment methodology:

Layer 2 — Deployment Example

In a Layer 2 deployment, the CounterACT appliance is configured with one or more channels. Each channel will consist of 2 ports: a MONITOR PORT (typically a TRUNK PORT if SPANNING multiple VLAN's from the switch, or an interface SPAN, spanning all traffic passing on a specific interface from a switch or router) and a RESPONSE PORT. The CounterACT will also have a third port which is used for management. Therefore the minimum number of ports required in a Layer 2 deployment will be 3 ports. The following diagram shows this configuration:

Layer 3 — Deployment Example

In a Layer 3 deployment, the CounterACT appliance is typically configured with one channel. In this scenario, the channel only requires two ports: a MONITOR PORT (typically a TRUNK PORT if SPANNING multiple VLAN's from the Switch, or simply an interface SPAN, spanning all traffic passing on a specific interface from a switch or router) — it is important to note that the monitor port is optional in L3 mode given that the CounterACT is now able to build its database of devices and hosts from the MAC/ARP information it receives from network switches and/or routers through the switch plugin — and a MANAGEMENT PORT, which will now also act as the RESPONSE PORT in the channel configuration. The following diagram shows the configuration and typical network deployment topology:

Hybrid (L2 & L3) — Deployment Example

In a hybrid deployment topology, the CounterACT appliance can be configured to communicate centrally with remote sites via its management interface to poll switches/users and authentication servers for user/device discovery and completely network visibility. In some environments the CounterACT appliance is deployed at both L2 (receiving a SPAN/MIRROR of all network traffic at the core/distribution layer of the central site and responding via a dedicated L2 response port — typically in trunk mode) and L3, whereby the L3 element is simply another channel that uses the management port to poll remote network devices for network discovery and visibility, including policy enforcement (where applicable) for specific network or user actions and enforcement.
Network Device Detection (Wireless Access Devices)

CounterACT provides the ability to discover network devices that may be connected to a corporate network, allowing administrators to see instantly where the change has occurred and then provide a means to respond to this activity and either restrict or disable the device entirely. It is important to note that CounterACT effectiveness at detecting network devices, such as a switch, router or wireless access point, is dependent on how where the CounterACT appliance is deployed (and in which mode) and how CounterACT receives notification of a new device on the network (passively through a L2 monitor port, or through SNMP/CLI access to a switch/router or through integration with authentications or DHCP server log information).

Ultimately when a new device is discovered the interrogation techniques are the same and the CounterACT will actively interrogate a new device, to discover its type. In the case of a wireless access device, CounterACT relies on the following:

**Passive & Active Interrogation**
CounterACT will passively and actively interrogate the newly discovered device, to discover as much detail as possible as to the OS Type, available services and location of the newly connected device, and display this information in the CounterACT management GUI. Once the network device has been identified, CounterACT can automatically compare the device against a list of authorized devices and classify the device accordingly.

**Multiple MAC Address (Switch Port)**
In the case where a switch or access point (in bridge mode) has been connected to the network, CounterACT can be configured to notify the administrator when it sees more than X number of MAC address sitting on a non-trunk switch port. In this case it is evident that a network device has been connected and as such a policy can be configured to monitor further activity or prevent access entirely.

**NAT Device Detection**
ForeScout has developed a proprietary and accurate NAT detection analysis engine to identify when a network device is connected to the network, such as to an existing router or switch port, and where that device is not known to the CounterACT appliance it is shown immediately as non-corporate or unauthorised device. By observing the ARP requests and/or DHCP and network events from newly connected devices and through active interrogation, CounterACT is able to quickly enumerate a NAT device/host and ensure that it is locked down (as per compliance policy) or reported on in real-time.

Through the detection of the above events, CounterACT can accurately identify new network devices that are connected to the network, either centrally or remotely, and then check these devices against the configured compliance policy to classify them as either rouge, unauthorised or corporate devices and permit/deny the relevant level of access to critical network resources.