Full protection for all networks

Dr. Götz Güttich

With CounterACT 7, ForeScout offers a comprehensive security solution that enables companies to monitor and protect their networks. CounterACT not only keeps an eye on devices, operating systems and applications, but also an eye on every user account. The product can be used to protect important data and network components without inhibiting the productivity of your staff or business partners. CounterACT even enables administrators to safely enable guest devices or external users such as auditors, consultants, etc. on to the corporate network. In addition, the ForeScout solution can be seamlessly integrated with many other security solutions such as Nessus by Tenable, Microsoft's System Center Configuration Manager or McAfee ePO (ePolicy Orchestrator). We have tested CounterACT's performance with great scrutiny at the test laboratory.

CounterACT can be used for safeguarding a system without having to install software or an agent. Nor does it require any configuration changes of network clients. The product is available both as an physical and virtual appliance and can therefore be easily integrated into networks.

The solution uses powerful NAC (Network Access Control) functions to secure corporate networks. Therefore, it is not only able protect components against external attacks in some ways like a Firewall does, but, it also safeguards the integrity of networks by protecting them against threats from within the enterprise. For example, CounterACT ensures that visitors are able to use certain company (network) resources; that wireless and BYOD devices can safely communicate with the company network – but rogue devices have no chance to tap into the LAN. The product also protects your network from malware, worms and botnets. At the same time, it ensures that all devices in the network comply with company policies.

After installing the appliance, policies that should be applied to the network have to be defined. These policies might for instance to identify or block data transmission to all unknown devices in the network, or limit wireless components' access to the Internet while restricting their access to company resources. They are also able to identify and quarantine non-compliant computers, such as those without patches or an antivirus solution; to restrict network access for guests; and to run vulnerability checks. The results of policy assessments (device discovery and compliance checks) are available at all times via a web-based dashboard.

Functions

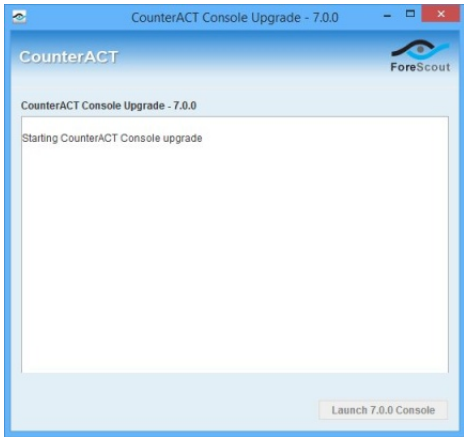
CounterACT does not only implement policies; it comes with a great number of other functions, including support for 802.1X with an extra RADIUS server; support for LDAP and AD authentication and a real-time inventory function. The latter ensures that administrators can monitor, supervise and protect applications, user accounts, services, ports, processes etc.

In addition, a tactical map displays all devices, their exact position and the location where an issue has occurred. The drill-down function ensures that problems can be detected and mitigated quickly.

As mentioned before, CounterACT also offers wide-

ranging endpoint compliance functionalities. Those enable IT-staff to ensure overall compliance with configuration standards (such as antivirus and patch policies) throughout the network; that personal firewalls work (are installed and active) and that no unauthorised applications are running on systems.

If a computer does not comply with company policies CounterACT informs the



As soon as CounterACT has been installed it first updates the management tool

administrators of the user, the device's location and the problem identified by the solution.

Thanks to close monitoring of users and their devices, the system can identify users who are running Peer-to-Peer-Software (P2P), or engage in any other undesired activities. Using CounterACT, the IT department may send a warning to these users, restrict their data access via a virtual firewall, or kick them out of the network. The product also protects systems against hackers by offering a behaviour-based IPS with honeypot features.

The solution is also available with high-availability configuration, thereby ensuring that network protection can remain active even in case of a hardware failure. According to the manufacturer, CounterACT delivers a good performance even in very large environments with more than 500,000 endpoints. There are several models available which are suitable for environments of all sizes.

The Test

We tested the CounterACT appliance by deploying it into our network. The corresponding management tool, the CounterACT console, was installed on an administrator work station. We let the solution collect data about our environment and defined policies to ensure that all our components are working properly. This included policies for the classification of existing systems, for compliance and handling malicious hosts. Policy violations were eliminated with the help of remediation actions.

The next step was testing guest management. In addition, we analysed the way CounterACT was protecting the network from rogues. Then we tested features for BYOD (Bring Your Own Device) and MDM (Mobile Device Management), as well as CounterACT's interoperability with third-party solutions. We used Nessus by Tenable, McAfee's ePO and WSUS by Microsoft for this test.

Installation

The CounterACT appliance normally operates with three different interfaces: The management interface is used for managing the solution. The monitoring interface monitors network information and traffic, while the response interface transmits information to take action from corporate network in case of security problems, for instance by blocking rogue DHCP servers or interrupting data transmission.

We tested the solution in our network on a monitoring port of a Cisco Switch (SPAN. For the response port we used a VLAN trunk on the same switch. Many other configurations are also possible as described in detail in the product documentation. For example response and management ports can be merged (layer 3 installation) in smaller environments.

After connecting the appliance, we assigned an IP address via the local console and set the administrator password. Then we accessed the appliance from the management client via the URL http://{IP address of the appliance}/install to download the installation file with the management software. Setting up the product was fairly easy from this point on. Installation basically only requires one output path. As soon as the output path is chosen, setup is done automatically and the console can be used immediately.

First Login

At opening the management console, we could log on to the appliance with the IP address and administrator credentials. The installation wizard started automatically, asking for the main parameters required to start the system. This includes for instance setting the user directory for network authentications and

correlate user details. In addition to the Active Directory used in our test, the ForeScout solution also supports Sun Java System Directory, IBM Notes, LDAP, Novell ‘s eDirectory, as well as RADIUS and TACACS systems.

The assistant then asks for domain credentials, which ensure that the ForeScout appliance can closely monitor the network hosts (without the use of agents). Under “authentication servers” additional authentication systems – such as exchange servers – can be added to the network. The

define the internal network and to configure CounterACT switch plug-in that the system uses to monitor and adjust switch configuration in the network.

The last dialogue box in the wizard is called “inventory”. It is used to display network assets and activities (for example process and services) of logged-in users and devices in real-time within in the management console. This information can again be used to create or improve security policies. For instance, if the administrator uses

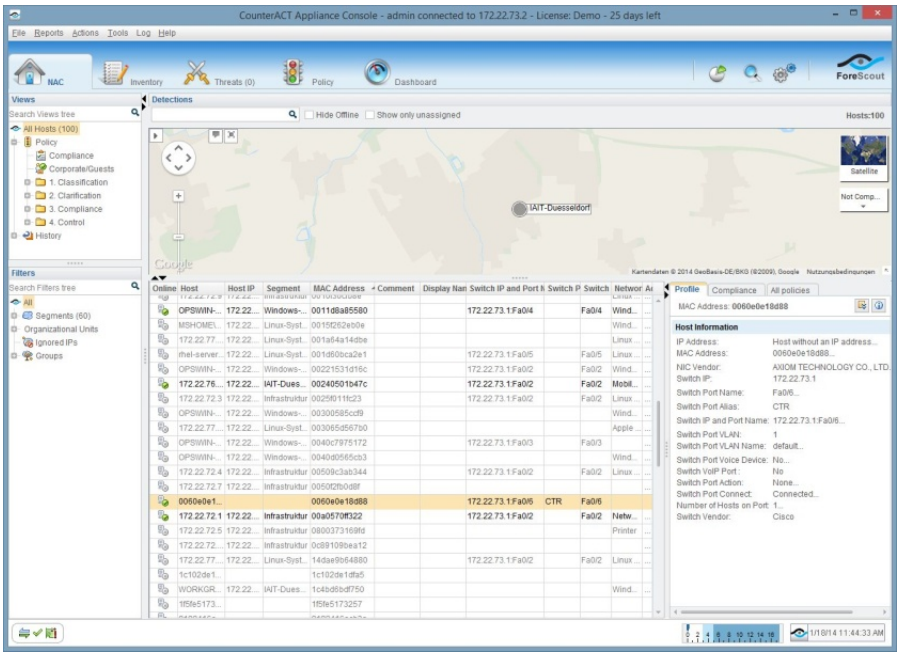
displays a tree structure directory with all policies and filters to limit the number of components to view.

This also includes network segments, internal organisational units and internal groups. If you select a policy or a filter object – for example a group with Windows computers – the hosts will be listed in the workspace in the middle of the screen. The workspace not only provides detailed information on the system, but the list can also be used to get a quick overview of the security status of the network. The list does includes data such as the IP and MAC address, as well as offers additional fields with information on activities, compliance, host status and other details. Company IT staff can always delete or add fields to the chart in order to customise it according to their individual needs.

It is even possible to integrate data from third-party solutions into the list. For example, they have the option to monitor the current state of the McAfee ePO data based on the ePO server and display this data directly on the list. In addition there is also a “history view” function, allowing users to check system conditions at a certain point in the past.

Right-click on the tree structure for administrative tasks such as adding details or to run the policy manager. It is also possible to start, stop, import and export policies.

By right-clicking on an entry in the list, administrators can initiate certain actions: Starting or cancelling the secure



The NAC overview provides a list of monitored devices and a mapping function

domain controller, that we had added previously, was automatically displayed at this point.

The authentication servers help the appliance to identify which hosts are able to authenticate themselves in the LAN. The product supports the following authentication services: HTTP, Telnet, NetBIOS-SSN, Microsoft-DS, FTP, IMAP, POP3, rlogin and MAPI. The wizard also enables the user to

the inventory function to detect an unauthorised service running on one of the guest devices, he can put a policy in place that blocks this service for guests.

Management Console Features

When the administrator logs on to the ForeScout CounterACT management console in normal operation mode, he will be directed to a screen which has been subdivided into eight areas. The most important area is called “NAC”. On the left hand side it

connector (this is an optional client component of CounterACT that can be used if a host is not accessible otherwise, or if hardware management e.g. of USB ports is necessary), adding the system to specific groups, cancelling processes, starting updates, blocking data transmission, etc. [Note: these actions can also be automated in a policy.]

The second important area of the management tool is the inventory. The solution again provides different views in a tree structure, which can be narrowed down by using filters. Available views include users, registration for guests, open ports, installed applications and OS-specific data for Linux, MacOS and Windows computers. When selecting a Windows system (for example), the solution shows running processes and services, as well as Windows versions. If the user selects a view, all corresponding items, such as a list of open ports, and problem issues appear in the workspace.

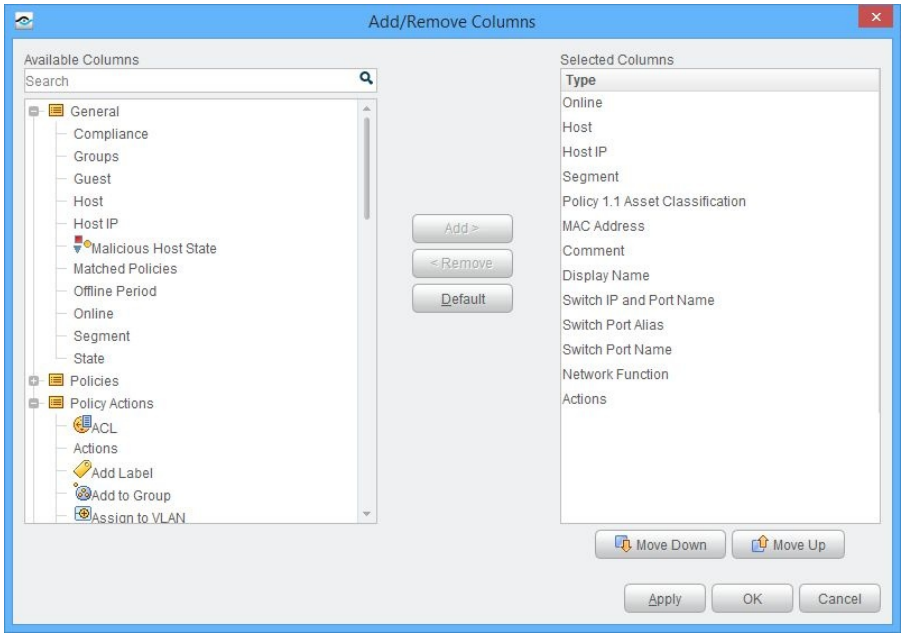
Threats are also displayed with the help of views and filters. All current threats are listed here. If the administrators select a threat, an overview of the affected system is shown.

The policy manager enables the administrator to define and manage policies. Policies consist of one or more criteria that must be met or may just be of interest. They are complemented by actions, which are implemented by CounterACT according to the policies.

A simple policy criterion could be for instance whether a specific system is a member of the domain. After having verified this criterion, it implements the action: the system in question is either included in the group "domain members", or is moved to the group "guests". By combining several criteria, complex policies can be created. For example the solution identifies a handheld computer and is able to differentiate whether it is an Android or an IOS device.

They also detect if the device has been rooted or jailbrocken. Finally they also analyse whether the user has signed in to the network through an authentication system. Depending on the results the administrator may define several actions, for instance granting full access to the company network to authorised, non-jailbroken IOS users, while Android users are only granted Internet access.

The policy manager administers the definition of these policies and enables authorized persons to define exceptions or change settings. For example, we set up the ForeScout solution to check every two hours whether systems are still compliant with policies. CounterACT provides extensive templates for defining policies and actions, including a great number of functions which can be linked meaningfully.



The CounterACT summary list can be tailored by activating numerous fields having additional information, making sure that administrators can always keep an eye on all relevant network occurrences

Linkable criteria are for example operation-system-specific data, such as: registry keys under Windows, fingerprints, SNMP information, etc. There are also numerous actions to choose from: audits (send message/log, start scan), notifications, problem-solving functions (disable P2P transmission, run script or similar) and restrictive actions (moving hosts to VLANs and blocking ports).

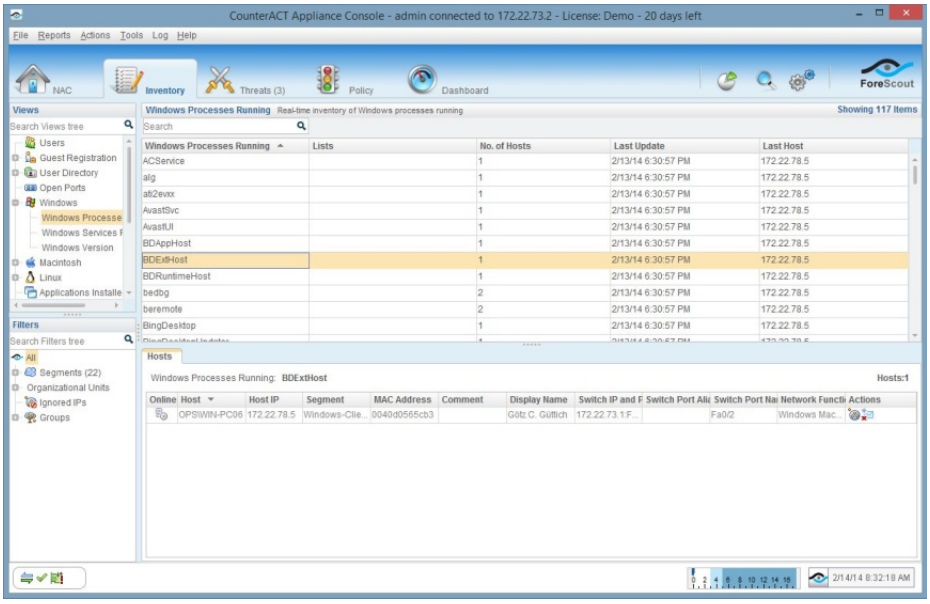
The next items of the administration solution support a web interface, which can also be used as a stand-alone feature if necessary. The dashboard Tab

shows an overview of the network status using graphic representation. The reports Tab gives access to the CounterACT reporting functions. There are many reports available, such as "Assets Inventory", "Policy Trend", "Policy Status", "Compliance Status", "Device Details", “Registered Guest" and so on. Reports can be automatically created with a scheduler on a regular basis.

The "Assets Tab” offers a search function that enables the administrator to analyse all data previously gathered by the security solution. The last item in the management tool enables configuration of CounterACT. In the field “Options” administrators can add updates, configure plug-ins, define how the solution interacts with the network, work with guest registration, specify the Active Directory-Server (if available) and enter mail data for notifications. In addition, they also ensure the seamless interoperability of CounterACT with external systems, such as the System Center Configuration Manager (SCCM), Windows Server Update Services (WSUS) by Microsoft, ePolicy Orchestrator by McAfee, Nessus and MDM (Mobile Device Management) solutions like MaaS360. The number of executed actions such as blocking data traffic can also be set in this menu. The same applies to policies for the virtual firewall, as well as for the management console’s user profiles.

Working With Policies

After having integrated the CounterACT system into the network and examined the scope of services, we continued our tests by taking a closer look at working with policies. All policies are given a name, a scope of where they are applied – such as a group of host systems – and conditions, which define the actions CounterACT shall take if needed. One example for such an action could be blocking P2P traffic.



The inventory view of ForeScout CounterACT showing Windows processes currently running

In our test we used the policy manager to generate and implement policies. The first policy that we applied had already been created during initial configuration. It classified devices already discovered on the network.

This (real-time asset monitoring) provided a clear intellience, simplified the management of all components and created the basis for correct system handling by CounterACT. The policy categorized all devices under supervision according to their type and/or tasks. Windows devices for example were assigned to a different group than Unix/Linux systems or network components. The policy was fairly easy to configure. First of all, the administrator has to define the segments that the policy should be used for. In our testing environment, we applied policies (using templates) to all network components. Several conditions were establish: one condition was to check whether the device analysed is a Windows device. If so, CounterACT needed, in this case, to add the device to the Windows group. If it was not a Windows device, the system simply moved on the next set of conditions.

In this case, checking whether it is a handheld device. If it was a handheld, it was moved to the correct group. If not, the system moved on to the next set of conditions. This procedure would be carried out until every step was completed. Devices that still remained unclassified were put into the “unclassified” group by CounterACT.

This group allows further refinement of the policies at a

later point, enabling all devices in the network to be eventually classified (and assessed).

A large number of built-in policies are available to identify the device type, this includes networking functions: open ports, MAC addresses, DHCP device class, DNS names, and many more. All terms are listed in a dialog box. They are arranged in groups, so it is straightforward to find the entries you are looking for. There are main categories like “Classification", "Device Information", "Guest Registration", "SNMP" and "Wireless".

The second policy we chose was the corporate/guest policy, which was supposed to separate corporate from guest workstations. To this end, the system assessed endpoints to see whether they were a domain member or able to login to an authentication server.

If these conditions were met, they were moved to the group “Corporate Hosts”. All other components were assigned to the “Guest” group. There are more options available than simply assigning systems to certain groups. They can also be used to secure the network, for instance by restricting network communications for specific devices with the help of CounterACT’s virtual firewall policies.

The next policy we focused on is handheld devices. We had handheld devices that were registered in our MDM system (we were using an Mobile Device Management solution from IBM called "MaaS360” in our test) assigned to the group "MaaS360 Enrolled Devices” and given full access to our network. All others would receive an HTTP notification as soon as they were trying to access the network, and if they were unknown to the MDM, the user would be informed they woul have to register first to get network access.

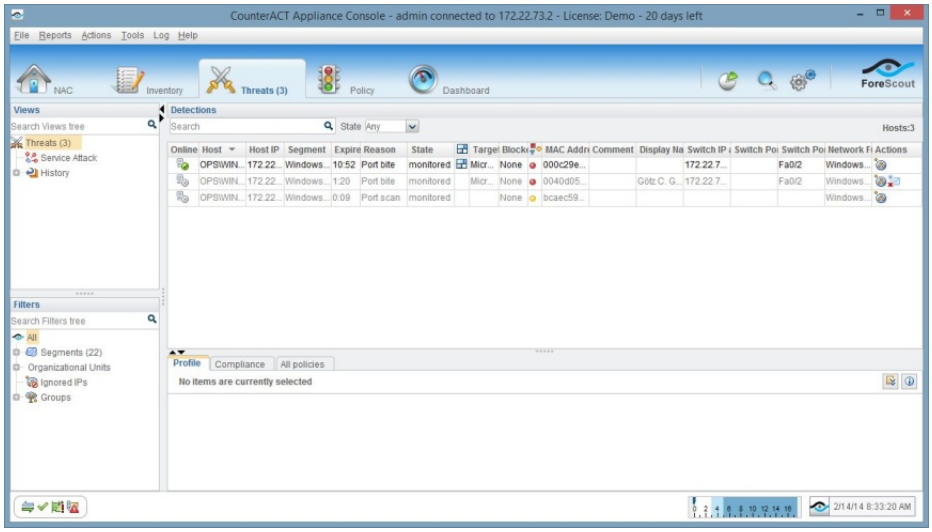
We added another policy to enable additional classification of MDM devices, for example differentiating between Android and iOS devices. Generating policies always follows the same schema: you define the segments (or groups) that the policy applies to, specify the terms which determine what to do and the actions to be implemented.

After having grouped all our network components, we started creating compliance policies to safeguard our network. The first two policies ensured that all Windows workstations have the latest patches and antivirus solution. If these criteria are not met, the system is deemed to be non-compliant and therefore in violation. In that case several remediation actions can be initiated to restore the effected workstation’s compliance.

Our antivirus policy for example offered three different measures: if there was no antivirus product installed on the device, the person responsible received an email. If the device had an antivirus programme installed, but the programme was not running, it was started. If the antivirus programme was using outdated/obsolete signatures, an update was initiated.

If Windows systems were not up-to-date, the policy automatically initiated a Windows update. An additional compliance policy ensured that administrators were notified if the Windows firewall was not running on a Windows client.

Other policies focused on malicious hosts and ensured that the person responsible was notified via e-mail if suspicious activities were detected in their system. These suspicious activities include: port scans, communication with suspicious mail servers, password scans,



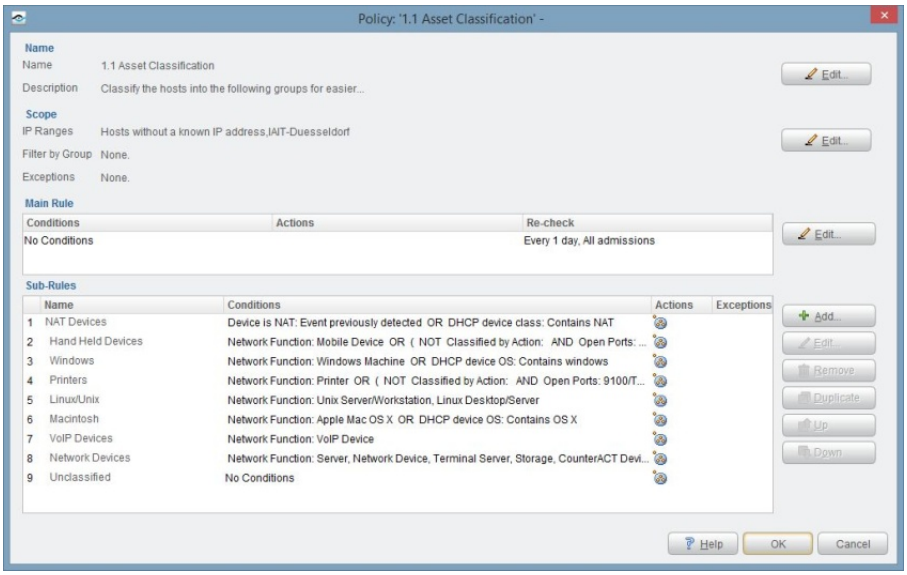
The threat overview keeps the administrator updated on current threats in the network/ lists the latest threats to the network

service scans and many other activities. In general, defining policies with the help of the policy manager and the templates proved to be rather simple and convenient.

Managing Guests
As soon as all policies were in place and running, we turned to managing guests. By establishing policies, we had already ensured that CounterACT differentiates between company workstations and guest devices. Guests were permitted to register to the network and receive login data. CounterACT provides a login registration form for this purpose. There is also an optional (guest management) setting that requires approval of guest device registration by authorised company staff – a so called sponsor – via email, who can have such a code. This way it is possible to limit the number of guest devices.

In addition, ForeScout CounterACT also enables the use of guest tags. They can be used to assign registered guest devices to specific groups. This way users can be granted different rights. In our test, all these functions as well as access control restrictions were running smoothly from the start.

BYOD
Integration of BYOD components – devices, which are not corporate hosts, but belong to an authenticated corporate user who is authorised to access the company network – can be done just like all other network security measures with the help of policies. This is easy to do –



The threat overview keeps the administrator updated on current threats in the network/ lists the latest threats to the network

also define rules such as access password and use. If necessary IT staff can also add or delete guests accounts and devices manually any time. In addition CounterACT also offers so called registration codes. They ensure that only those guests can register (to the network) who all the administrator has to make sure of is to assign user rights to user accounts rather than to devices.

Working with Tenable Nessus
As mentioned before, various plug-ins enable seamless integration of external services. To test interoperability with Tenable Nessus, we first installed the product on a host in our LAN and checked whether it was working properly with a few quick security scans. As soon as we had assured that everything was running smoothly, we installed the "VA Integration Module" to the CounterACT appliance with CounterACT's Nessus plug.

With the help of configuration options, we entered the Nessus server, the port and access data and tested the connection. After the positive test, the plug-in configuration offered various scan policies, which had been previously created and provided on the server. These scan policies determine how scan inquiries are handled.

When this configuration was completed, we were able to use Nessus just like a CounterACT feature. Nessus scans can for example be used in policies. We tested this function by creating a policy, which was scanning all active company workstations with Nessus once per day(and at log in). No problems occurred during our testing period.

McAfee-ePO
Integrating the E-Policy-Orchestrator by McAfee into the CounterACT environment does not only require the installation of a plug-in to the ForeScout system, but also installing an extension on the ePO server. As soon as the plug-in is installed, the CounterACT appliance offers the ePO extension for download via a web portal.

As soon as the download is completed, the extension can be

installed to the McAfee system and configured via the ePO web interface. Configuration is explained in detail in the ePO plug-in documentation, so we will not go into that matter further. It is enough to say that our test environment with McAfee ePO 5.1 worked flawlessly.

Plug-in configuration on the CounterACT side was just as smooth as on the ePO side. Basically all you need to do is enter connection data such as IP addresses, ports and database credentials. The connection is established immediately and all ePO functionalities can be used within the framework of CounterACT policies.

The policies can be used to monitor the ePO database, identify clients which have not been communicating with the ePO server for a certain period of time, or see which clients are or are not managed by the ePO. It is also possible to access ePO events or view information on the NAC health status of the endpoints.

Integration of WSUS Server in LAN

It is particularly useful to integrate WSUS server in the LAN, given that they hold available updates and patches for Windows systems, which are necessary for automatically installing these updates. If the person administrator can not enter/specify WSUS environment settings in the configuration of the (CounterACT) HPS inspection engine under “windows updates”, ForeScout CounterACT will use the Microsoft update server as the source to enable patching. Since our test network already had a WSUS server, all we had to do was to enter server addresses and ports under "URL of WSUS server" and "URL of report server”. Clients managed by CounterACT were now downloading their updates from the LAN.

Conclusion

CounterACT has shown excellent functionality and intuitive operator guidance in our test. The solution offers very powerful policies, which can be used efficiently for full protection and proactive safeguarding of all services and components in company networks. Since it does not require an agent in the system to be secured, it can be smoothly integrated into existing networks.

We did not encounter any problems or unpleasant surprises while working with CounterACT in our test environment. We had even set up a rogue DHCP server just to see how CounterACT would deal with it. Soon we found out that DHCP clients were indeed unable to obtain an IP address as soon as we had switched off our authorised DHCP server. CounterACT blocked the DHCP server by claiming all available leases within less than a second and thereby blocking it for other systems. Problems with Windows systems and antivirus solutions, which had not been updated, were also handled fast and efficiently by CounterACT.

The greatest highlights were the captive portal and guest management functionality, and fast, simple and secure integration of external systems. CounterACT plug-ins for seamless interoperability with third-party solutions also proved very useful, as they enable administrators to create a central point for security management in their environment. Everyone working in IT dealing with security one way or form should at least take a look at this product. We award ForeScout CounterACT “IAIT Tested and Recommended”.

The dashboard gives a quick overview of the network status