HAKIN9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

NETWORK SECURITY

BUILDING
AN EFFECTIVE SECURITY STRATEGY

KEEPING
YOUR ENTERPRISE'S NETWORK SECURE

ENHANCING
YOUR NETWORK SECURITY TOOLS

Vol.7 No.09
Issue 09/2012(57) ISSN: 1733-7186

PLUS

AN INTERVIEW WITH ALEX KIRK FROM SOURCEFIRE
RIFEC REVIEW OF FORESCOUT TECHNOLOGY

ForeScout Technology Mobile Security Software

According to latest market statistics, smartphone and tablet devices will outnumber personal computers by 2013, becoming the most used devices for accessing Internet, processing and storing personal data.

RIFE
Research Institute of Forensic and E-Crime

Some of the newest models have the same features and hardware capabilities of a normal laptop, such as: fast CPU, large storage, microphone, high definition video camera and display, network connectivity and so on. For those who still ignore the potential of these devices, it is worth pointing out that they can also be used to access and manage: bank accounts, sensitive data and any other kind of personal information stored or processed within the device. This aspect makes these *Jewels of technology "the perfect target for hackers and malicious attackers". Mobile devices together with applications and Cloud services may represent a lethal cocktail of security threats, exposing users to a number of critical risks that may result in financial and reputational impact. More so, personal mobile devices are being brought into the workplace whether organizations like it or not, or are even prepared for them. The term "IT Consumerization"is top of mind as companies need to reckon with how to allow more secure use of these devices.

Mobile Communication Threats

There are a number of possible threats that a malicious source may attempt to exploit on the users or the vulnerable application and design weaknesses of the device.

Accidental or intentional Data leakage: a stolen or lost mobile device without effective protection, may easily grant access to data. The device may also be thrown away, or transferred to another user without removing sensitive data. And the device may be used at the enterprise to access network resources and company data.

Rooting: Power users may want to customize their mobile device by way of a root kit, which are easy to come by. In the process, the user can potentially eliminate or expose the mobile OS safeguards.

Phishing: Social Engineering techniques or malicious code may allow an attacker to collect and steal user credentials (i.e. passwords, card numbers, SMS or email) and personal identification data.

Network spoofing attacks: A malicious attacker creates a fake Wi-Fi access point to the network and users connect to it. The attacker intercepts the user communication and develops further attacks.

Spyware, Software surveillance, Dialer-ware/ Malware and other Viruses: Spyware and Surveillance software are malicious programs that allow an attacker to spy and control remotely the target machine. These types of programs are also used for data theft. A malicious source may attempt to steal money using hidden Dialer-ware that activates SMS services, or calling specific numbers.

There are malware designed to steal credit card numbers, login credentials for online banking and e-commerce.

One of the biggest areas of concern for mobile device security is the workplace.

Personal and corporate provided smartphones and tablets are increasingly accompanying or replacing laptops and PCs as a normal way for employees and contractors to perform their job. This has changed the very dynamic to address protection strategies and mechanisms. This is where ForeScout Technologies mobile security solutions mission starts.

ForeScout Security Platform

I am currently employed as IT Security Engineer and Risk Analyst for a large financial institution and as part of my roles and responsibilities I have to evaluate security software and solutions. Some of the tested Applications are well designed but practically not able to deliver (apart from the amazing description of inexistent features and capabilities, readable on the Marketing slides) the fundamental elements of quality, reliability and manageability, expected within a critical environment, where protection is a primary concern.

During the years I have developed an educated skepticism for the exciting promises and enchanting descriptions delivered during the initial phase of a product proposal and evaluation. Now I tend to approach reviews inspired by a religious zeal, using the proverbial incredulity of Saint Thomas.

I have been invited by HAKIN9 to review ForeScout Security products and surprisingly I must admit that there was much more to the product than the usual enchanting marketing slides.

Let me start by describing what ForeScout technology is, what they propose as Security solution and how Users and Organizations may benefit from ForeScout products.

ForeScout is a leading provider of automated security control solutions for enterprises and government organizations. During the Live Demonstration, a senior *sales engineer* (SE) at ForeScout gave me the opportunity to explore and evaluate some of most important applications and features provided by ForeScout. Specifically we've tested ForeScout CounterACT NAC (*Network Access Control*), ForeScout Mobile Security Module, ForeScout Mobile Integration Mobile (CounterACT plug-ins) and ForeScout MDM (a custom version of MaaS360, the full mobile device management system by Fiberlink).

CounterACT NAC is a product that allows an organization to control how all users, systems and devices, including mobile devices and VMs, access network resources and applications, gaining complete control over network without disrupting corporate and end-user productivity. This application can dynamically remediate violations, such as an unpatched system, out-of-date anti-virus, a misconfigured personal firewall, or de-activated encryption software, without operations intervention. Everything is contained within a single appliance that integrates into one's existing environment. CounterACT can also identify and provide network-based control mechanisms for managed and personal mobile devices.

The Test Lab

For this Review we have tried to equip our lab to be as close as possible to a typical production environment. The test area network had about 130 Servers remotely connected and running different Operating Systems versions such as: Microsoft Windows (Ultimate, Professional and Server 2008) and Linux (Ubuntu and Red Hat Enterprise). The network was divided in 8 different VLAN / Subnets, managed by 2 Routers + 3 smart Switches. Network is comprised with Servers running DNS, DHCP, LDAP/AD, email server and few more common services. Moreover we had 2 instances of Apache Web server, 2 Oracle instances + 2 SQL servers, 3 different Firewalls + IDS, 3 Antivirus Servers, 1 VMWare ESX, 1 Microsoft Hyper-V and few Android and Apple devices connected Wirelessly. On top of this I have my personal Laptop with a Linux BackTrack connected, just to investigate a little deeper.

Pre-installation steps

Prior to installing the software and related plugins, there needs a bit of planning. The appliance should be deployed in a network position where all the network devices can be reachable to ensure all connections to the network (local and/or remote) are monitored and controlled by the CounterACT solution

The installation

We have performed a full installation of CounterACT Virtual instance (CounterACT Appliance is available as a physical hardware component) on a normal Laptop with a Microsoft Windows 7 Ultimate running VMware ESX, without any specific hardware or software requirements (note that the system did not meet ForeScout's VM specifications). One of the first things I have noticed was the professionalism of ForeScout's SE. This is very meaningful to me, a remarkable quality element. SE's represent the Vendor presence and reputa-

tion on customer sites, thus it's extremely important to provide skilled and professional resources.

The second remarkable thing was regarding the installation process. Commonly these NAC applications are complex, with a number of pre and post-installation steps to perform. Well, CounterACT is an integrated Appliance, thus, there is no need to struggle with different components, agents deployment (note that agents are optional), Database installation or other time-consuming configuration settings. Network availability checks, some licensing work and we were ready to install the CounterACT Management Console. The console is built into the appliance and is the central management application used to view, manage and analyze the activity detected by one or more CounterACT Appliances. It's easy enough to open a browser connect to the appliance IPAddress and follow the screen instructions. (Other installation methods such as: CD, DVD are available). The first impressions I had of the Console GUI was definitely of friendly interface, intuitive and easy to manage. We've verified that all the critical connections that CounterACT uses to perform tasks, may benefit of SSL encryption.

The System Access Security

Access to the systems and protection Models are some of the first concerns for security experts in regard to the security of an application. Especially when sensitive information and critical management settings can be performed using a high level of permissions.

CounterACT login system can be fully integrated within the local or remote MS AD, RADIUS, TACACS, and any user-defined LDAP server. It is also possible to install and manage the user accounts locally using an integrated Database as credential

Figure 1. *CounterAct Login window*

repository. We decided to use our own Active Directory Service, thus we were authenticated and granted access, quickly, securely and successfully.

The software design provides a RBAC (Role Based Access Control) access control mechanism with a policy management server built into the appliance. This provides a good granularity over the permissions management and enables a wide operational control, enforcing the overall security (Figure 1).

Network Access Control

CounterACT NAC automatically started a thorough inspection over the entire Area Network (we report not much impact on Firewalls and IDS) it progressively started to populate the console with all the discovered objects creating a visual inventory. We have detected both active and passive scanning activities using Network monitoring and detection applications. Apparently, as long as the device has an IP address or is connected (Wireless or wired) to a device with an IP address it will be detected and presented within the inventory available on the management console. The only device that CounterACT was not able to detect was a completely passive Ethernet line tap (Figure 2).

The system automatically updates the existing online inventory once a device attempted to connect to the network. So the inventory templates (which can be customized) classifies all discovered devices and related details such as user, location, and configuration as discovered. Policy templates determine if the device should be allowed, limited or blocked from access on the network, or if some configuration element should be fixed based on what is discovered and the access policy. Using the built-in manageable policy and other features, CounterACT was able to identify and distinguish if the access that was requested and performed was from a "good" or a "bad" user/device. Guest management is also a part of the system but was not tested here. *ForeScout Mobile Plug-ins***.** The following step was to install and evaluate. The ForeScout Mobile Security Module extends CounterACT's level of control granularity with regards to Android and iOS security. It is comprised of an XML file added to the CounterACT system and a lightweight mobile app for Android (and iOS) devices. The Android application collects information for each device on which it is installed and reports this to the appliance. This allows determining the compliance of the Android device, restricting network access on the basis of that information, and sending automatic notifications to users to help them remediate policy violations and security problems,

such as password, encryption and application requirements. CounterACT can also send requests to the mobile device that is similar to that of MDM systems. We have done similarly for iOS Module on iPad and iPhone. With iOS, CounterACT uses Apple's live push and MDM services which is implemented through a Profile accepted by the user on their iOS device. This allows organizations to automatically find unmanaged corporate (or non-corporate) iOS devices and make them manageable/visible to the network security and policy compliance teams. Here too, a broad number of security features can be managed. There is also plug-in also allows for interoperability with other MDM systems – Fiberlink was tested. *ForeScout MDM (Mobile Device Management) MaaS360 by Fiberlink***.** During the review, we have noticed that this was looking as an external product, then the SE gave us some background information regarding their ForeScout MDM solution. This product is part of a partnership with MDM SaaS developer Fiberlink that gave life to a fully integrated MDM and network access control (NAC) solution. MDM incorporates a customized version of Fiberlink's MaaS360, a cloud-based management system for smartphones and tablets, working with client-side software that installs as a profile on IOS devices and as a mobile agent on Android through a self-guided process. The software seems to be also available for BlackBerry and other platforms. CounterACT has a connector to the MDM which allows the NAC system to gain a much greater degree of visibility and control of all mobile devices controlled by the MDM. ForeScout MDM is cloud-based and offers lifecycle management from enrollment to securing device data and applications, providing the ability to remotely locate and wipe. While ForeScout MDM managed MDM controlled devices, CounterACT can apply network-level controls to unmanaged and MDM connected devices. It detects in real-time unidentified devices attempting to enter the network, and it can automatically implement controls to block, register as guest, push into an HTML for virtual desktop enrollment, or enroll via MDM on-demand with full device inspection and agent deployment. The benefit being fourfold: controlling unmanaged devices, enrolling devices into MDM, requesting the MDM to check the security profile of the device on network entry, and to control what network resources an MDM-managed device can access (Figure 3).

The screenshot above shows the Console GUI we have installed on the test machine. We have immediately familiarized with the available menus, trying to run and activate some of the integrated options and Tools.

Testing phase

Using both Policy base and Manual processes, we went through a number of tests, on IPad and Android mobile devices. We've evaluated some of the most critical scenarios as well as the effectiveness and manageability of CounterACT with ForeScout Mobile and ForeScout MDM (Maas 360). Non-

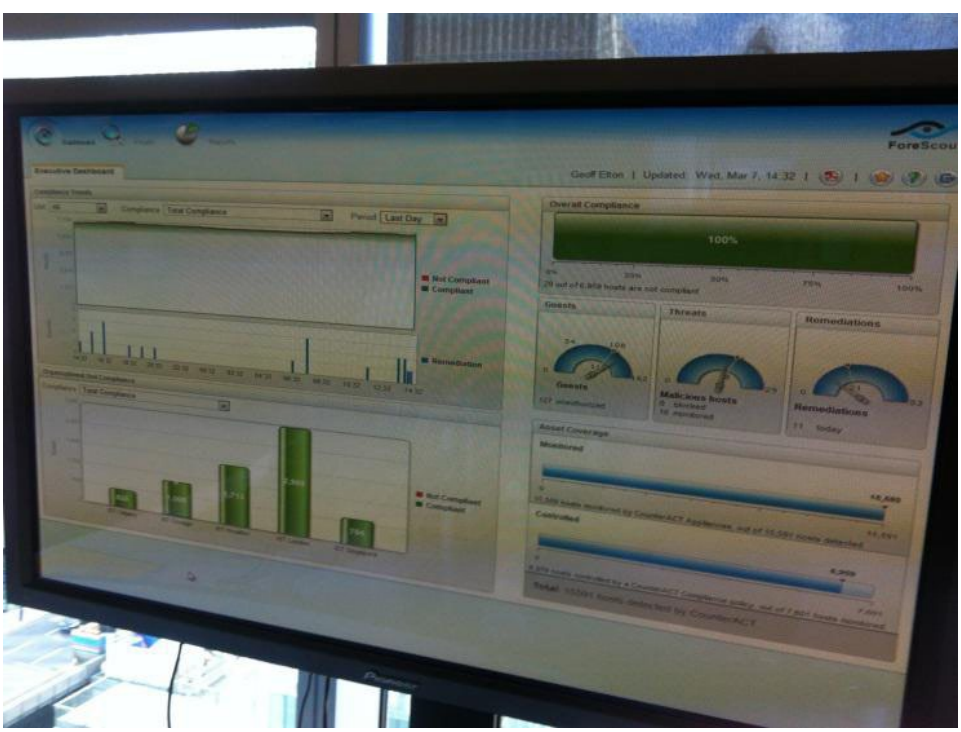

Figure 2. *Device detection*

corporate, external or personal device connection over internal protected networks is extremely dangerous and should be monitored and restricted. CounterACT NAC + MDM provides this functionality.

Automated enrollment
A device was connected to test network and checked for manageability by CounterACT. The device was prompted to install a profile, demonstrating the streamlined process of managing the device OS.

NAC – hijack and request network credentials
An initial test was performed trying to connect a device to our test network via Wi-Fi, attempting to access the Internet. The device was hijacked and requested to authenticate against the access control system, demonstrating the ability of the software to control network access by requiring non-corporate devices to authenticate.

- The device joined Wireless Network
- Matched "Network Authentication" Policy and an HTTP Authentication Actions committed to the endpoint.
- Received the HTTP Authentication prompt and logs using demo/demo credentials.
- After the successful authentication, network access was provided.

Using the pre-configured policy, the software successfully Hijack the BYOD and non-managed devices and apply the corrective action.

Testing Policy – Camera disable
We've created a rule to disable camera on manageable device. Joining the test network, the device was firstly checked for manageability by CounterACT and subsequently was prompted to install a profile.

The policy rule forced the device to disabled the camera, demonstrating the ability to interact with the mobile device and apply restrictions to applications.

We've successfully tested the same scenario running the process manually.

Adding web clip to the mobile device
On the same device was pushed a web clip linking an icon on the home screen to the ForeScout web site. The device matched an iOS Manageable Non-Compliant sub rule and an action adding a policy to deploy a web clip was applied. As matter of fact, the device received a new icon on the home screen linking to *www.ForeScout.com*. The same process was successfully performed manually.

Device access configuration management – password
A manageable device was required to utilize a screen lock password, to demonstrate the abil-

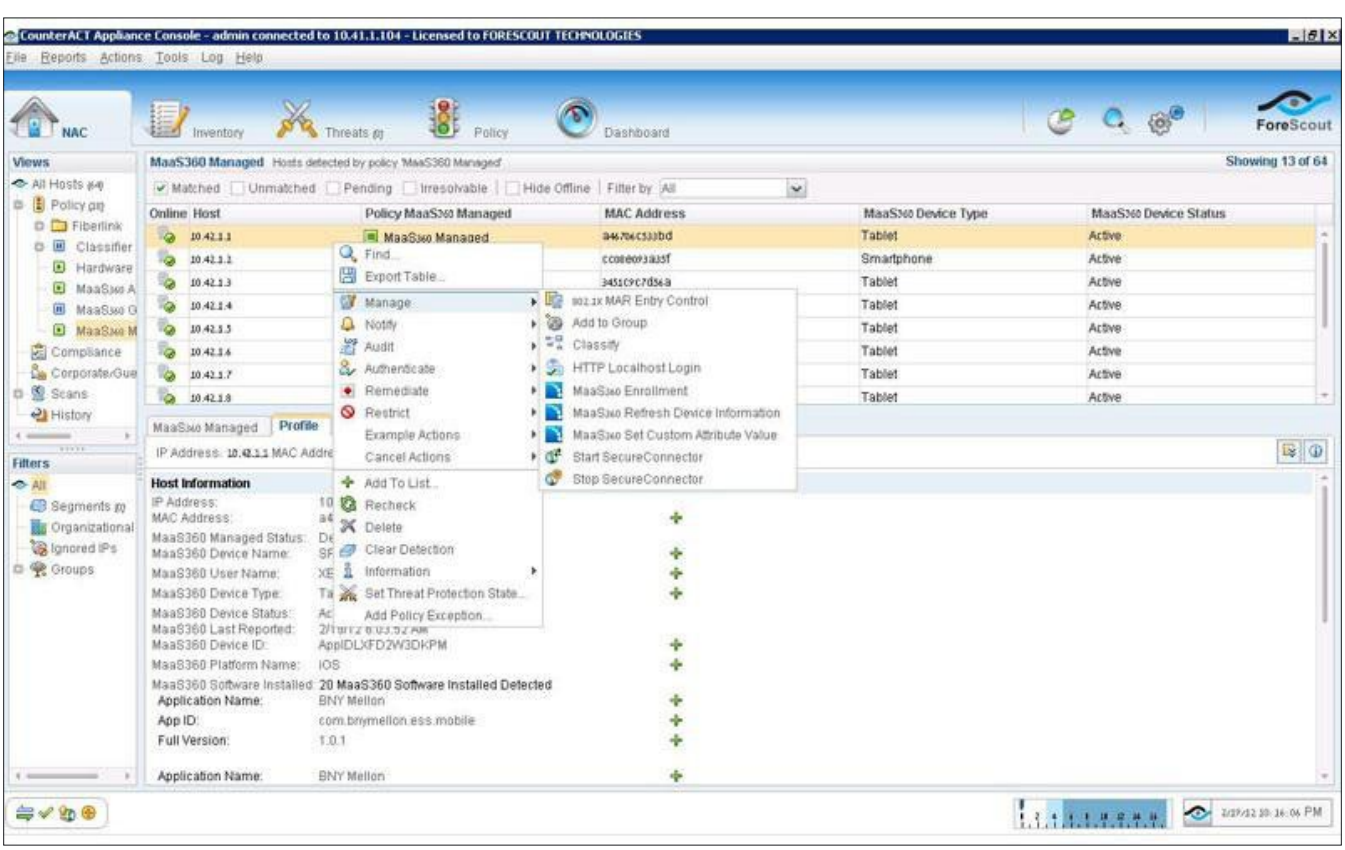

Figure 3. *Managing in CounterAct*

ity to enforce security configuration. The device matched an OS Manageable Non-Compliant sub rule and the action to add a policy to enforce a screen lock was applied. We have verified that the device prompted to choose a password. Based on the same principle but adding some new policy we could also successfully create a strong password policy and application restriction.

Selective Wipe
We tried to remove the profile of the device from CounterACT console. This was blocking the device from any further access and action, demonstrating the effectiveness of the policy and profile configuration. We could evaluate that policy and profiles are customizable by users and groups, providing a large number of configurable permission and access type.

Using Virtual Firewall to quarantine non-compliant devices
We have applied a CounterACT virtual firewall rule on a device with access granted to verify the firewall restriction effectiveness. The device dropped out of network connectivity and Internet access. We have then determined how Virtual Firewall was committing such actions. Apparently, VFirewall uses packet injection and TCP reset mechanism to dynamically control network traffic. Essentially, using a TCP reset mechanisms, which send the RESET to the source after the data is already on the wire and sending the RESET to the destination after the first SYN, tearing down the connection before the handshake completes. We've tested trying to reset a TCP connection of a joined device. As result the device lost the connectivity. Other enforcement (see ACL) is available but this method enables enforcement without any infrastructure changes that for some organizations would be compelling.

Appendix 1

Materials/Documents provided by ForeScout

- Overview of NAC (by EMA analyst)
- Overview of CounterACTplatform
- Overview of market (by Frost and Sullivan)
- ForeScout CounterACT datasheet
- ForeScout Mobile datasheet (this is the mobile security plug-in)
- 451Research report on ForeScout Mobile

PDF
- FS-Abridged-NAC-report.pdf
- ForeScoutMobile_the451.com_-2.pdf
- ForeScout-Mobile-Datasheet.pdf
- Tolly212105ForeScoutComparativeNAC.pdf
- FS_Overview-Dec2011-FINAL.pdf
- EMA_AchievingNACResults.pdf
- FSCounterACT_Eval_Guide_2011.pdf
- ComputerTechnologyReview-CounterACT-Aug2011-web.pdf

Video
https://www.youtube.com/watch?v=QxMsU7lt5sc

ACL enforcement
We have enabled and tested ACL Enforcement on: Firewall, Router and Switches within the test network. We have configured a specific ACL rule to block access to a specific port. We have then changed the ACL settings to roll back and to perform access using the same port. All the tested configurations were successfully verified.

Conclusions
We have spent many hours in our test Lab going through the extensive range of checks and verifications on ForeScout products, we have also tried to find potential bug or gaps on CounterACT to verify how easy it could be for an expert user to exploit a vulnerability on CounterACT NAC and ForeScout MDM, but we failed.

In our opinion the integration of CounterACT NAC, its Mobile add-on modules and FS MDM, had demonstrated to be a valid and effective end-to-end Security solution, addressing network access and mobile security concerns and delivering total control over the managed network and devices using:

- Detection
- Monitoring
- Protection
- Administration
- Remediation

We believe that ForeScout products are able to satisfy the network access and endpoint security exigencies of corporate and governments but at same time the increasing request of mobile security, triggered by the wide use of smartphones and tablets.

ABOUT THE EVALUATOR
SEMBIANTE MASSIMILIANO
IT Sec&Risk Eng. at UBS Bank
M.Sc. Computer Security
Can be reached at: msembiante@rifec.com