



ForeScout

NETWORK ACCESS. CONTROLLED.™

NETWORK ACCESS. CONTROLLED.™

ForeScout Security Assessment Service

Giving you the knowledge

ForeScout's customers, worldwide, all desire the same common theme :

Visibility – Our customers realise the importance of knowing what's out there and who is connecting to their network. With the knowledge comes the power to manage effectively and precisely.

Why would you use this service ?

Here are some examples why customers use this service :

- 1) A simple internal audit - because you want a snapshot of what's out there.
- 2) Compliance – A demand to comply with internal or external compliance such as PCI, SOX etc.
- 3) Post attack assessment – You may have experienced an issue / attack and want to be sure issues have been resolved and that certain security measures have been put in place and are active.

What do I need to do ?

- 1) Complete the pre-assessment application form. This tells us about your environment, and what you want to achieve from the service.
- 2) Discuss with us on the phone. We will review the details with you on the phone with a ForeScout qualified engineer prior to any commitment from you.
- 3) Commitment. Once you are happy with the customization discussed, you commit to the service and we set dates. Please note that once both parties have agreed on the scope of work, it will not change.
- 4) Network configuration – You will be required to setup your core switches prior to the arrival of the engineer, but this is a straight forward process and we can guide you if required.
- 5) Assist the engineer – You will need to provide some technical advice about your environment to the engineer when he is on site performing the installation.
- 6) Attend the follow up calls, 1 week and 2 or 4 weeks later.

For more information please contact Darren Parker
at Cohort Technology

Email: dparker@cohorttechnology.com

Tel: 0845 094 8828

The Service

ForeScout's security assessment service is based on our technology called CounterACT. CounterACT is an unobtrusive, out of band appliance that monitors the traffic on your network to determine who and what is connected. Once we are aware of a connection, we have the capability to report on :

- 1) What the device is
- 2) Who's using it
- 3) What software is installed (and running)
- 4) What settings are enabled (or disabled)
- 5) Devices that are attempting to spread malware

We will discuss with you the reports that you require, and these are presented to you at the end of the assessment (see reverse).

What are the time scales ?

- 1) Implementation is straight forward and usually takes no more than half a day.
- 2) A telephone review is set for approx 1 week after installation to check that the unit is reporting as desired.
- 3) After 2 weeks the final reports are generated and the unit is removed from site.

What does it cost ?

The cost for a 2 week assessment including 5 reports is £1000 + expenses for shipment of goods and engineer travel costs.

A 2 week extension is an additional £500.

Additional reports can be added at £150 per 5 additional reports.



ForeScout

NETWORK ACCESS. CONTROLLED.™

NETWORK ACCESS. CONTROLLED.™

Checklist of Reports

Here is the list of standard reports, however, it is possible to create custom policies, please speak to us if you think you have a requirement.

Essentially customers look for :

- 1) Things they want to see e.g. Anti Virus running/up to date
- 2) Things they don't want to see e.g. rogue wireless access points

Please indicate which reports you require

- | | |
|---|--|
| <input type="checkbox"/> Rogue or unauthorised devices | Non corporate assets including PC, wireless AP |
| <input type="checkbox"/> Anti Virus applications | Which ones and are they running ? |
| <input type="checkbox"/> Microsoft patching | Are these up to date ? |
| <input type="checkbox"/> Peer to Peer applications | Do you want to detect if these exist ? |
| <input type="checkbox"/> Instant Messaging applications | Do you want to detect if these exist ? |
| <input type="checkbox"/> Server Vulnerabilities | Detect and report |
| <input type="checkbox"/> Removable devices | Such as USB, iPhone |
| <input type="checkbox"/> Personal firewall applications | Should these be running ? |
| <input type="checkbox"/> Malicious hosts | Devices attempting to spread malware |
| <input type="checkbox"/> Suspicious access | Users that are access resources they should not |
| <input type="checkbox"/> Dual homed devices | Devices that are connected via wire and wireless simultaneously |
| <input type="checkbox"/> Asset list | A report of what devices have been detected on the network |
| <input type="checkbox"/> User list | A report of users that have accessed the network |
| <input type="checkbox"/> Application list | A report of what applications are installed |
| <input type="checkbox"/> PCI Reports | We have a list of policies that cover PCI compliance – this takes your 5 policy allocation |