



Technology Note

# CounterACT:

Powerful, Automated Network Protection  
*Inside and Out*



## Introduction

*When the recent Conficker outbreak wreaked havoc upon Windows-based LANs in enterprises worldwide, CounterACT customers called in to say: "our network is perfectly safe – CounterACT's automatic zero-day threat prevention provided us with the 24/7/365 protection we have come to expect and rely on!"*

Conficker (aka Downup, Downadup and Kido) is an aggressive worm that targets Windows-based systems. It's been estimated that the bug infected over 10 million PCs in just a few short weeks (over a million in a single 24-hour period) ... making it one of the most prolific, dangerous and widespread infections in recent times.

Anyone using a Windows-based system was cautioned to verify that their system was free of the Conficker worm and was running the latest, patched version of Microsoft Windows.

CounterACT users, of course, had the peace of mind that their systems were automatically protected: here's why.

### **CounterACT: Powerful, Automated Threat Protection against Conficker**

CounterACT offers a powerful, automated 24/7/365 network solution for preventing the infection and spread of the Conficker worm. It both shields uninfected systems and remediates infected hosts, offering network users these security benefits:

- **Prevention & Protection** – CounterACT ensures that the MS-Update service is always running on every Windows device. It also blocks Conficker infection using strong, built-in threat prevention technology.
- **Enforcement & Remediation** – CounterACT ensures other IT protection tools ( anti-virus, anti-spyware, etc.) are working and "always on" and automatically remediates infected hosts.
- **Monitoring & Reporting** – CounterACT continuously monitors endpoint security posture and maintains a clean, secure network. It also records all remediation/enforcement actions taken against Conficker on malicious and/or infected hosts.

#### **How the Conficker Worm Works**

- The worm exploits a bug in the Windows Server service used by Windows 2000, Windows XP, Windows Vista, Windows Server 2003 and Windows Server 2008. It self-replicates as the downloadable library file %System%\[RANDOM FILE NAME].dll, deletes any user-created System Restore points and creates the service, netsvcs.
- The worm then creates a registry entry and connects to three URLs to obtain the IP address of the compromised computer: <http://www.getmyip.org>, <http://getmyip.co.uk>, <http://checkip.dyndns.org>.
- It then downloads and executes a file, creates an http server on the compromised computer on a random port, sends this URL as part of its payload to remote computers, then connects back to this URL to download the worm. In this way, each exploited computer begins to spread the worm without needing to re-download it from a web location.
- The worm then connects to a UPnP router, opens the http port, then attempts to locate the network device registered as the Internet gateway and opens the previously mentioned random port to allow access to the compromised computer from external networks. The worm then attempts to download a data file. It spreads by exploiting the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874).
- Finally, the worm attempts to contact the following sites to obtain the current date: <http://www.w3.org>, <http://www.ask.com>, <http://www.msn.com>, <http://www.yahoo.com>, <http://www.google.com>, <http://www.baidu.com>. It uses the date information to generate a list of domain names. The worm then contacts these domains in an attempt to download additional files onto the compromised computer.

## How to Use CounterACT to Protect vs. the Conficker Worm

Take the following steps to protect your corporate network against the Conficker worm.

### **ONE** Use CounterACT's Ready-to-deploy Policy Templates to Speed Endpoint Protection

- **The Windows Update Compliance Policy** ensures endpoints are patched with MS08-067.
- **The Microsoft Update Policy** ensures the Microsoft Update service is running on all endpoints.
- **The Anti-Virus Compliance Policy** ensures that an anti-virus application is installed, running and up-to-date on all endpoints.
- **The USB Device Compliance Policy** - detects/blocks all connected USB devices or all devices that are not allowed.

### **TWO** Track Corporate Compliance via Comprehensive Reports

### **THREE** Apply Extra Threat Protection

- **CounterACT's IPS/Threat Protection Policy** prevents worms from re-entering /spreading inside the network.

### **FOUR** Ensure that the Microsoft Update Service is Running

- **CounterACT also helps** automate (enforces) the Microsoft update service.

## ONE Deploy Endpoint Protection Policies

CounterACT is delivered with ready-to-deploy *NAC Compliance templates* that can be used to create and deploy policies in five easy steps:

1. Open the CounterACT Console and select the **Compliance** icon from the Console Toolbar.
2. The **NAC Policy Wizard>Compliance** folder opens.
3. Select the following policy templates and configure them by following the on screen instructions:
  - Windows Update Compliance
  - Anti-Virus Compliance
  - USB Device Compliance
  - Malicious Hosts
4. The policies you create appear in the NAC Policy manager.
5. Select the **Apply** button.

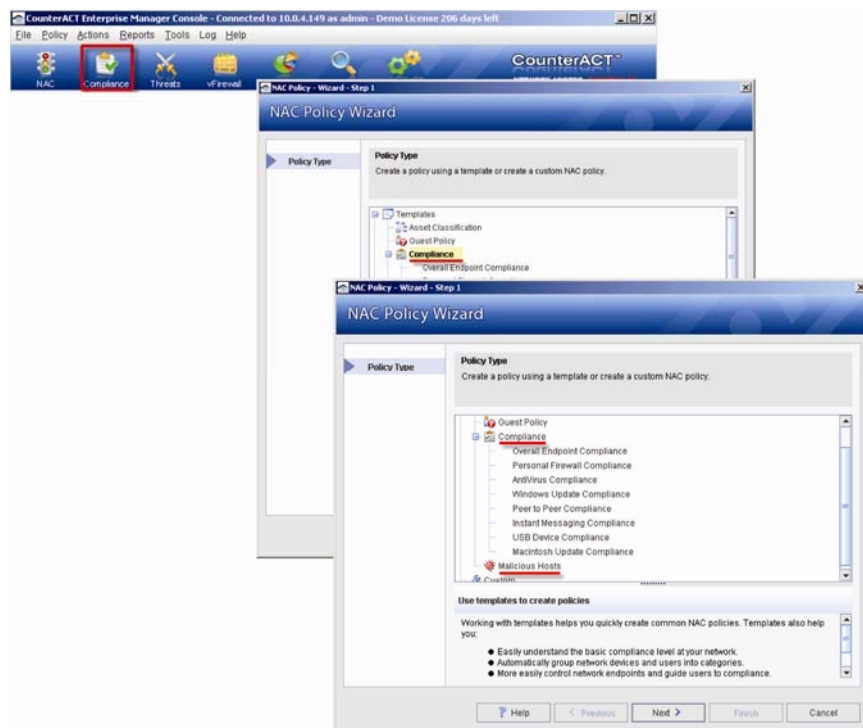


Figure 1: Deploy Endpoint Protection Policies.

## **TWO** Track Corporate Compliance to Policies via Comprehensive Reports

CounterACT offers easy-to-build reports that help you track corporate compliance to policies. The reports can be tailored to include the exact level of information you require, and can generate in five easy steps:

1. Select the **Reports** icon from the Console toolbar.
2. Select the **NAC Policies Compliance Details** link.
3. Define reports settings in the page that opens.
4. In the **2. Scope >Select Policy** section, choose one of the policies you created.
5. Scroll down and generate the report.

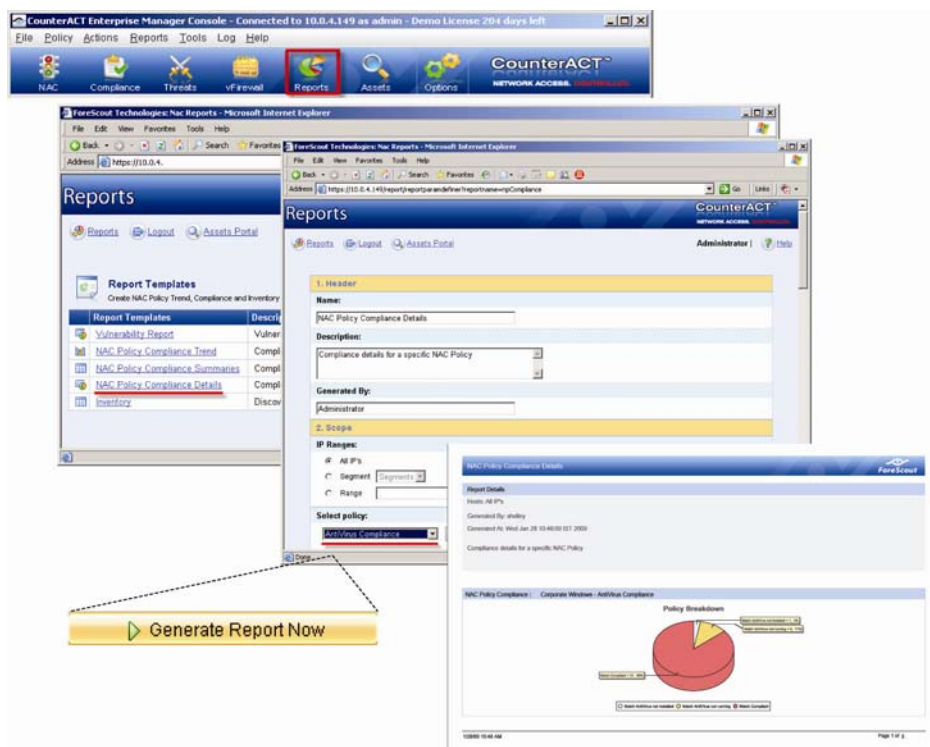


Figure 2: Generate the Compliance Report.

## THREE Apply Extra Threat Protection

For additional protection, you can deploy CounterACT's IPS/Threat Protection Policy as follows:

1. Select the **Threats** icon from the **Console** toolbar (for version 6.3.2 and above) For versions 6.3.1 and below select the **IPS Manager** icon).
2. The Threat Protection Policy pane opens.
3. Select **Port Block** from the **Action on Bite** dropdown menu in the Network Worm Policy section.
4. Select **Host Block** from the **Action on Email Worm** dropdown menu in the Email Worm Policy section.
5. Select **Customize**. The **Customize, Scan** tab opens.
6. Select the **Login** type and verify that it is enabled.
7. Select the **Details** button and verify that the **Password Scan** and **User Scan** are enabled.
8. Select **OK** and **Close**.

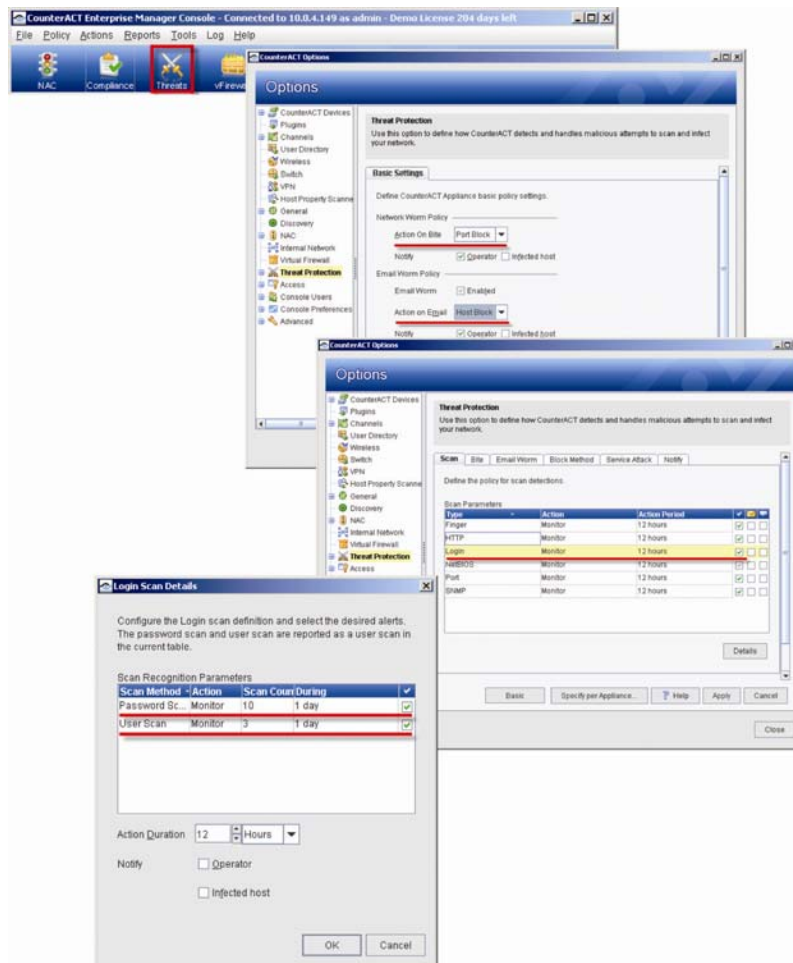


Figure 3: Deploy a Threat Protection Policy.

## FOUR Schedule/Enforce the Microsoft Update Service

To ensure the Microsoft Update service is running regularly:

1. Select the **Compliance** icon from the Console Toolbar.
2. The NAC Policy Wizard opens. Navigate to the **Custom** folder.
3. Select **Next**. The Name pane opens.
4. Add a policy name and description and select **Next**. The IP Address Range dialog box opens.
5. Define the range of IP addresses to be inspected for this policy. Select **Ok** and then select **Next**. The Main Rule dialog box opens.
6. Select the **Add** button from the Condition section. The Condition dialog box opens.
7. Navigate to the **Windows OS** folder and then select **Service Running**.
8. Select the **Does not meet the following criteria:** radio button.
9. Select the **Matches** option from the drop down box and type in *Automatic Update* in the field that follows.
10. Select **Ok**. The Main Rule dialog box reopens.
11. Select **Add** from the Actions section.
12. Navigate to the **Remediate** folder and then select the **Run Script on Windows** action.
13. Enter the following command in the **Command or Script** field: `net start wuau serv.`
14. Select **Ok**. The Main Rule dialog box reopens.
15. Select **Finish**. The policy appears in the NAC Policy Manager.
16. Select **Apply**.

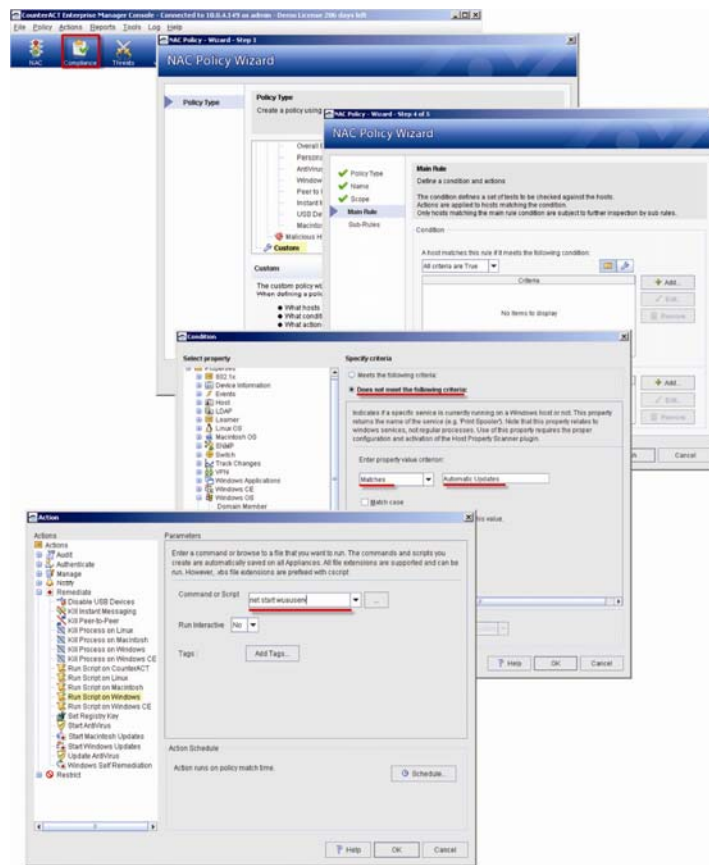


Figure 4: Ensure Microsoft Update Service is Running.