

## Automated Quarantine Engine

### Automatic detection and containment of viruses

**Do you long for the time when the biggest demand on your IT department was from users who needed help retrieving forgotten passwords?**

**While IT life may never be quite that simple again, Alcatel's Automated Quarantine Engine (AQE) can help you eliminate your biggest headache – security issues from worms and viruses. Alcatel's AQE identifies and locates the infected network devices and automatically creates the policies necessary to quarantine the infected devices – and does it in seconds without impact on other devices!**

**Sound expensive? Actually, it will save you money because:**

- **There's no additional hardware required on Alcatel switches**
- **There's no additional software required on Alcatel switches**
- **It's fully interoperable with other vendor switches**
- **It cuts network downtime keeping employees up and running**

So how does this work? A good analogy is the travel industry's check-in process. A few years ago when you arrived at an airport, you would get in a check-in line that wrapped endlessly because ticketing and check-in was a labor and time intensive operation. By offloading labor to an automated check-in process, staffing costs are reduced and passenger waiting time is reduced.

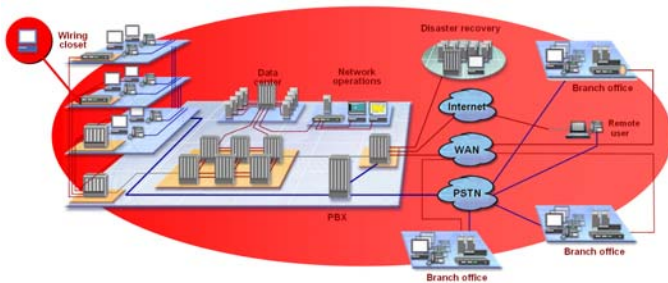
Today, travelers walk up to an airline's kiosk, insert an identification card such as a driver's license, select a seat, and get a boarding pass in less than a minute and are on their way. Problem passengers are isolated and required to check-in via an agent saving the business money, and most customers a great deal of time. Your network security should be this automated and fast!

The network is the heart of a defense system. Security appliances are good, but inadequate since they are too costly to be widely deployed, most of them only detect, and those that can act only act locally. Only the network can act everywhere, and in particular, at the source of an attack. Cooperation of appliances and the network is the key – appliances detect or act locally while the network acts and punishes at the source of the problem.

## Enterprise security today

Most enterprise networks constantly struggle with new security threats from outside as well as within. All it takes is one contaminated device with a virus or worm to infect the network within minutes and take it down for hours or days, tying up IT resources and frustrating users.

For example, the IT staff works on identifying the signature and locates the user manually with available tools. Once identified, the user is denied network access, doesn't understand why so he moves to another port, continuing to spread the virus. Again, the IT staff tries to contain the virus and manually loads patches to infected computers, playing a never-ending game of catch-up. Add to this mix wireless users and your staff stays busy putting out infections and trying to prevent unauthorized access instead of focusing on projects that are more productive.



*Typical virus containment solution*

## Automated Quarantine Engine

To address these security issues, Alcatel offers the Automated Quarantine Engine (AQE). AQE is a combination of hardware and software, which provides an automated mechanism that denies access to an endpoint that is not secure to the network infrastructure, including wireless devices. The AQE receives alerts from security appliances or LAN switches and acts to quarantine network devices that threaten the IT infrastructure or have violated any security policy. Violations such as network level types of attack as detected by Alcatel switches and/or application types of attacks as identified by intrusion detection system (IDS) appliances. These policies can be any or a combination of the following:

- **Virus related signatures (traffic patterns)**
- **Blocked web sites**
- **Hacker attempts (traffic indicating an attempt to launch an attack)**
- **Violation of any policies that have been set up in the IDS**

AQE is designed to push the front line of security out to the edge of the network to find insecure network devices before they can negatively affect the network and isolate the infected machines at the point of entry, the edge port.

For example, the following diagram shows an infected station attacking a sever (e.g., port scan). IDS identifies the attack and source of attack. IDS then notifies AQE of the type of attack, and the source of the attack. The user is moved into a quarantine VLAN or denied network access. Quarantine policies are updated and applied to the

# Automated Quarantine Engine



entire Alcatel network infrastructure so that the user cannot get access to any sensitive resources even if he moves and changes his physical port. Once in the quarantine area, the infected device still maintains network connectivity for remote remediation. After remediation is completed, the AQE will let the network administrator move the “cleaned” device out of quarantine.

## The benefits of AQE

The AQE receives input from an intrusion detection system (IDS), automatically locates the source of the attack on the network, and then automatically creates the quarantine policy to be applied at the edge of the network, the point of entry for the attack. The automatic process reduces the need to have a network engineer create and apply a policy (VLAN, ACL) to manage network access, which minimizes the need for manual configuration and application of network user policies.

Furthermore, AQE does not require any additional network software or hardware beyond the basic Alcatel switch from a network infrastructure viewpoint, it is fully interoperable with other vendors' switches, and is flexible to accommodate a wide range of IDSs, protecting the customer's investment.

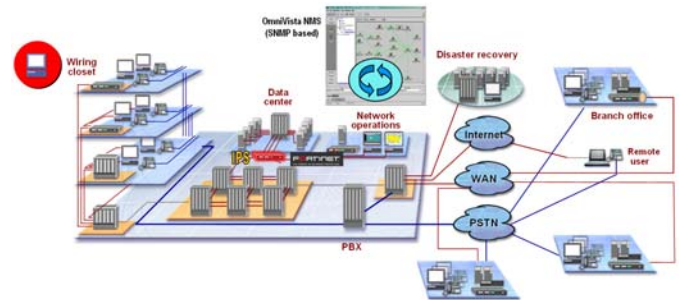
Once implemented AQE reduces operating expenses, automates configuration of edge-port security parameters, works on wired and wireless infrastructure, and implements quarantine policies throughout the network edge providing secure user mobility with minimal configuration changes.

## Why Alcatel?

Ask your current vendor if they can automatically contain a rouge, infected, or misbehaving device then isolate it. Ask if they allow for the offending device to keep a network connection for remote remediation. Ask if they keep offending users in quarantine when they try to connect somewhere else in the network or if they leave it to hang until someone from IT can get around to manually cleaning and inspecting the offending device.

Only Alcatel provides policy-based, network-wide responses to security attacks enabling secure mobility over its network infrastructure. And, just like self-help kiosks in airports, it allows users to be mobile while being able to identify the security threats. The dangerous users are segregated to areas where they can remediate and resume their regular activities.”

To find out more about how Alcatel's AQE can automatically protect your network, contact your local Alcatel representative or visit: [www.alcatel.com/enterprise](http://www.alcatel.com/enterprise)



*Alcatel's trusted network intrusion prevention through network response.*

**Alcatel**

26801 West Agoura Road  
Calabasas, CA 91301 USA

**Contact Center**

(800) 995-2612 US/Canada  
(818) 880-3500 Outside US

[www.alcatel.com/enterprise](http://www.alcatel.com/enterprise)

Product specifications contained in this document are subject to change without notice. Contact your local Alcatel representative for the most current information. Copyright © 2004 Alcatel Internetworking, Inc. All rights reserved. This document may not be reproduced in whole or in part without the expressed written permission of Alcatel Internetworking, Inc. Alcatel® and the Alcatel logo are registered trademarks of Alcatel. All other trademarks are the property of their respective owners.

P/N 031551-00. 11/04

