Testing Endpoint Security

Rodney Thayer
Mandy Andress

Who we are...

- Independent testers
- Mandy Andress: Security consultant with a background in Enterprise Security (Dir. Security, etc.); book author; Author/tester for Network World (and other pubs)
- Rodney Thayer: Security Analyst, exploit researcher, network security architect, Author/tester for Network World

The Testing Process

- It's secret and mystical – NOT
- Imagine what you'd do in your own test lab to show your management
- Try to use good science and good engineering
- Small but reality-based sample configurations
- Bounded time and budget for testing (just like in the real world)

What is “Endpoint Security”?

Endpoint Security: Background

- Traditionally, the network had an edge, and an interior
- There were firewalls at the edge (if you were careful)
- Nodes were Servers or Desktops
- A small number of mobile (laptop) machines
- A small amount of remote (VPN) access

Endpoint Security: Today

- 75% [1] of client machines are mobile
- Firewalls, VPN's of 2 or 3 flavors
- Web access
- Significant amount of Enterprise work happens with machines not within a defended perimiter

[1] (That's a guess.)

Today's Network Edge

- The mobile machines are just as much edge devices as the firewall
- Modern attack methods mean that even desktops are effectively part of the edge
- Defense of the edge means defense of the end systems (laptops and desktops)

What's NOT “Endpoint Security”

- Cable locks and other physical security tools
- Disk encryption tools
- Non-network oriented security tools (Anti-virus)
- Application security tools (anti-spam)

How do Enterprises look at Endpoint Security?

Enterprise Requirements

- Must be centrally managed
- Defense of the endpoint system is a goal
- Defense of the network is a goal
- Practical issues: budget, how many add-on tools per seat do I need?, something else to update

Enterprise Issues

- Must consider how many times each machine will need an extra package loaded
- Must consider what threats the end systems could bring into the enterprise
- Watertight doors: saving the enterpise net is worth sacrificing an individual system

How do Attackers look at Endpoint Security?

Attacking the Endpoint: Objectives

- Denial of service
- Access to the Enterprise network
- Theft of data
- Sneaking illicit software onto the endpoint system
- Zombie conscription

Attacking the Endpoint: Targets

- The endpoint sytem itself
- The Endpoint Security system
- The Enterprise network
- The entire public Internet

Attacking the Endpoint: Methods

- Attack endpoint systems that you can reach and which have no intervening defenses
- Worms across workgroups
- Attack a laptop when it's in an Internet Cafe
- Attack a laptop when it's on a home network
- Email and other application attack vectors
- Attack the Endpoint Security server
- Custom virii

The Endpoint Security Marketplace

Solution Categories

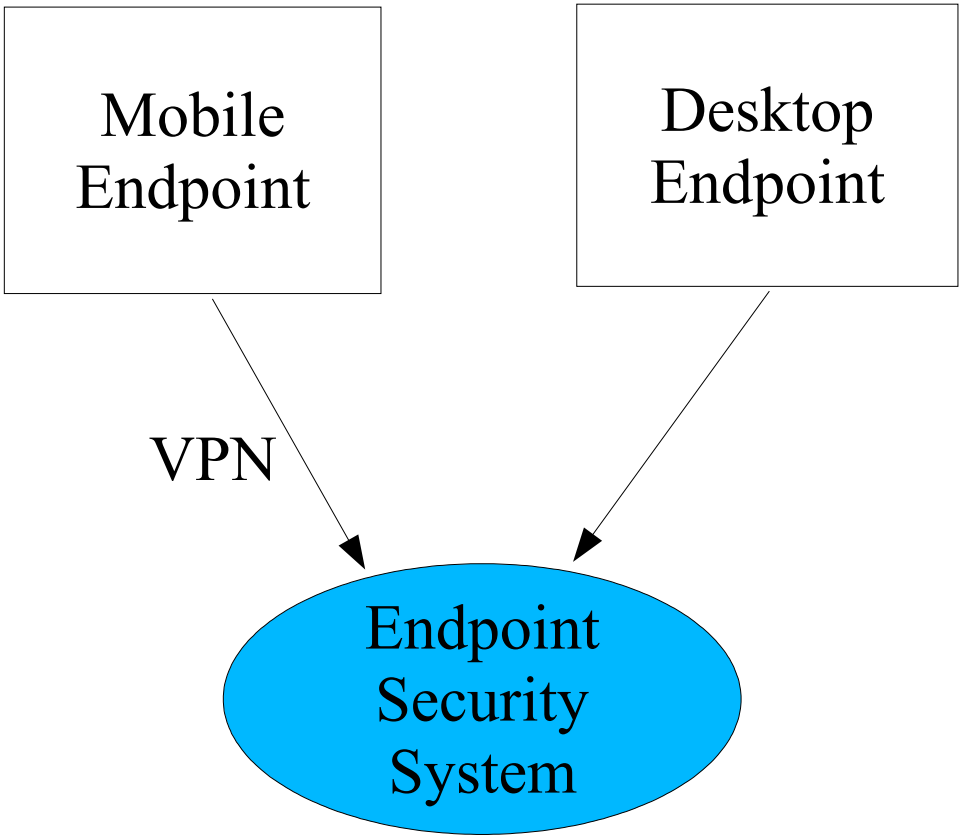
- Endpoint firewall
- Endpoint IDS
- Endpoint IPS
- Execution containment
- Whitelist / Blacklist
- Anti-virus

Deployment Scenarios

Requirements

- Central management
- Reporting capability
- External event logging if possible
- Integration with network management infrastructure
- Integration with Security Infrastructure
- Integration with Patch Management infrastructure if possible

Sample Network (for testing)



Managing Endpoint Security

- “First do no harm” - compatability with other software on the endpoint
- Goal is to reduce or eliminate attacks
- Visibility into what's going on at the perimiter
- Defense of the network
- Defense of the endpoint system

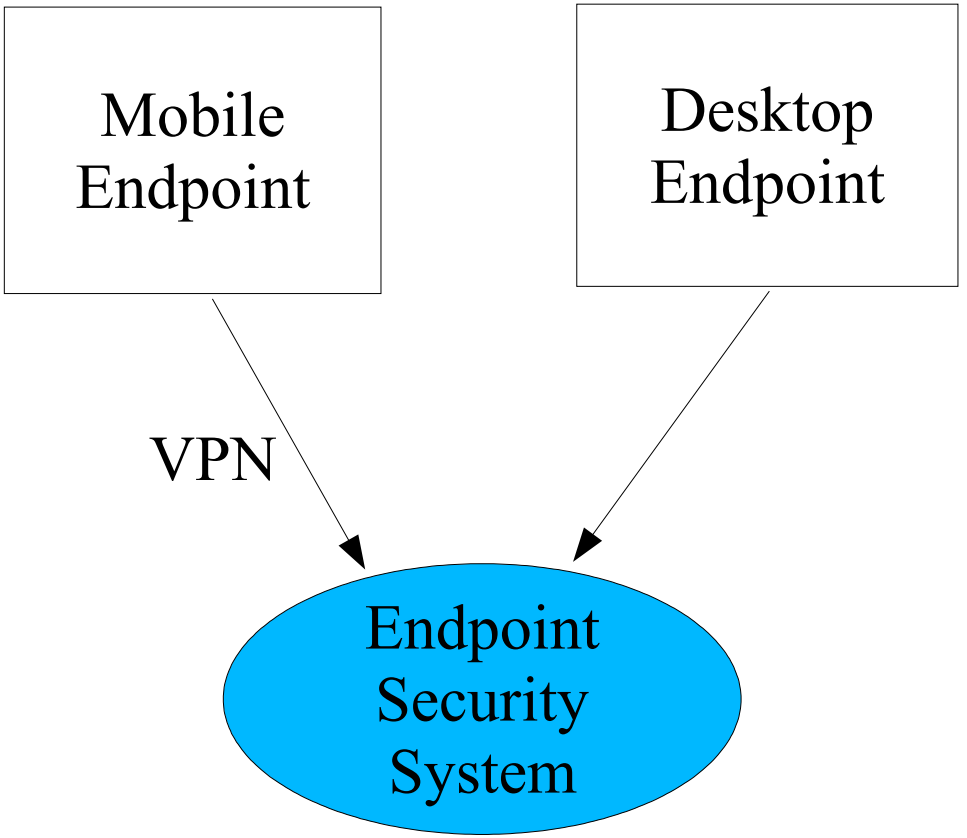
How the Test was done

Process

- “the out of box experience”
- Standard installation, except we *really* do read the manuals
- Minimal acceptance test
- Execute the test plan
- Evaluate the results

Attacking the Endpoint

Sample Network (target analysis)



Attack Categories

- Get some software onto the endpoint
- Get past the enforcement mechanism
- Attack the Endpoint Security server
- Forcefully remove the endpoint security component

Attack: Insert Rogue Software

- Try loading netcat
- No “install”, no registry
- Try tweaking it so the (MD5) hash is different
- Results: This never worked

Attack: Bypass mechanism

- Classic network attacks (Nessus, NMAP, Metasploit)
- Suppress reporting to management server
- Results: some solutions fail to detect this

Attack: Management Server

- Go after the Endpoint Security management server
- Justification is – it's in the infrastructure, juicy target
- Use standard network traffic as a basis, attack the protocol
- Attack using standard protocols
- Results: didn't work, looked promising
- Note: GPL (Legal/administrative attack) also possible

Attack: Forced removal of Endpoint Component

- "Rip out the client"
- Requires finding the client
- With or without reboot required
- With or without cover traffic to management server
- Results: worked in several cases

Conclusions

Conclusions - Results

- I don't like Whitelists
- It's too easy to rip out the client
- What if a mobile (or stationary) machine goes missing?
- The servers make good targets
- Where's the firewall/IDS? Shouldn't there be a firewall? What about IDS/IPS?
- How many products per seat must you deploy?

References

- The article: http://www.networkworld.com/reviews/2004/0920rev.html
- Mandy Andress: http://www.arcsec.com
- Rodney Thayer: http://www.canola-jones.com