
ZONE
LABS
The Leading Provider of Endpoint Security Solutions

Innovative Policies to Defend Against Next-Generation Threats

Conrad Herrmann

CTO and Co-Founder

Zone Labs, Inc.

Network Security Is an Uphill Battle

Network security challenges:

- Malware and hackers
- Targeted attacks and corporate espionage
- Social engineering
- Unapproved or unpatched apps in your network
- Changing network topology

ZONE LABS

What's at Risk?

If attacked, your company could loose:

- Intellectual property
- Business plans
- Customer data
- Financials
- Your reputation

How Large is the Risk?

Maybe your company will be lucky.

- 20% of companies are likely to experience a "serious Internet security incident" through 2005.[1]
- Cleanup costs will exceed prevention costs by 50%.[1]
- Companies lost more than $200,000,000 to computer security issues in 2002.[2]

1. Gartner G2, 5/2/02 *2. 2003 CSI.FBI Computer Crime and Security Survey*

ZONE LABS

Beware the Targeted Hacker

Targeted attacks on the rise

- More hackers motivated by profit
- Hacker tools (esp. spyware and Trojans) widely available and easily customizable
- Vulnerable remote endpoints—the easy targets
- Case study—Microsoft

Of all security crimes, theft of proprietary information caused the greatest financial loss to the enterprise in 2002.[1]

1. 2003 CSI.FBI Computer Crime and Security Survey

ZONE LABS

Threats have evolved

Yesterday

- Worms
- Basic vectors of propagation: email, “sneakernet”

Today

- Advance viruses
- RATs
- Multifaceted threats like Nimda

You are here

Tomorrow

- Incredibly complex multifaceted threats

Future Traits of Intrusions

Multifaceted

- Many propagation vectors and payloads
- Developed through team hacking

Endpoint-targeted

- Number of endpoints constantly increasing
- More remote access breaches
- Remote laptops, wireless access, family PCs

Industrial espionage through RATs

- Broad attacks camouflaging specific targeting

Peer-to-peer-based

- Propagation and payloads that exploit IM and other peer-to-peer apps

Target security applications

ZONE LABS

Future Traits of Intrusions

- Attacks on wireless devices
- Polymorphic
  - Evolve in the wild to fool pattern-based solutions
- Automated
  - Autolaunching—no social engineering required
  - Scans for vulnerable systems
- Exploit Microsoft vulnerabilities
  - Bugs and ill-considered features
- Exploit vulnerabilities in open source code

ZONE LABS

Future Traits of Intrusions

Spread like spyware

- 40-50% of PCs are compromised by spyware[1]

1. ZDNet, 2/24/03

Traditional Security Technologies Fall Short

Perimeter Firewalls

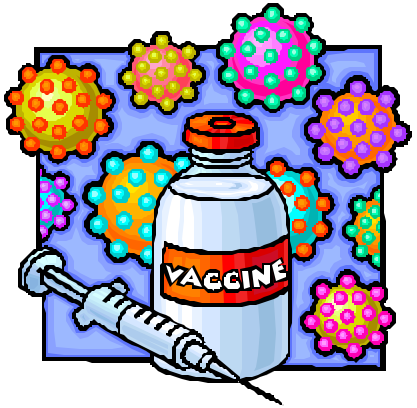
- Unable to stop outbound attacks—trojans, spyware, etc.
- Protects remote computers only when connected

Intrusion Detection Software

- Safeguards only against known patterns of attack

Antivirus Software

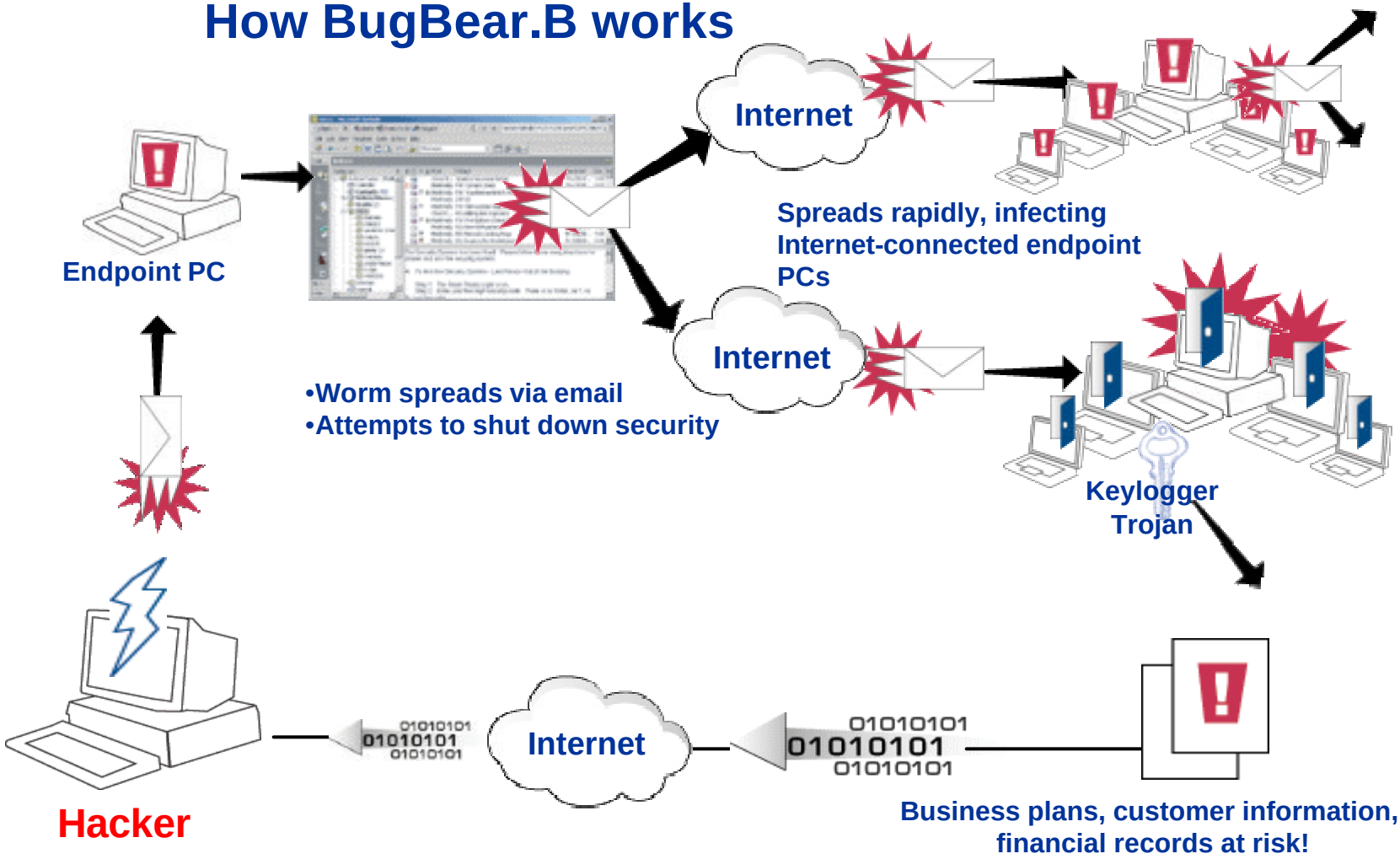
- Reacts only to known infections
- Fails to recognize attacks disguised as legitimate computing behavior



ZONE LABS

Case Study: BugBear.B

How BugBear.B works



Case Study: BugBear.B

BugBear.B is a tool for a targeted attack

- Elaborate snooping mechanisms
- Special payload for financial institutions
  - Compares target to list including J.P. Morgan, AmEx, BofA
  - Steals passwords and other critical data
  - Emails to virus creator
- Hijacks modem
- Possible proof-of-concept test

Source: "BugBear worm: New kind of crime?" Bob Sullivan, MSNBC.com

ZONE LABS

Security practices have evolved

Yesterday

- Island defense

Today

- Perimeter defense
- Reactive measures

You are here

Tomorrow

- Proactive measures
- Defense in depth
- Integrated defenses

Solution Goals: Protected *and* Productive

Security must NOT sacrifice productivity

Central management

How easy is it to deploy, configure and manage the solution?

Cooperative enforcement

Does it work well with other security products in a multilayered architecture?

Interoperability

Does it seamlessly integrate to leverage legacy investments?

Flexibility

Is it adaptable to multiple use cases and evolving business requirements?

Reliability

Does it protect? Is the solution mature enough to deploy without undue risk of downtime and helpdesk calls?

ZONE LABS

Integrated Defense

The first step towards a fully integrated defense solution is total awareness of the entire network environment.

- Machines
- Operating systems
- Software
- Malware
- Network traffic profiles
- Expert interpretation

ZONE LABS

Integrated Defense

Successful intrusion prevention relies upon integrated and manageable security tools.

- User policies
- Education
- Forensics
- Enforcement
- Logging
- Accountability

ZONE LABS

Integrated Defense

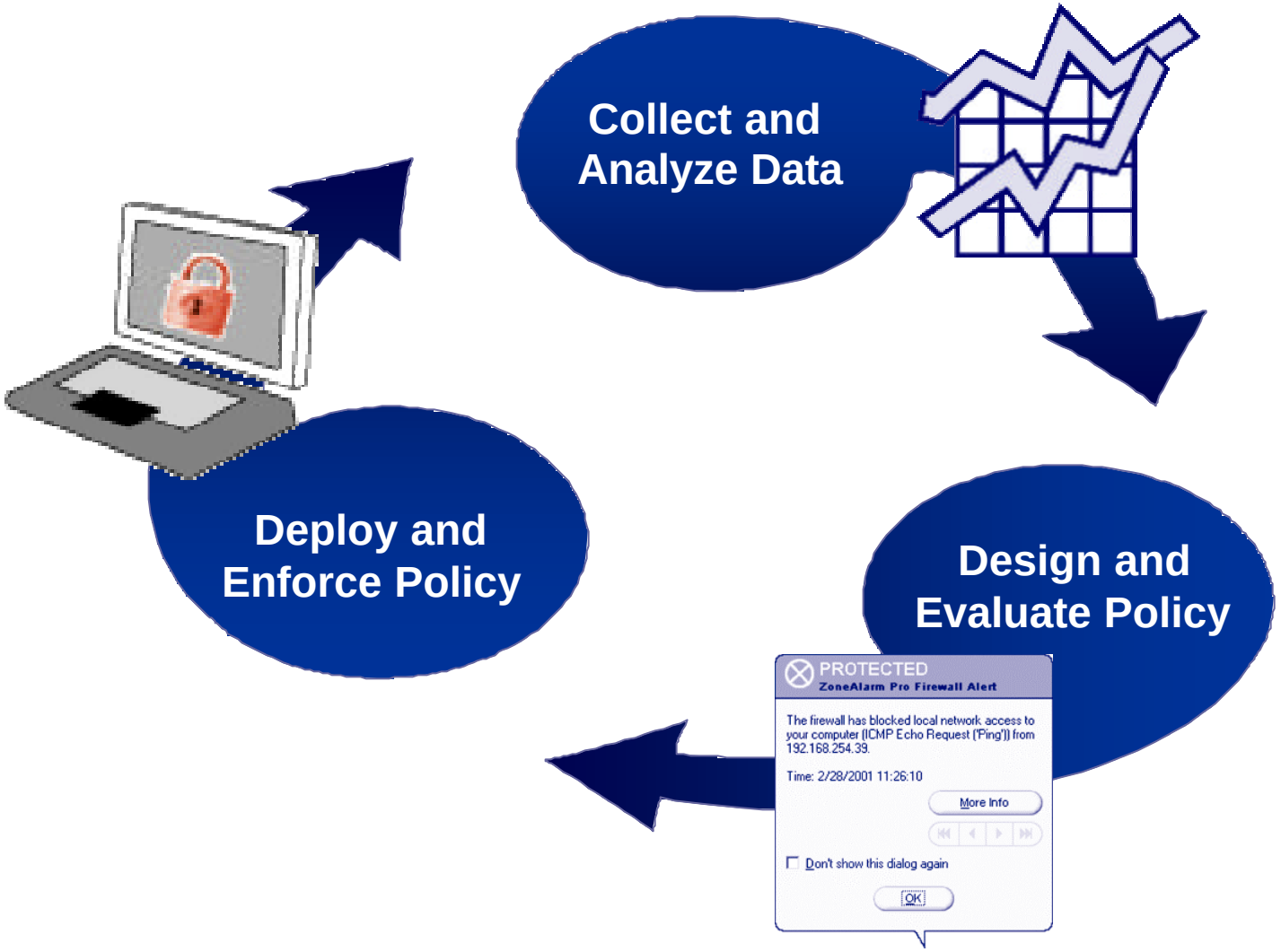
Security policy needs of the enterprise:

- Granular control over network access rules
- Wide choice of firewall rules, from classic “port and protocol” restrictions to application-specific
- Dynamic policy creation options
- Patch management
- Control over rogue applications
- Enforcement capabilities

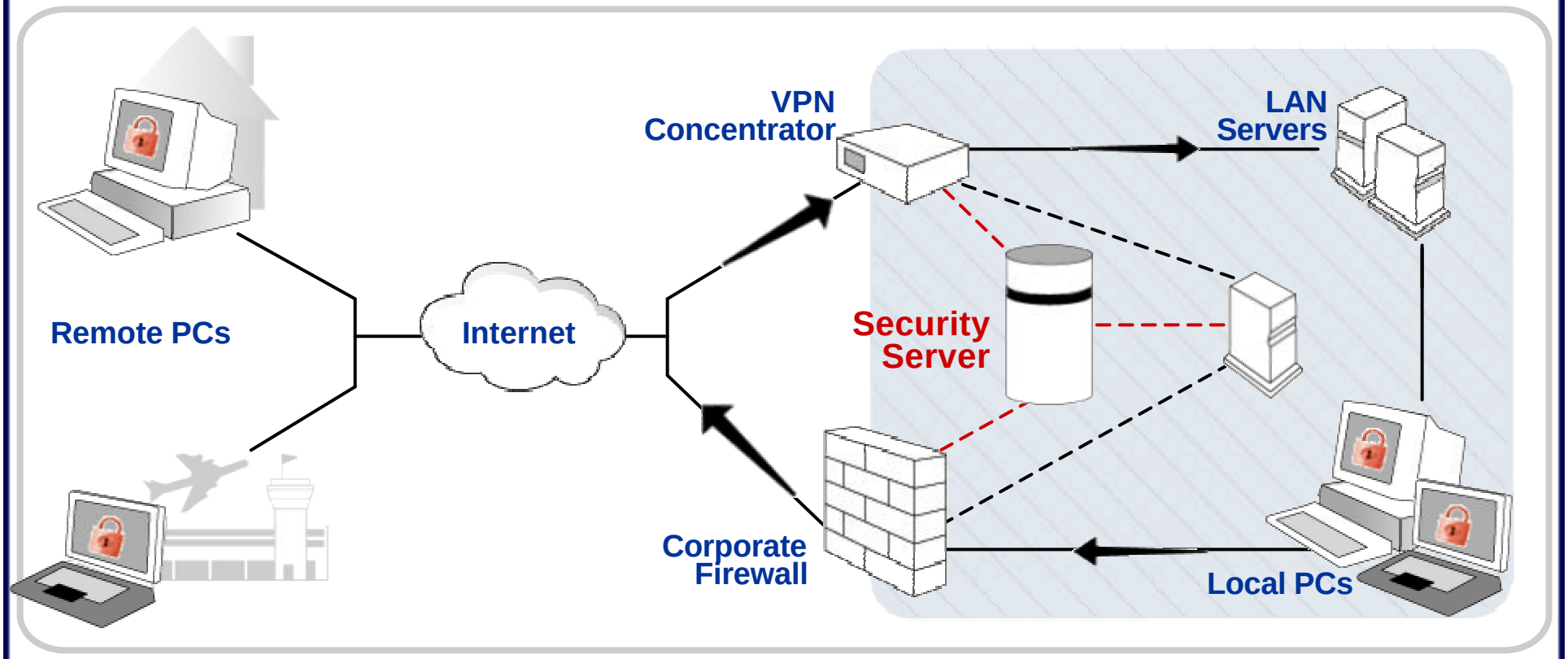
When possible weaknesses are controlled with policies, attacks against the network are unsuccessful.

ZONE LABS

Integrated Defense



Enforcing policy



Finding the Right Solution

When evaluating integrated defense technology, ask:

- Does it cooperate?
- Does it detect the threat?
- Can it protect against the threat?
- Will it protect against the multifaceted threats of the future?
- Is it manageable?
- Is it able to log data for forensic investigation?
- Does it protect itself from being disabled?


ZONE
LABS
The Leading Provider of Endpoint Security Solutions