Trends in IT Security

Enabling Productivity

InZero® SYSTEMS

Table of Contents

Executive Summary

Most organizations see themselves as having solid, impenetrable walls surrounding their IT infrastructure. As a result they believe their data to be safe.

But that theory is not completely realistic. An inflexible IT perimeter often conflicts with an increasingly flexible business perimeter – creating significant new vulnerabilities and requiring expensive patchwork solutions.

The goal of much of today's IT security is to mitigate the ever-increasing risks of open internet access through endpoint protection, network access control and the use of virtual private networks.

With these strategies in place, organizations believe they are well-protected. But in reality, these pillars of network architecture are insufficient against the tidal wave of new and increasingly sophisticated malware.

There is an alternative. Consider that it is possible to put an endpoint (laptop, workstation, or server) behind a separate, dedicated device that would take over network functionality, physically separating the endpoint from network traffic.

Network applications would reside in the device's dedicated read-only memory, which would ensure that malicious software is *denied the environment for execution*, delivering a level of protection far superior to signature-based virus recognition.

This approach, coupled with an organization's existing IT security perimeter, would allow organizations to:

- Redefine their approach to IT security by preventing malware from ever reaching a PC
- Choose the highest levels of productivity *and* security, instead of having to choose between them
- Turn all IT security unknowns – guest users, remote users, overseas partners, etc. – into fully-controlled network environment components with an outstanding IT security posture
- Place strict controls on IT security expenditures

"More than 35 million data records were breached in 2008 in the U.S., a figure that underscores continuing difficulties in securing information, according to the Identity Theft Resource Center (ITRC). It documents 656 breaches in 2008 from a range of well-known U.S. companies and government entities, compared to 446 breaches in 2007, a 47 percent increase.

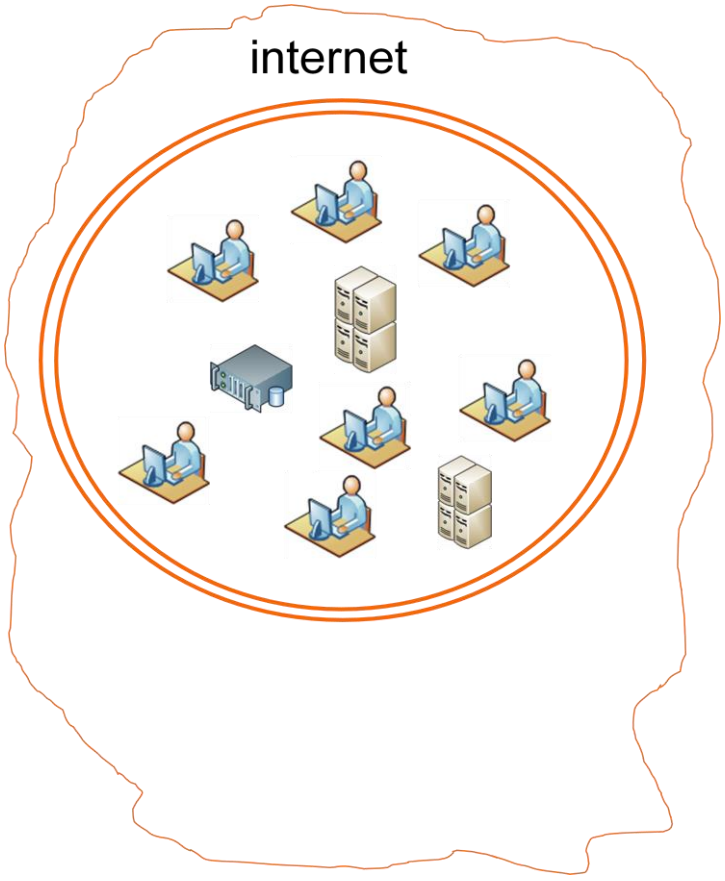
The business community had the most breaches, comprising more than a third of the 656 breaches. BNY Mellon Shareowner Services reported the highest number of breached records: 12.5 million. A box of computer tapes containing names, social security and account numbers was lost. A lock on the truck transporting the tapes was broken, and the truck had been left unattended, according to news reports. The tapes were not encrypted."

— Jeremy Kirk, CIO.com, January 2009

The IT Security Environment

In the Past…

Historically, IT security has been an afterthought in the business planning process, primarily because organizations saw themselves as having well-defined perimeters. This assumption allowed them to put in place the necessary IT infrastructure and build a "wall" around it for protection.



There were valid reasons for this approach, but the implementation of a set perimeter resulted in strategic shortcomings that appear to be gaining in prominence and threatening the status quo:

- Quick band-aid solutions were applied to counteract new emerging threats
- Productivity was often sacrificed in the name of security
- Security costs escalated

"Security vendors hyperbolically claim that application firewalls completely solve the software security problem by blocking application-level attacks caused by bad software, but that's just silly"

— Gary McGraw, CTO, Cigital Inc., December 2007

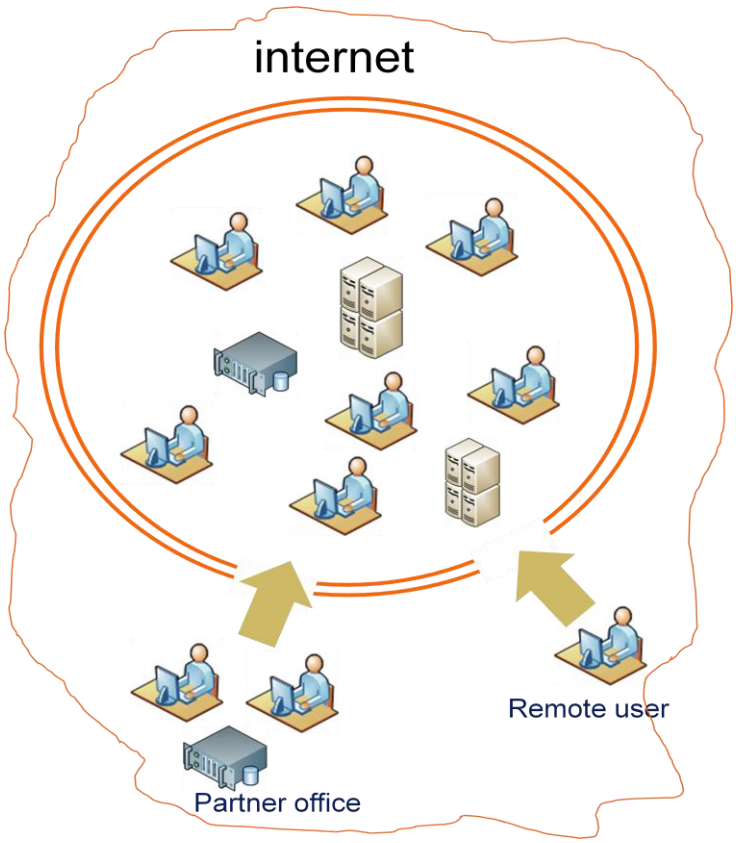
"IT security budgets are consuming 10% of IT operating budgets and rising amidst growing concern over data breaches and an increasing need to protect sensitive data."

— Forrester Research, September 2008

Current IT Security Challenges…

In addition to those already discussed, new business trends are making it even more difficult for organizations to continue with their existing IT security systems:

- Increasing de-centralization of business structures – outsourcing, globalization, telecommuting – is making it harder to maintain a rigid outer perimeter
- Proliferation of new malware capable of bypassing existing solutions, aimed at the general public or specifically targeted at an organization
- Competitive pressures require increased productivity, while security concerns have a negative effect on productivity



It is helpful to consider how these trends impact existing IT security systems by looking at three pillars of a well-designed network:

- Endpoint Protection
- NAC (Network Access Control)
- VPN (Virtual Private Networks)

Many believe that an organization will have achieved a solid level of IT security if it has secured its endpoint devices, has in place enforceable policies of network access criteria, and automatically encrypts data-in-transit.

But how much piece of mind do these solutions really provide?

Endpoint Protection

Protecting laptops and desktops from malicious network traffic is one of the foundations of IT security. Therefore it can be surprising to learn that endpoint vulnerabilities are on the rise. Users – individual and corporate – stand to lose more because they store and access significantly more confidential data then even just a few years ago.

"In fact, less than 50% of American PC users are safe from malware, and the percentage is even lower in countries like China and Brazil."

— Business Week, November 2008

The essence of the problem is simple: existing security solutions, for all their complexity, *do not* physically separate endpoints from network traffic. As long as malware has access to an endpoint there is always the potential for a malware infection, regardless of the protection mechanisms deployed.

The majority of endpoint security software is based on virus signature recognition, an approach that is quickly becoming outdated as existing viruses morph and change their signatures, and brand new vulnerabilities are discovered. As a result, signature-based malware solutions are providing poor protection against known threats, and no protection against new, unknown threats.

Network Access Control (NAC)

NAC uses policies, including pre-admission endpoint security policy checks and post-admission controls, to control access to a network.

It has long held a promise of alleviating most pressing IT security concerns. At its core it combines access control, endpoint security assessment, and user authentication. However, NAC deployment lags behind industry forecasts, primarily because of its high cost and lack of true security.

"The majority of current network access control (NAC) solutions fail to address basic security problems."

—IT Week, March 2008

Deployment costs can run into the millions, depending on the size and complexity of an organization. In addition, NAC security concerns are of a fundamental nature: if the endpoint is asked to self-authenticate, what prevents a compromised endpoint from misrepresenting its security posture? Basically, without a bulletproof endpoint security enforcement mechanism, most current NAC solutions can be overcome by hackers.

Virtual Private Networks (VPN)

A VPN is a solid, proven technology. However, when out-of-the-office users (employees or partners) use a VPN to connect to their office network they are exposed to the possibility of session hijacking – the use of authorized network access to gain unauthorized access to data.

That possibility is becoming a more prevalent concern as more and more endpoints become infected with increasingly sophisticated malware.

These concerns are especially prominent in highly security-centric organizations. Due to the increased risk of unauthorized access to sensitive data, many of them have decided not to implement VPNs – even at the cost of significant productivity.

Lastly, the complexity of implementing and maintaining some VPN solutions places a serious strain on IT support and maintenance, increasing the risk of human error.

"A security expert discovered a VPN device bought on EBay automatically connected to a local council's confidential servers."

—PC Pro, September 2008

In Summary…

The three cornerstones of a seemingly well-designed network architecture – endpoint protection, NAC, and VPN – are in reality lacking in security, costly to implement, and require significant resources to maintain.

This is primarily because they operate independently of each other, and therefore fail to present a unified front to the malware attempting to compromise a network.

This lack of interdependence has an increasingly negative impact on productivity and will force organizations to look for new solutions to achieving an appropriate combination of IT security and productivity.

"Despite the efforts of the computer security industry and a half-decade struggle by Microsoft to protect its Windows operating system, malicious software is spreading faster than ever…Computer scientists and security researchers acknowledge they cannot get ahead of the onslaught."

—NY Times, December 2008

The Future of IT Security…

Organizations that can enable their users (employees, partners, contractors, customers, etc.) to communicate freely and securely from anywhere in the world will have a significant competitive advantage over those that hold on to the existing restrictive IT model.

This restrictive model is proving imperfect in this new environment. As a result, IT security is on the cusp of a fundamental change – just when organizations have become adept at continuously patching their existing IT perimeters.

After years of add-ons designed to address individual breaches, legacy systems are overburdened and struggling to maintain balance – often negatively impacting productivity in the process. The complexity of these band-aids has created security vulnerabilities, not to mention the skyrocketing costs of maintenance and configuration efforts.

This multi-layered complexity calls for a new approach to IT security, one that is best defined as enterprise *de-perimeterisation*.

Instead of trying to build walls around continuously shifting and changing business environment, organizations would be well-advised to focus on safeguarding their data – a goal that can be accomplished through de-perimeterisation.

The good news is that with the right set of products existing systems and practices can compliment this new approach.

Accepting the concept of de-perimeterisation may require nothing more than implementing a de-perimeterisation solution to address acute existing problems (guest users, remote users, wireless users, etc.) and letting results dictate how this solution will be rolled out further in an organization.

This gradual implementation process will allow for the coexistence of the two concepts – perimeterisation and de-perimeterisation – and will give organizations the ability to measure the benefits of this new approach.

"…in tests of 36 commercial antivirus products, fewer than half of the newest malicious software programs were identified."

—NY Times, December 2008

"De-perimeterisation is simply the concept of architecting security for the extended business boundary and not an arbitrary IT boundary."

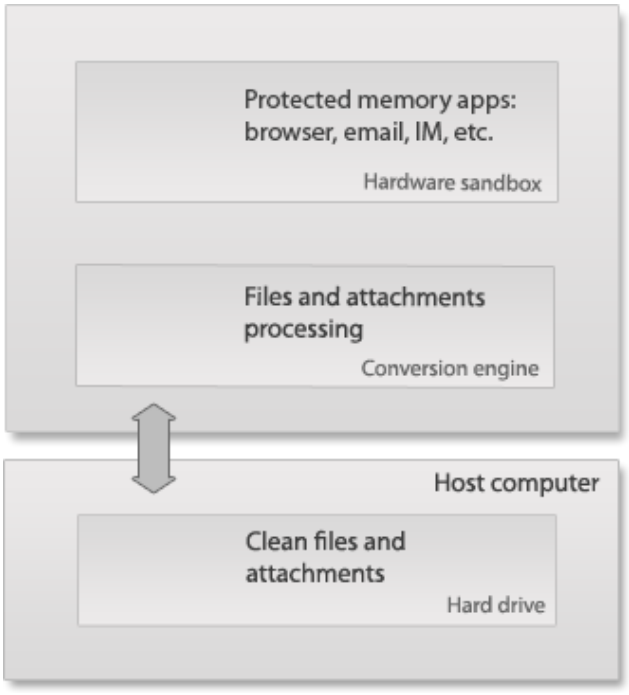
—Jericho Forum, 2007

A New Approach:

Preventing Malware Execution

Today's IT security approaches attempt to mitigate the risks of open network access. But there is a better way to solve the IT security riddle.

Consider that it is possible to put an endpoint behind a separate, dedicated device (with its own processor, memory, and operating system) that would take over network functionality.



Safely access internet, download files and email attachments.

Convert all documents and store them safely on host computer. Also convert documents from host computer before sending them out.

The device would physically separate the endpoint from network traffic. Network applications would reside in dedicated read-only memory – a hardware sandbox – that would ensure any malicious software is *denied the environment for execution.*

This is no longer signature-based malware recognition; instead, all internet and network traffic is treated as untrusted and physically separated from the host computer on a hardware level.

To enable further productivity gains, the technology also uses a conversion engine to process all email attachments and downloaded

files – again treating all of them as untrusted and converting them *before* saving them to the host computer in an encrypted format.

This conversion engine offers powerful protection in both directions.

It does not allow any malware to get into the protected host computer, nor does it allow any malware on the protected host computer to infiltrate the network. This makes any infected laptop innocuous to the rest of a network.

These devices can be interconnected and managed by the network administrator, enabling rules, policy administration and enforcement that is user-specific versus endpoint-specific.

In effect, this approach creates a micro-perimeter around each endpoint, challenging the existing status quo and allowing organizations to achieve three things simultaneously:

- Advance significantly in the "stay ahead of new malware" game that has become IT security
- Reclaim the productivity lost because of current restrictive IT policies
- Make IT security expenditures predictable and an easily-controllable budget item

About InZero® Systems

InZero Systems was founded in late 2004 by a group of cyber security experts, entrepreneurs, and senior Fortune 100 executives.

InZero Systems' intellectual property is protected by a number of U.S. and international patents. The company is headquartered in Herndon, Virginia and has grown to 50 people with three offices and multiple product offerings.

To find out more about InZero Systems and InZero Security Platform, please visit www.inzerosystems.com or call 703.788.6571.

About InZero® Security Platform

InZero Security Platform offers "plug-and-play micro-perimeter defense" based on distributed hardware devices – InZero Gateways – redefining how organizations look at IT security.

These micro-perimeters give organizations a reinforced, flexible, de-perimeterised IT security solution, which compliments, solidifies and extends the perimeter they have around their entire IT infrastructure.

Vulnerability	InZero Solution
• Currently most attacks are aimed at network applications	• Internet applications run in a hardware sandbox, protected by microcontrollers
• The most dangerous of these attacks aim to use a browser as a vehicle for malicious activity	• Due to read-only memory protection mechanism, programs cannot be changed in sandbox
• Code injection is another dangerous type of attack	• Unique protection design prevents malicious code execution within hardware sandbox
• Most of attacks aim to compromise sensitive user data	• Physical isolation of hardware sandbox ensures that malware has no access *of any kind* to the host computer
• Limited protection against a compromised computer connecting to a network	• Malware present on host computer can not bypass InZero Security Platform

Several comprehensive penetration tests of InZero® Security Platform were conducted by Lockheed Martin, British Telecom, and SAVVIS Federal Systems among others. The ultimate security of InZero Security Platform was proven with zero intrusion result.

Being hardware-based, this technologically-advanced solution provides unprecedented levels of security, requires less maintenance and configuration efforts compared to software-only solutions, is simple to implement, and enables *higher productivity* and *lower total cost of ownership*.

InZero Security Platform unifies the three fundamental components of a successful network design:

- Unprecedented endpoint protection
- Secure NAC
- Advanced VPN

Higher Productivity

- Attachments can be safely viewed, printed, edited, saved – enhancing communication with partners, vendors, and customers
- No network restrictions; users can browse any web site – or use instant messaging – with zero risk of infection
- Teleworking can be implemented in a most security-centric organization, saving time, money, and environment
- Network traffic is easily monitored and users abusing network resources can easily be identified

Lower TCO (Total Cost of Ownership)

- Cost of security breaches is eliminated
- No need for initial or ongoing user training
- Limited admin training is required, as policies are easy to set up and manage
- Security patches – notorious for damaging network environments and interrupting business activity – are no longer needed
- Staff that previously was tasked with maintaining data security can now be directed to productivity-enhancing tasks

Sources

"Business rationale for de-perimeterisation." Jericho Forum White Paper, 2007 (http://www.opengroup.org/jericho/Business_Case_for_DP_v1.0.pdf)

"Beyond the PCI Band-Aid." Dark Reading, December 10, 2007. (http://www.darkreading.com/security/showArticle.jhtml?articleID=208803544)

"Council sells security hole on EBay," Matthew Sparkes. PC Pro, September 29, 2008 (http://www.pcpro.co.uk/news/227190/council-sells-security-hole-on-ebay.html)

"ISR News: 35MM Records Breached in 2008," excerpted from CIO.com's Jeremy Kirk. Information Security Resources, January 9, 2009 (http://information-security-resources.com/2009/01/08/isr-news-35mm-records-breached-in-2008/)

"IT security devours 10% of operating budgets," Jon Brodkin, ComputerWorld UK (online), September 5, 2008 (http://www.computerworlduk.com/management/security/datacontrol/news/index.cfm?newsid=10842&x)

"Microsoft to Stop Charging for Home PC Security," Aaron Ricadela. Business Week (online), November 19, 2008

"Thieves Winning Online War, Maybe Even in Your Computer," John Markoff. New York Times (online), December 5, 2008

"Weak networks need NAC bypass: confusion reigns due to lack of clear definitions," Martin Courtney. IT Week, March 9, 2007 (http://www.computing.co.uk/itweek/news/2185181/weak-networks-nac-bypass)