The Case for Secure Ethernet/IP Access and Address Management

A Return on Investment Analysis

ViAScope USA

Executive Summary:

In an increasingly competitive global environment, today's IP-enabled organizations are looking increasingly to smart investments in Information Technology to maximize intellectual property, mine customer and competitive data, optimize business processes, increase productivity, and speed customer and market responsiveness. The communications backbone of these ongoing IT investments is the enterprise-wide Ethernet and IP network. IP networks have created compelling economics and ease of use to take over as the defacto standard of corporate networking. Nonetheless, the open nature of IP communications also creates security risks. With more demanding data and sensitive converged Voice and Video applications flowing over Ethernet and IP networks, ensuring the security, privacy and integrity of the network has become more important than ever. However, while organizations have invested heavily in externally-facing security systems, a serious hole in security and management controls over internal network access remains in the vast majority of organizations, beginning with the trivial ease of access and network address resource allocation that exists in most internal enterprise networks.

IPScan is the leading solution for Ethernet/IP network access and address control, deployed by hundreds of large enterprises, service providers, government and military agencies and educational institutions. IPScan provides IP-enabled organizations with highly valuable risk mitigation and operational efficiency benefits in four key areas: securing the network against internal breaches, preventing inadvertent network disruptions, mitigating against the risk of non-compliance with regulations concerning sensitive data, and increasing IT's operational efficiencY.

This white paper establishes the business case for the IPScan solution using an overall Return on Investment (ROI) model that easily justifies the total cost of ownership (TCO) across the four major areas outlined above. Detailed ROI are presented for each area in each of the four areas' respective sections to provide both financial and technical context.

ViaScope's IPScan can bring significant benefits to any IP-enabled organization, and help contribute to its ongoing success by supporting greatly enhanced IT security, continuity, compliance and operational efficiency.

Summary Return on Investment Model

IPScan delivers a rapid, positive ROI in four key areas as outlined in the executive summary. Below is a summarized view of the ROI model for IPScan based on a network with 1000 IP devices, showing that an IPScan solution inclusive of three years maintenance fees can achieve a positive ROI in less than six months by reducing operations costs, and mitigating risks of security breaches, network disruptions and regulatory non-compliance. Note that while industry averages for network downtime, security and regulatory non-compliance reported by analyst surveys are very high, this ROI utilizes significantly lower, conservative estimates, which further underlines the value of the IPScan solution. For a detailed breakdown of the assumptions and technical context behind each category's ROI calculation, please refer to the appropriate section referenced in the table of contents.

Category	Industry Average Cost/Risk of Loss	Assigned Risk/Cost	Annual Occurrence or Risk	Solution Cost	Year 1	Year 2	Year 3	Total
IPScan Solution				$90K	$16.2K annual maint	$16.2K annual maint	$16.2K annual maint	$138.6K
Opex Savings	Five minutes IT staff time per device per month, for address mgmt operations of 1,000 devices, or $39K per year, reduced by 80%	$31K	Each year ongoing		$31K	$31K	$31K	$93K
Security Risk Mitigation	Average $4M losses from unauthorized info access reported in FBI/CSI 2004 Report	$100K	Once		$100K	$100K	$100K	$300K
Network Disruption Risk Mitigation	Industry average per downtime occurrence is 1.5 hours per Dataquest. One hour of downtime on average costs minimum $96K per Infonetics.	$144K	Once		$144K	$144K	$144K	$432K
Regulatory Non-Compliance Risk	$2M non-compliance fine + brand damage if public	$100K	Once		$100K	$100K	$100K	$300K
Annual Cost/Risk of Loss					$375K	$375K	$375K	$1.12M
ROI Timeframe in Months					***5***			

Operational Expense Savings with IPScan

IP address management is a time-consuming, yet absolutely necessary IT task. According to Network World's May, 2005 report, IP address management is becoming more important:

> Several factors are driving IP address management from the back burner to a more prominent place on the IT to-do list.
>
> - Data center consolidation is sending more LAN applications over the Internet, which is driving efforts to better manage IP addresses within IT shops.
> - VoIP, by making phones an IP device, potentially doubles the number of IP addresses.
> - Security concerns in terms of network access and potential virus infection from unknown devices are forcing companies to better manage network access.
> - The demand to deliver QoS and applications to end users is pushing IT managers to more closely monitor IP addresses

Based on information collected from its base of large enterprises, service providers, government and military agencies and educational institutions, ViaScope estimates that IP address administration requires 5 minutes per device, per month on an annualized basis. On this basis, address management for 1,000 devices requires the equivalent of 39% of one full time employee's work hours annually. Utilizing $100,000.00 as the fully burdened cost of a full-time network administrator, the cost per year of IP address management is $39,000.00 per year.

Due to its comprehensive detection, monitoring, audit trail documentation, administration and policy enforcement capabilities, IPScan reduce IP address management by 80%, leading to a cost savings of $31,000.00 per year. The following table summarizes the operational cost savings that IPScan delivers in regards to IP address management:

IPScan IP Address Management IT Opex Savings

Annualized hours of IP Address Mgmt of 1,000 devices @ 5 minutes per device per month	1000
Work hours per year	2440
Full-time equivalent required for IP Address Management	39%
Cost per IT network administrator, including overhead	$100,000
Annual cost of IP Address Management	$39,000
Percent of IP Address Mgmt Time Savings from IPScan	80%
Annual savings	$31,000

Security Risk Mitigation with IPScan

IPScan delivers a powerful security solution to mitigate against the considerable risks of insider security breaches. IPScan provides a comprehensive, policy-based access control enforcement solution that ensures that only authorized devices can connect to the internal network, whether via wired or wireless media.

The Prevalence and Cost of Insider Security Breaches

Insider security breaches are both commonplace and costly. The 2004 CSI/FBI Computer Crime and Security Survey reports 68% of organizations reported that they had suffered at least one, if not more insider security incidents, as shown in figure 1:

How Many Incidents From the Inside?	1 – 5	6 – 10	>10	Don't Know
2004	52%	6%	8%	34%
2003	45%	11%	12%	33%
2002	42%	13%	9%	35%
2001	40%	12%	7%	41%
2000	38%	16%	9%	37%
1999	37%	16%	12%	35%

Figure 1: 68% of 280 surveyed organizations reported insider security breaches

Furthermore, many of the most common occurrences of reported security breaches involved insider network abuse, and related security issues such as theft of authorized devices (laptops/mobile computing devices), unauthorized access to information, and system penetration, as is show in figure 2.

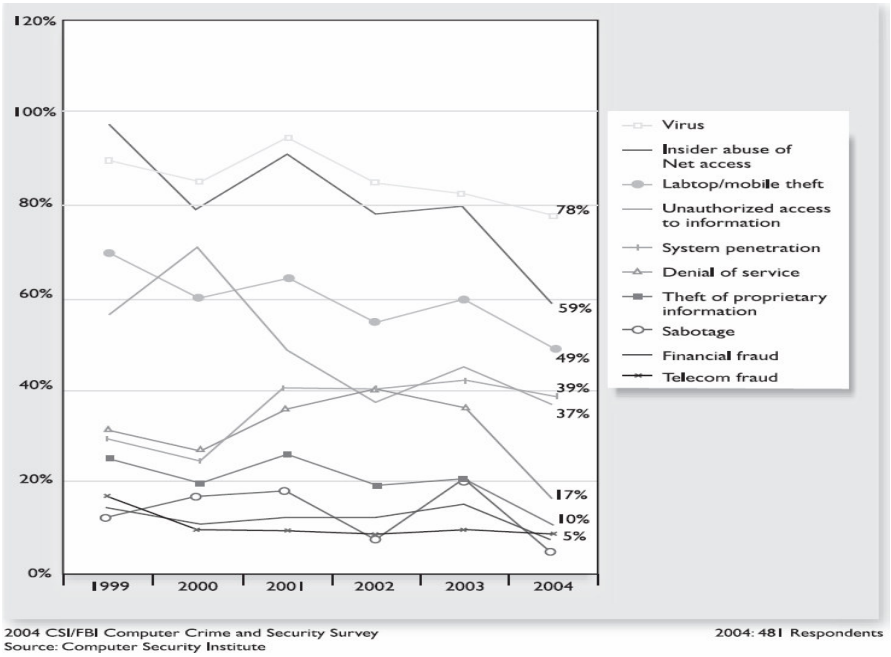

Figure 2: Types of Attacks of Misuse Reported within Responding Organizations over last 12 months

The cost of security breaches is very high, as reported by survey respondents. Figure 3 shows the reported average cost of various security breaches. Insider network abuse, wireless network abuse, laptop theft, and unauthorized access can each cost millions of dollars.

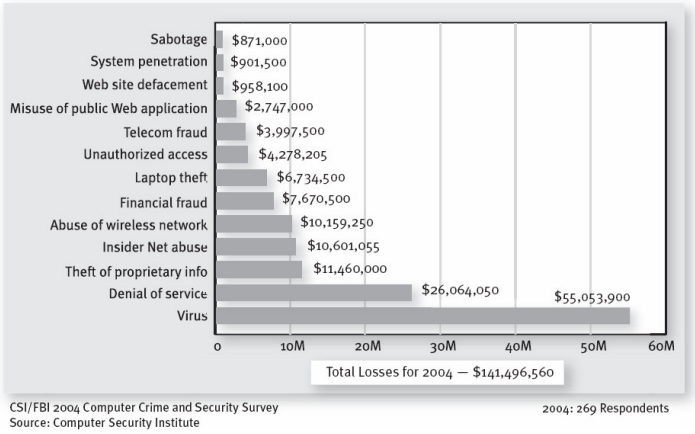

Figure 3: Dollar amount cost for various security breaches

IPScan Fills the Network Access Control Gap

The breaches and related costs outlined above occurred despite the fact that the most organizations overwhelmingly employ firewalls and anti-virus software, and a large percentage also deploy a wide variety of other security tools, as seen in Figure 4. However, most of these security tools are aimed at preventing security breaches from external sources, while there is a noticeable lack of internally oriented controls. Clearly, current security measures are not enough. One of the most significant holes in internal network security is the lack of comprehensive network access controls.

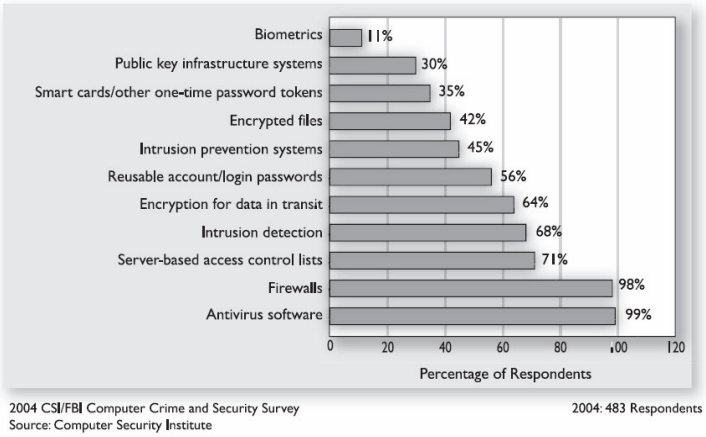

Figure 4: Percentage of organizations deploying various security solutions

IPScan provides comprehensive protection against unauthorized access to the network, for all Ethernet and IP devices, providing a critical front-line of defense against unauthorized communication and access to proprietary or sensitive information. IPScan allows network managers to centrally define and update globally

enforced access control policies so that only authorized Ethernet and IP addresses (static or dynamic) and hostnames in defined combinations, may communicate at the IP layer on the network. IPScan provides significant risk mitigation against insider security breaches across a variety of risk categories such as:

- Theft of proprietary information (average loss = $11.46M)
- Insider network abuse (average loss = $10.6M)
- Abuse of wireless network (average loss = $10.15M)
- Laptop theft (average loss = $6.7M)
- Unauthorized access (average loss = $4.3M)

IPScan's Value as Security Risk Mitigation

IPScan delivers a powerful return on investment when compared to the significant risks of loss due to insider security breaches. In order to conservatively calculate the value of IPScan as a risk mitigation solution, the risk mitigation model utilizes only the lowest risk of loss category—unauthorized access, even though IPScan is applicable to all the outlined risk categories above. In addition, the average loss is rounded down to $4M. While no security solution or product defines full "security" on its own, and must be combined with proper internal security policies, processes and practices, IPScan enables an unprecedented degree of administrative control over fundamental network access while remaining transparent to users, since it requires no installed client software, and no further login processes. This ease of use and the real-time, automated nature of enforcement support the execution of consistent control processes—which increases risk mitigation by eliminating human error or circumvention. For this reason, IPScan can deliver significant risk mitigation—calculated at 75% of the risk of unauthorized access—or $3M mitigation value in absolute terms. The model then factors a smaller enterprise size at 1000 devices by taking only 20% of this risk--$600K, and selecting an arbitrary, low percentage value of the absolute mitigation value (16.7%), arriving at $100K annual risk mitigation value. Note that this is an extremely conservative model, since survey results can easily support a much higher annual risk mitigation value for IPScan.

IPScan Internal Security Breach Risk Mitigation Value

Average loss reported due to unauthorized access (rounded down)	$4M
Percentage of value that IPScan brings to mitigating against insider network security breaches or abuse	75%
Absolute mitigation value of IPScan	$3M
Annualized, highly conservative annual risk mitigation value for a 1000 device enterprise	$100K

Mitigating Network Disruption Risk of Loss with IPScan

Today's business environment depends heavily on IT automation for productivity. Correspondingly, network downtime can be very costly. Industry measurements of the losses associated with an hour of network downtime have been established by Dataquest for a sample of industry verticals. Notably, transaction-driven businesses such as financial services incur heavy losses from downtime:

- Financial/Brokerage: $6.45M lost per hour of downtime
- Financial/Credit Card: $2.6M lost per hour of downtime

In addition, anecdotal reports show that many data-driven organizations place a high dollar value of loss on network downtime. For example, large pharmaceuticals organizations report that downtime at data-driven manufacturing facilities can cost on the order of $5M per hour, since a whole production batch must be disposed of if connectivity and control process monitoring of the manufacturing is lost. Gaming is another data-driven business with large costs for network downtime—In an April, 2004 article, Secure Enterprise magazine reported that downtime at the Mohegan Sun casino on a busy Saturday night, was calculated at $2M per hour. However, even in business where downtime doesn't directly affect financial transactions in real-time, Infonetics calculates $96K per hour lost per hour of downtime.

According to the Forrester Group, 15% of all application downtime is caused by network issues, and a majority of the root causes of network-based downtime is due to IP addressing problems. IP address conflicts that bring down connectivity to key servers, or worse, to key routers can cause costly network downtime. This means that under-managed IP address space is a business risk liability to every organization.

IPScan can virtually eliminate the risk of network downtime due to IP address conflicts, since it enforces complete policy-based address management controls over not only dynamic (DHCP) addresses, but also static IP addresses and even Ethernet addresses and hostnames.

IPScan's value in mitigating downtime risk due to IP address conflict is calculated based on a $96K cost of downtime per hour, with one downtime incident calculated per year. Infonetics reports that the average downtime lasts 1.5 hours, making the total risk of address conflict downtime per year $144K. The following table summarizes IPScan's network downtime risk mitigation value:

IPScan IP Addressing-Based Network Downtime Risk Mitigation Value

Calculated loss reported due to network downtime, per hour	$96K
Average downtime duration, per Infonetics	1.5 hours
Annual downtime loss risk—IPScan's annualized value	$144K

Mitigating Regulatory Non-Compliance Risk with IPScan

A wide variety of organizations must concern themselves with regulatory requirements around data security, privacy and continuity. Most prominent examples are criminal charges and heavy fines associated with Sarbanes-Oxley (SOX) section 404 for publicly held companies, and healthcare HIPAA requirements. Another example is financial service banking organizations, which must comply with strict regulatory requirements to close all bank branch books on a daily basis, with stiff fines for delays. Any regulated industry requires solid, auditable security and continuity processes for all portions of the IT infrastructure.

IPScan provides an automated and centrally managed platform for network access control policy definition, propagation and enforcement. IPScan also records a history of every device's access to the network, to provide solid documentation of the control processes for compliance purposes. Without IPScan, a breach of data privacy could be easily shown to be the result of poor control processes on fundamental network access, which may result in stiff fines and penalties. The loss associated with non-compliance fines is calculated at $2M per incident, which does not factor in brand damage. The model then assigns a conservative annual value of $100K to IPScan for mitigating compliance risk, as is illustrated in the following table:

IPScan Regulatory Non-Compliance Risk Mitigation Value

Cost of Non-Compliance	$2M
Conservative, annual risk mitigation value of IPScan	$100K