TippingPoint®

360° Network Access Control with TippingPoint NAC

WHITE PAPER

Contents

...applying 360° Network Access Control with TippingPoint NAC effectively redefines the network perimeter into a model that accounts for the many user types, network access devices, and various paths into the network. Combining visibility and control in this manner enables organizations to monitor network activity at a fine-grained level and to take fitting corrective action, facilitating compliance with internal policy and regulatory requirements.

Introduction

Protecting enterprise networks from attacks has been improved immeasurably over the past several years. Yet, for all of the deployment of perimeter security firewalls, application security gateways, ID management systems, desktop protection software, and other network security devices, major network breaches leading to loss of personal privacy information, intellectual property and other critical data continue to make headline news.

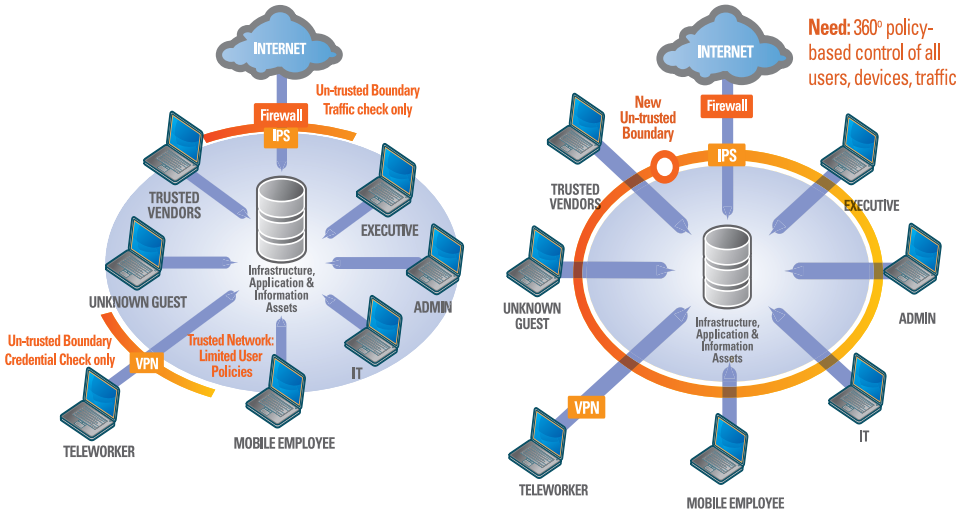
The evidence is clear – organizations are challenged just as much by internal attacks as they are by attacks coming from outside of their "network boundaries." With the advent of distributed Internet connectivity, VPNs, wireless technology, laptops, network-connected PDAs, and extranets, enterprise networks are now 'borderless.' The modern workforce of internal employees, contractors and consultants telecommute and/or regularly connect to the network from home via the Internet – and not just for e-mail – but for accessing critical internal information. This increased connectivity has led to enormous employee productivity for those who depend on easy access to information resources anytime and from anywhere, but has also created a security nightmare. Consequently, organizations realize the need to enforce granular network access policy for all forms of external access as well as internally tethered endpoints.

Further, companies can no longer just focus on securing business assets for their own survival. They must now demonstrate appropriate security measures and practices to avoid embarrassing public exposure and penalties or lawsuits from failing to meet government compliance regulations.

These needs have ushered in a new defense in depth approach to security – Network Access Control (NAC). NAC is an intelligent network solution that can identify devices trying to enter a network, perform integrity checks on those devices, identify the user on the device, and grant conditional access to specific locations or resources based on an integrated network access policy. More advanced forms of NAC take the model even further. Rather than performing those steps only at network entry, full post-admission security, including intrusion detection and prevention at the session level, can now be utilized to create a powerful security policy around each user/device at network entry and for the duration of their time on the network. This shift in how network access is granted and how network policy is enforced fundamentally shrinks the network "perimeter." Previously, policy control was about access into the trusted network; now, organizations have the ability to control network compliance across many entry points on a continuous basis.

Figure 1

Previously, policy control was about access into the trusted network; now, organizations have the ability to control network compliance across many entry points on a continuous basis.



The potential for NAC, particularly when combined with powerful and effective network-based intrusion prevention, is both enormous in and of itself, as well as disruptive to a number of stand-alone security devices. Having policy-based control over who and what is on a network at all times; being able to stop unwanted intrusions and asset uses; having the ability to prove solid IT practices and security governance; and doing so while simultaneously lowering IT cost of ownership; is driving organizations of all sizes to invest in NAC.

Evolving Security Landscape

Organizations today face many information security threats and challenges, including:

- Borderless business boundaries

  Mobile users connect laptops and handheld devices to airports, home, hotel, and coffee shop networks, and then reconnect to the corporate office. Remote-access users connect from homes and public locations. Partners, suppliers, contractors and guests all have access to the network – some deeper than others. Even traditional 'fixed location' workers can introduce threats through Internet access, e-mail, instant messaging and peer-to-peer applications. Traditional security defenses like perimeter firewalls and selective VPN appliances are simply inadequate in today's borderless organizations.

- Financially motivated attacks and exploits

  The days of script-kiddies breaching a network out of curiosity or hacker-community notoriety are not gone, but are now trumped by attacks and exploits motivated by profit and financial gain.

- Zero Day Impact

  The time between vulnerability discovery and the production of exploit malware has been reduced from months to hours in many cases. Network or system downtime, recovery, and clean up from these threats remains expensive.

- Corporate governance and compliance

  Increasing concern and risk over being out of step with regulatory compliance requirements like

HIPAA, SOX, GLBA, PCI DSS, SB 1386, etc. can result in fines, penalties, press exposure, stock valuation hits, and even criminal repercussions for senior management

New Network Security Requirements

Given these exposures, enterprise customers are looking for a new level of network security that meets the following requirements:

- 360° policy-based control – capable of enforcing policy-based network access and use control around the entire 360° perimeter – including all internal wired and wireless ports, VPN and traditional WAN perimeter points
- Comprehensive security policy scope – capable of enforcing not only 'point in time' user/device admission policies on entry and at some post-access interval, but also integrating with 'continuous traffic' (flow) policies – since that is the most effective way to think about the problem, and the most comprehensive way to think about policy construct
- Flexible enforcement – to accommodate different risk tolerances for different types of users or areas of network entry
- Non-disruptive deployment – minimal impact to network infrastructure, user experience and application performance
- Affordable – the above must be available in the $15-$50 endpoint range in order to fit within an increasingly tight security wallet and must lower cost of ownership for an already strained IT/security workforce

NAC Defined

Network Access Control (NAC) is a network security mechanism that enables policy-based management of which devices and users are allowed on a network and what resources they are allowed to use, based on something known or unknown about the user or device. Typically, NAC solutions perform the following functions:

- User authentication – usually via credentials already stored in existing network access infrastructure servers including Active Directory, LDAP-based directories, etc.
- Device integrity check – O/S type, configuration, and patch level; personal firewall and AV presence, activation, configuration, patch level; presence of malware (or benevolent but undesired protocols or services) emanating from the device. Integrity checks can be performed passively by a dissolvable or permanent agent
- Authentication / integrity / authorization policy check – compare the authentication and integrity check results against policies in the NAC policy server database. Functional integration between the NAC policy / services server, network admission point (wired or wireless Ethernet switch, VPN concentrator, WAN gateway device), and back-end user / device data repositories (DHCP server, RADIUS server, Active Directory, LDAP, etc.) is required to exchange information about a device / user pair on network entry so a policy-based entry decision can be made.

- Admission policy enforcement – make a decision about what a particular user can do, given the results of the authentication and integrity check. Enforcement options can include block, alert, allow, quarantine and force to remediation, rate-shape, selectively allow at protocol or service level, etc. Once a policy decision is made, the policy server instructs an enforcement point (DHCP, appliance, 802.1x switch, etc.) to perform the appropriate enforcement action.

- Audit / compliance reporting – provide audit and forensic reporting capabilities for proving security policy adherence, as well as evaluating where to tighten or loosen policy according to desired security posture

What NAC Provides

The decision to investigate and ultimately deploy NAC is typically driven by one or more of the following recognized enterprise IT / security needs:

- Protect corporate resources from unauthorized users

- Provide controlled access for contractors, partners and/or guests

- Demonstrate adherence to security / access policies for external compliance purposes, with primary external compliance drivers including Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Act (FISMA), Cardholder Information Security Program (CISP), Payment Card Industry Data Security Standard (PCI DSS), Gramm-Leach-Bliley Act (GLBA), Basel II

- Protect network infrastructure including isolation and segmentation of wireless and wired access and securing non-standard devices (printers, control systems, etc.)

TippingPoint NAC

The TippingPoint NAC solution enables enterprises to enforce device and user policies to ensure endpoint compliance and granular network compliance even after initial network entry. In a TippingPoint NAC environment, access policies subject each device and user pair to rigorous authentication, authorization, posture compliance checks and enforcement. Non-compliant devices are directed to remediate based on policy class. User access rights are controlled through integration with existing rights management systems including Active Directory, LDAP and RADIUS.

There are three elements to the TippingPoint NAC solution:

1. NAC Policy Server
2. NAC Policy Enforcer (optional)
3. Endpoint Posture Agent (optional)

1. NAC Policy Server

The NAC Policy Server provides centralized policy management as part of the TippingPoint NAC solution and offers advanced reporting and event correlation. The centralized Web-based console allows network administrators to quickly scan through the entire network, in real-time, and view

the activity and performance of all users, applications, connections and devices. This greatly reduces troubleshooting time and expedites problem resolution.

The NAC Policy Server economically scales to accommodate network infrastructure growth of users, groups and applications using a variety of enforcement methods including the inline TippingPoint NAC Policy Enforcer appliance, DHCP and 802.1x. A single NAC Policy Server can support up to approximately 10,000 users. The NAC Policy Server works in concert with existing or newly deployed directory infrastructures, including RADIUS, multiple EAP types and 802.1x authentication as well as Active Directory support with the convenience of a seamless Active Directory login. It also supports other LDAP-based directory structures. Network activity can be tracked and enforced by user, group and destination, and network connections are tied to MAC address, IP address and username. The NAC Policy Server enables provisioning of internal users, authorized guests and remote employees. Because the NAC Policy Server spans the network infrastructure, it can support wired, wireless and remote users.

2. NAC Policy Enforcer

The TippingPoint NAC Policy Enforcer is an optional in-line appliance that provides access control enforcement based on user and device criteria from the NAC Policy Server. It allows network administrators to designate access rules based on user identity and device type, rather than traditional port-based segmentation that may only restrict by location. As consultants, contractors and guests are authorized for internal network access, an inline enforcement tool based on identity is necessary to permit only eligible users onto the network with access to designated authorized resources. Working with the NAC Policy Server, the NAC Policy Enforcer receives up-to-date policies for any new connection on the network and receives any changes in a user's authentication state, time and location-based rules.

The TippingPoint NAC Policy Enforcer sits in-line on the network as a layer 2 bridge, and is typically deployed at the network core. Operating at Layer 2, the NAC Enforcer is transparent to Layer 3 networks and does not require changes to existing Layer 3 infrastructure or IP address allocations. A single NAC Policy Enforcer supports approximately 500 users and has four external 10/100/1000 copper ports. The NAC Policy Enforcer is also equipped with availability features including redundant power supplies and fans and supports stateful failover options.

3. Endpoint Posture Agent

The endpoint posture agent can be utilized on devices either as a permanent client or a dissolvable agent. It supports Windows NT, 2000, XP, Vista, Apple OS Leopard, Apple OS Tiger and Linux operating systems. The agent can be deployed to determine endpoint compliance regarding O/S service packs, patches and hot fixes, installed, running, and up-to-date anti-virus, anti-spyware, and personal firewall software. Agents can be set to check endpoint

posture and status at configurable intervals and ongoing heartbeats.

Taking NAC to the Next Level

Everything described to this point is what any buyer should expect of a traditional NAC solution. However, from a 360° perspective, if this is all that is considered to secure an enterprise, the problem that needs to be solved is only half complete. NAC has traditionally been thought of as a "health check" for machines connecting to the network. Now IT security personnel are recognizing the broader need for post-admission classification, enforcement control and classifying all traffic from the endpoint in real time to look for new policy violations or the presence of security risks.

TippingPoint is not focusing exclusively on NAC because NAC alone can not completely address the full network security need that customers are trying to address.

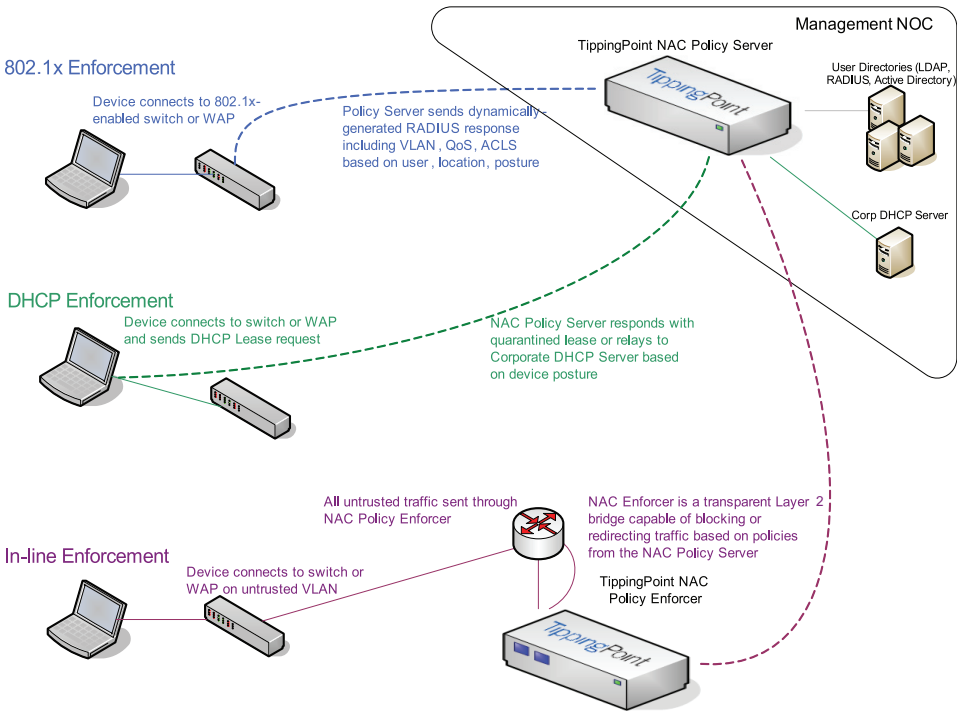
First, let's look at what business TippingPoint has been in – the intrusion prevention business. An Intrusion Prevention System (IPS) classifies flows and then enforces a policy-based action like block, allow, alert, rate-shape, or quarantine. In order to be deployed in-line in a network where you can enforce policy in real time, an IPS must meet a stringent set of engine performance and security filter coverage, speed and accuracy criteria, as shown in Figure 3.

These requirements match up to the principles and philosophy of TippingPoint's Bi-Planar network architecture and lead to what we call IPS-Secured Networks, logically represented in Figure 4.

Simply stated, IPS-Secured Networks convert uncontrolled, unclean devices, users and flows to those that are controlled and clean. The IPS is fundamental to this customer-expressed need owing to its proven deep-packet inspection, classification and enforcement features. NAC

Figure 2

TippingPoint NAC Deployment Options



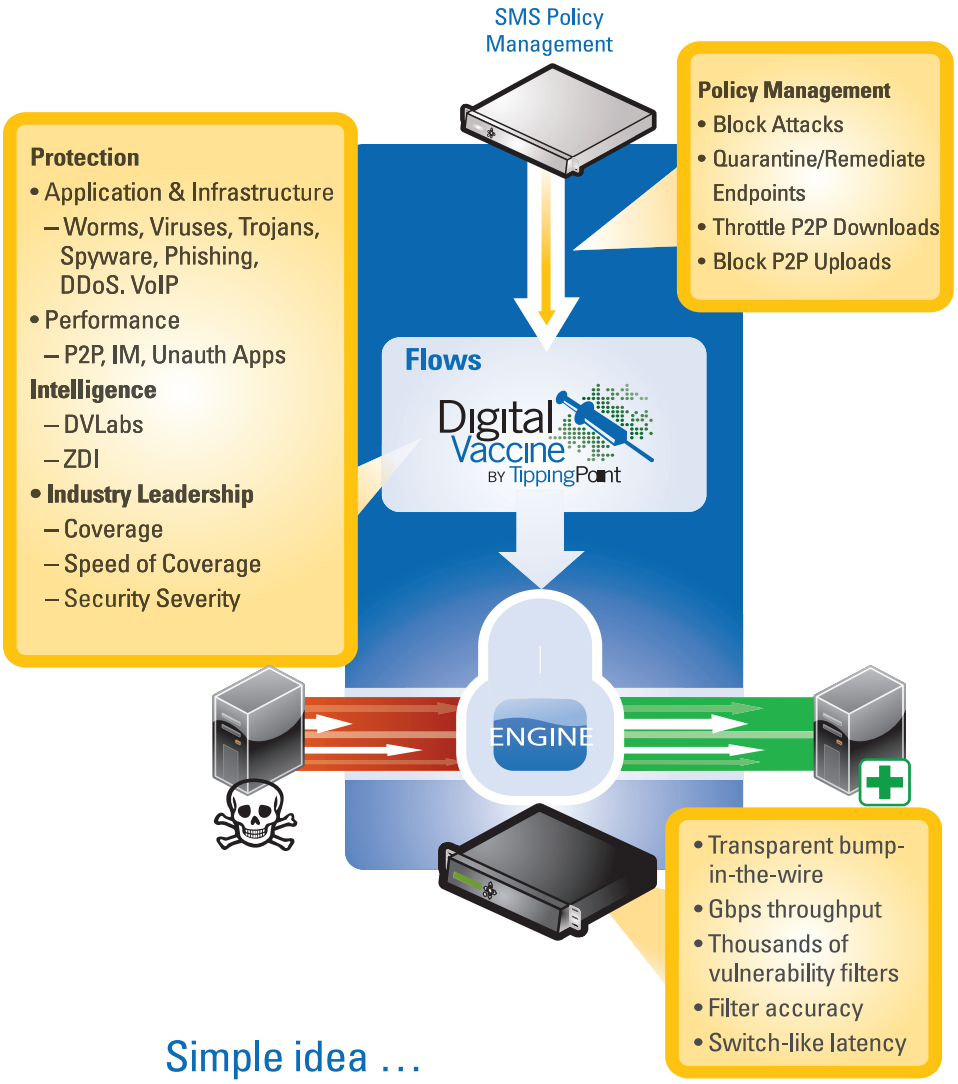


Figure 3
TippingPoint IPS Solution

Simple idea …

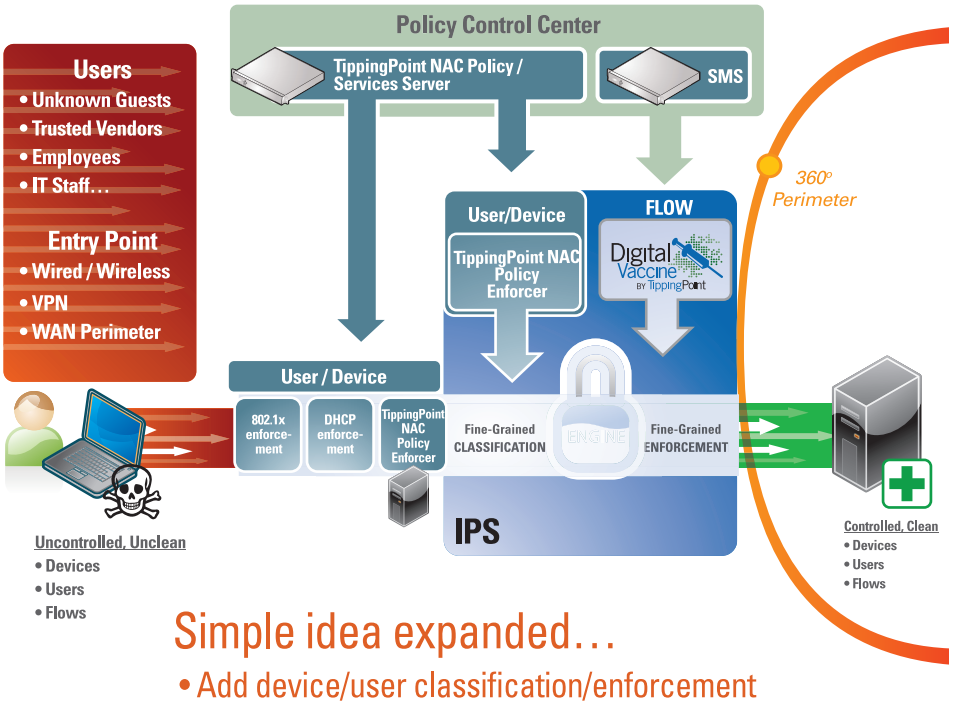
- Transparent, bump-in-the-wire device
- Classify traffic and take action based on policy

has its place, but it is not the end game. Network security in the 21st century requires an integrated ability to policy-control devices, users, and flows to have any chance of addressing the rapidly evolving threat landscape; the difficulties of managing virtually-open networks due to the forces of employee/device mobility; and an increasingly intolerant regulatory compliance environment.

TippingPoint's solution goes beyond traditional pre-check and post-check NAC solutions by linking device and user policies to fine-grained, continuous traffic control made possible only by an IPS. By integrating device, user and IPS-based traffic classification and enforcement, enterprises have much greater control over network access and usage, while reducing network security cost and complexity.

In an IPS-Secured Network, TippingPoint NAC interoperates with the TippingPoint IPS to ensure all malicious traffic is blocked from each endpoint and suspect or non-compliant traffic triggers

Figure 4
Extending TippingPoint IPS with TippingPoint NAC



other policy-controlled actions, including blocking, quarantining, alerting or rate-shaping. Now, network and security personnel have unprecedented control over the entire network perimeter with integrated policy-based visibility and control of users, devices and traffic flows.

The key elements of an IPS-Secured Network are:

- Fine-grain flow classification and policy enforcement – the heart of an IPS and the centerpiece of effective network security in the modern age

- Comprehensive set of enforcement actions including allow, block, alert, rate-shape, redirect, quarantine, etc. (of which there are three options, each covered in more detail below):

  - Allow, Block, Alert, Rate Shape, Redirect – with a TippingPoint IPS inline, legitimate traffic passes freely without false positives; malicious traffic is blocked on a flow by flow basis using highly accurate filters generated by TippingPoint's DVLabs; and alerts are sent to notify administrators that action has been taken. Traffic can also be redirected based on its attributes. The TippingPoint IPS engine performs these tasks at wire speeds with very low latency. In addition, the IPS can be set to rate limit certain kinds of traffic, including application-specific rate limits. These capabilities together with the other quarantine options listed below combine to provide unprecedented visibility and control over network activity of users, devices and traffic flows

  - IPS Quarantine – upon filter violation, all traffic (or selective flow) is blocked from an endpoint. An optional notification panel to the user from the IPS is provided and an option to allow the

endpoint to have a single communication path to a third party remediation appliance is provided

- TippingPoint Security Management System (SMS)-IPS Active Response – upon receipt of notification from a third party control plane device that has determined its own policy violation, e.g., NBAD appliance, a quarantine action can be enforced on its behalf – empowering that device and enabling the customer to leverage a single security investment for all enforcement actions

- Active Response – upon policy violation, an 802.1x-enabled switch or router is signaled via the SMS to perform a quarantine – supporting customers who wish to employ switch-based quarantining only, as opposed to having some endpoint violations quarantined by a switch and others by an IPS

- Ability to keep network security elements 'evergreen' with the latest, most comprehensive vulnerability filters via a world class security intelligence team (DVLabs) and the security intelligence output (Digital Vaccine®)

- Policy management center that provides broad policy construction, real-time management, visibility, and reporting on security activity within the network

  - Broad policy construction enables customers to write policies around device type, device location, user rights, group rights, time of day, etc. For example:

    - All finance users are only allowed to access the SAP server, during business hours, and from internal wired Ethernet ports

    - The CEO, even if infected with a virus on network entry, will still be allowed to access the e-mail server, a remediation server, and the Internet – but all other traffic will be blocked

    - Any employee running a peer-to-peer protocol (typically used for music/video download) – whether on network entry or any subsequent point in time while on the corporate network – will have that traffic rate shaped to a maximum of 56 kbps and will generate an alert to IT

    - IT personnel can access any server, from any location, at any time, but all remote or wireless access events outside of normal business hours will generate alerts to the CISO

- Ability to extend fine-grain classification and enforcement of flows with a 'NAC plug-in' that adds the same level of control over devices and users

- Flexibility of using other forms of NAC enforcement that are either already in place or desired by customers who have varying budget / security risk tolerance zones within their network

IPS-Secured Network Features and Benefits

TippingPoint's IPS Secured Network solution, the integration of TippingPoint IPS and TippingPoint NAC, provides a set of security capabilities that transcend NAC and provide a greater policy control envelope from which to secure a network, its use and the critical information assets within it:

- Multiple NAC enforcement methods – (802.1x, DHCP, in-line) to meet customers budget / risk tolerance objectives

  - For organizations requiring soft enforcement (s/w overlay), TippingPoint can provide that requirement, and initiate and develop the course down the path of employee posture compliance

  - For organizations with parts of their network access layer upgraded to 802.1x, TippingPoint can signal to those elements for enforcement action via the TippingPoint SMS

  - For organizations requiring heavy enforcement, either in hot spots or network-wide, TippingPoint can accommodate this by using IPS's in a highly cost-effective manner without any network upgrade

- Fine-grained NAC enforcement – ability to enforce policy at the individual flow level – so a device / user is not handled in a heavy-handed fashion if unnecessary to do so

- NAC classification and enforcement integrated into IPS fine-grained policy enforcement – making comprehensive device / user / flow policy development straight forward, and preventing expensive dual enforcement investments

  - Combining NAC and IPS forms the basis for an evergreen 'control plane' investment that begins to eliminate network control 'box sprinkling.' Enabling customers to design, implement and enforce network access and usage control around consolidated user, device, and traffic-based policies simplifies network protection and compliance control.

  - NAC becomes a natural extension to IPS – the leading deep packet inspection, classification, and enforcement technology in the marketplace today.

  - That investment can be continually expanded to accommodate application control needs including WAN optimization, traffic visibility and extrusion prevention.

- Comprehensive 'post check' – not only checks device / user profile on a periodic basis, but continuously checks traffic for the duration of the user session, eliminating the greatest risk to the network (dangerous and/or unwanted traffic)

- In-line enforcement performance – proven, consistent network security performance leadership, multi-gigabit throughput, switch-like latency and robust redundancy

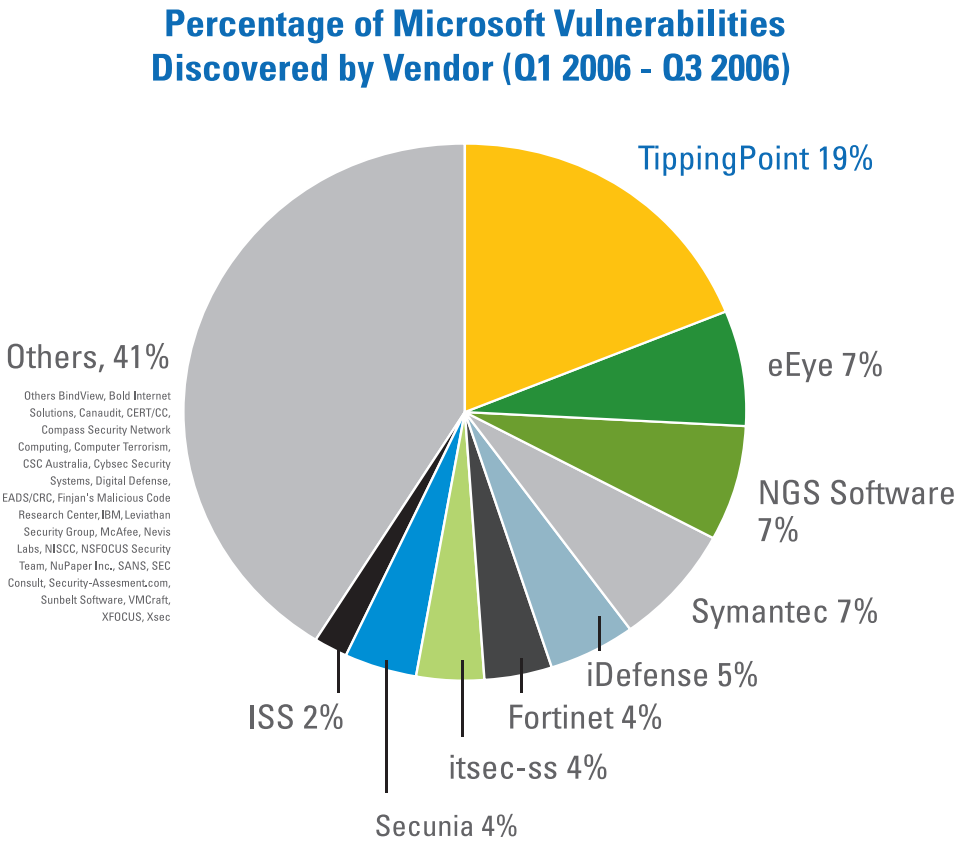


Figure 5

"TippingPoint is the fastest growing discover of new security vulnerabilities, has industry leadership in the percentage of Microsoft vulnerabilities discovered and holds the lead in high severity vulnerability discoveries."

Robert Ayoub, Industry Analyst

Frost and Sullivan

- Vulnerability discovery and protection leadership - clear industry-leader for new vulnerability discovery, severity level and speed of zero-day coverage as evidenced by the latest Frost and Sullivan report[1] on security vulnerability coverage

- Compelling economics - while other vendors will illustrate their NAC device/user policy-based enforcement for less than $50 per endpoint, TippingPoint is the only vendor that can provide 360° integrated policy-based network security (device, user and flow) for less than $50 / endpoint for any enterprise class network (250-10,000+ endpoints)

- Easy to deploy and maintain – TippingPoint NAC does not require any change to existing network infrastructure as it is deployed as a pure overlay. Agent deployment is flexible – ranging from dissolvable to permanent options. Using TippingPoint's existing and proven Digital Vaccine® service for filter and policy updates makes it easy for IT to ensure policy uniformity and rapid modifications

- Minimal impact to users/ applications and business operations – TippingPoint is the undisputed industry leader in 'transparent bump-in-the-wire' security technology. TippingPoint is able to perform deep packet inspection, classification and user/device/traffic policy enforcement at multi-gigabit rates, with thousands of active and highly accurate vulnerability and usage policy filters, all while introducing fewer than 100 microseconds of latency that's virtually undetected by users or applications

Summary

As security threats rapidly become more frequent, targeted and sophisticated, enterprises are tasked with raising the security profile of their networks. Tougher requirements for internal policy compliance and regulatory compliance add even more urgency for organizations to be able to monitor and control their networks. For most, this means implementing network access control, including visibility to endpoints, users, and network traffic, and enforcement of acceptable use of network assets. IT and security organizations are challenged with formulating appropriate network security policy, with classification of users, devices and flows, and finally with enforcement of established policies in a manner that is both timely and cost effective.

TippingPoint NAC combines powerful user and device classification with world-class network policy enforcement via the TippingPoint IPS, as well as providing flexible options for enforcement via 802.1x or DHCP. The ability to set policy; classify users, devices, and traffic; and administer policy enforcement through automated corrective actions like blocking, quarantining, rate-limiting, and alerting enables businesses to better thwart the ever-increasing security threat to their networks from both internal and external sources.

This method of applying 360° Network Access Control with TippingPoint NAC effectively redefines the network perimeter into a model that accounts for the many user types, network access devices, and various paths into the network. Combining visibility and control in this manner enables organizations to monitor network activity at a fine-grained level and to take fitting corrective action, facilitating compliance with internal policy and regulatory requirements.

[1] Ayoub, Robert. "An Analysis of Vulnerability Discovery and Disclosure." Frost & Sullivan, January 22, 2007.

Corporate Headquarters:
7501B North Capital of Texas Hwy.
Austin, Texas 78731 USA
+1 512 681 8000
+1 888 TRUE IPS

European Headquarters:
Herengracht 466, 2nd Floor
1017 CA Amsterdam
The Netherlands
+31 20 521 0450

Asia Pacific Headquarters:
47 Scotts Road
#11-03 Goldbell Towers
Singapore 228233
+65 6213 5999

TippingPoint®

www.tippingpoint.com

503188-004 11/08