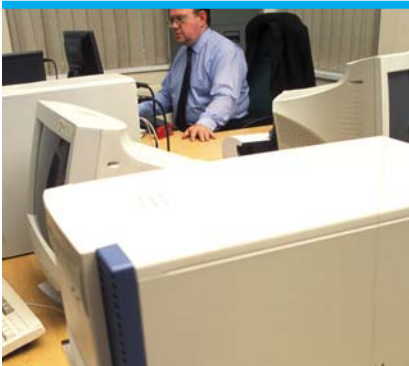




# VULNERABILITY MANAGEMENT TECHNOLOGY REPORT

## nCircle IP360



OCTOBER 2006

# CONTENTS

## nCircle IP360



nCircle, 101 Second Street, Suite 400, San Francisco, CA 94105  
Phone: +1 (415) 625 5900 • Fax: +1 (415) 625 5982

Test Environment and Network .....3

Test Reports and Assessments .....4

Checkmark Certification – Standard and Premium .....5

Vulnerabilities.....6

West Coast Labs Vulnerabilities Classification .....7

The Product .....8

Developments in the IP360 Technology .....9

Test Report .....10

Test Results .....17

West Coast Labs Conclusion .....18

Security Features Buyers Guide .....19



# TEST ENVIRONMENT AND NETWORK



For this Technology Report, West Coast Labs engineers created a network infrastructure similar to that found in most corporate IT environments. Each solution entered into this Technology Report was required to perform vulnerability tests against this network.

The network used by WCL consisted of between 20 and 30 distinct hosts, and included routers, managed switches, network servers, client machines, and printers. Included within the available services were web servers, mail servers, file and database servers. Customized web applications, designed by engineers at West Coast Labs and containing common scripting errors, were installed on servers across the network.

A variety of Operating Systems were used on the network, on different hardware platforms. A number of virtual hosts were also included. In building the network, some of the machines and services were installed with default settings. Various levels of patching were applied across the range of Operating Systems. In addition, a number of common mis-configurations were made in setting up and deploying particular services. Every host on the test network was imaged prior to testing, and restored to the original state before each round of testing for the individual solutions.

The test network was protected by a router, and ACLs were set to restrict access to the test network to and from IP addresses specified by the participating vendor, if appropriate. If the solution under test needed no Internet connectivity then the router was configured to block all access to and from the Internet for the period of test.

The test network was available to each solution for a 48 hour period.

# TEST REPORTS AND ASSESSMENTS

WCL have assessed the individual vulnerability assessment reports from each solution on the following basis, with Vulnerabilities on the target network classified under 4 headings:

**Critical vulnerabilities** – those that allow an attacker with minimal knowledge or skill to compromise the integrity of the network: this may include gaining control of a server or network device, gaining illegitimate access to network resources or disrupting normal network operations.

**Severe vulnerabilities** – those that allow illegitimate access to, or control over, network resources, but that require considerable knowledge or skill on the part of the attacker.

**Non-critical vulnerabilities** – those that allow attackers to gain access to specific information stored on the network, including security settings. This could result in potential misuse of network resources. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on hosts, directory browsing, disclosure of filtering rules and security mechanisms.

**Information leaks** – these allow attackers to collect sensitive information about the network and the hosts (open ports, services, precise version of software installed etc.)

The performance of each solution under test was evaluated on the following criteria:

- The ease of deployment of the solution
- The number of vulnerabilities correctly identified in each class
- The completeness of the report, including identification of any network changes made
- The clarity of presentation of the findings

# CHECKMARK CERTIFICATION

Solutions under test in this Technology Report are eligible for the Checkmark Vulnerability Assessment certification.

In order to achieve the Standard Checkmark Certification for Vulnerability Assessment the candidate solution must identify at a minimum 100% of the Critical Vulnerabilities and 75% of the Serious Vulnerabilities.

However, those developers identifying 100% of the Critical Vulnerabilities and a minimum 90% of the Serious Vulnerabilities will be awarded the Premium Checkmark Certification for Vulnerability Assessment.

[www.check-mark.com](http://www.check-mark.com)



# VULNERABILITIES

To ensure that the test network mirrored that found in many businesses, a variety of operating systems, on different hardware platforms, were included. A Windows domain was set up using a Windows 2003 Server and a mix of workstations running Windows XP and Windows 2000 Professional. Some Sun Servers running various Solaris distributions provided web services and file storage, assorted Linux boxes were included running Debian and RedHat distributions, and a host running BeOS completed the mix.

Some of the servers were installed with default settings and varying levels of patching were applied: some hosts were patched fully up to date while others had been left out of the process. Also, a number of common mis-configurations were made in setting up servers, and deploying particular services. For example, Windows servers were configured with open network shares, ftp servers with anonymous write access, smtp servers configured as open proxies. These are configuration errors that can have profound effects on network security but can easily be implemented by a hard-pressed administrator as a “temporary” quick fix to a connectivity problem.

The Windows 2003 Domain Controller hosted an UltraVNC server using a weak password, the DNS server itself was configured to be compatible with pre-2000 machines. Also installed on the PDC was IIS version 5.0 running default services. Alongside the Primary Domain Controller, a mail server was configured running Microsoft Exchange 2000, and this server also had an instance of UltraVNC running alongside popular game servers with known vulnerabilities.

One of the client machines was host to a vulnerable .ASP script written in-house by WCL engineers. This had a number of common programming errors in it allowing a user to bypass security measures using a number of different techniques.

A bank of Linux machines running a variety of Linux flavors and distributions completed the list of servers. The Linux systems were host to an array of services including FTP, sendmail, apache, and samba. Each of these was mis-configured with common errors, for example anonymous ftp access with write permissions and publicly writeable samba shares.

Each of the user client workstations were patched to different levels using official Microsoft Service Packs, historical patches and Windows Update. These machines then had different applications installed, ranging from popular game servers and UltraVNC through to IIS 5.0 and remote admin. Some machines were included in the Windows Domain. Back Orifice was installed on one machine on an unusual port.

The test network thus consisted of a series of machines with differing hardware specifications, operating systems, patch levels, and software installations, and multiple vulnerabilities. This Technology Report also saw the inclusion of common vulnerabilities found in software from leading vendors used worldwide along with those on the SANS Top 20.

# WEST COAST LABS VULNERABILITIES CLASSIFICATION

As a basis of the test program, West Coast Labs engineers built a series of known vulnerabilities in the network on which each of the solutions was installed. To mimic those vulnerabilities found in many corporate IT environments, the risk level of these varied between Critical, Serious, and Minimal.

As part of the scope of testing and certification, particular attention was paid to how each of the products detected and classified those vulnerabilities deemed by West Coast Labs to be of either Critical or Serious risk.

So that the performance of each product can clearly be understood, this report contains some examples of the types of vulnerability listed as Critical and Serious.

## CRITICAL VULNERABILITIES

- MS-Blaster patches not installed on servers
- FTP server with anonymous, writeable access
- Publicly available file shares using NetBIOS and Samba
- Blank Administrator passwords
- Back Orifice installations
- Open SMTP relays
- Completely unpatched operating systems (base installs)
- Base install of Windows Media Player 9 with no security patches
- Sun Solaris RPC vulnerabilities

## SERIOUS VULNERABILITIES

- Partially patched operating systems to known levels
- Default or weak passwords
- VNC servers
- Popular game servers with known vulnerabilities
- FTP servers with non-writeable anonymous access
- Web sites with back-end scripting vulnerabilities
- Instant Messaging clients
- Virtual office software
- Microsoft Desktop Remote Access

The classification of the above vulnerabilities is based on information provided by external sources including the SANS Top 20, Bugtraq, and other well known vulnerability lists and sites.

# THE PRODUCT

## IP360 FROM NCIRCLE

### nCircle SAYS ABOUT IP360...

nCircle IP360™ is a scalable, enterprise-class vulnerability and risk management system that proactively delivers a comprehensive view of network risk and enables cost-effective risk reduction.  
<http://www.ncircle.com>

### nCircle SAYS ABOUT IP360 BUSINESS BENEFITS...

nCircle IP360™ is a comprehensive proactive security solution that helps organizations cost effectively measure, manage, and reduce network security risk. nCircle IP360's unique, comprehensive risk profiling technology delivers endpoint intelligence that serves as the foundation for a balanced security ecosystem. nCircle IP360 enables organizations to:

- Measure network security risk using objective metrics
- Manage network security risk through dashboard reporting and integration with enterprise systems
- Reduce network security risk by focusing IT resources where they are needed most

nCircle IP360 also helps companies drive continuous regulatory and security policy compliance through endpoint intelligence discovery, risk metrics, and automation.

[www.ncircle.com/index.php?s=products\\_ip360](http://www.ncircle.com/index.php?s=products_ip360)

### nCircle SAYS ABOUT IP360 TECHNICAL BENEFITS...

nCircle IP360™ discovers detailed intelligence about IP-enabled devices on the network, and utilizes best-in-class reporting and analytics to prioritize vulnerabilities and provide a comprehensive view of network risk. Delivered via hardened, non-Windows appliances and designed for scalability, rapid deployment, and ease of management, IP360 is ideal for large, globally-distributed networks.

nCircle IP360 delivers:

- Comprehensive, agentless network discovery and profiling of all network assets
- Vulnerability and security risk assessment across global networks
- Comprehensive, flexible reporting for regulatory and security policy compliance

nCircle IP360 identifies over 1400 operating systems, 3800 applications, and 3500 vulnerabilities, and coverage grows daily.

[www.ncircle.com/index.php?s=products\\_ip360](http://www.ncircle.com/index.php?s=products_ip360)

# DEVELOPMENTS IN THE IP360 TECHNOLOGY

## AS STATED BY nCircle...

nCircle IP360™ was designed from inception to support extreme increases in the numbers of vulnerabilities over time, and it shows in nCircle's market-leading coverage. The product itself was designed to discover – non-intrusively and without using agents – the operating system, applications, and vulnerabilities on all IP-enabled devices.

In the last twelve months, IP360 has gained the ability to gather more detailed information about each device, including specific host configurations such as password requirements and file permissions. Also added is the ability to test for vulnerabilities using credentials via SSH and SNMP, which joins Windows credentialed testing (SMB) and remote, non-credentialed testing as methods of discovery.

## nCircle VERT

nCircle IP360 is backed by nCircle VERT (Vulnerability and Exposures Research Team) ensuring the most comprehensive and current offering in the industry. VERT focuses their efforts on identifying vulnerabilities as they emerge and building accurate, non-intrusive signatures that identify the latest vulnerabilities and applications for nCircle's customers.

## 24-HOUR MICROSOFT SERVICE LEVEL AGREEMENT

nCircle provides customers with a 24-hour Service Level Agreement that commits to provide vulnerability checks, within 24 hours, for all Microsoft Security Advisories. With this guarantee, nCircle's customers can be assured that within 24 hours of the announcement of a vulnerability by Microsoft, nCircle will provide a check with which they can test their systems for the vulnerability. No other vulnerability management vendor has made such a commitment to its customers.

# TEST REPORT

## INTRODUCTION

IP360 is an Enterprise level security solution developed by nCircle that can be deployed in a range of configurations to suit any network environment from a single site to a global infrastructure. The IP360 security solution consists of two separate device types. The first is the VnE Manager, which acts as the controlling unit, and the second device is the Device Profiler or DP for short.



The VnE Manager is of a standard rack mountable size and come complete with all the kit required for fitting. Taking off the removable faceplate gives access to the removable RAID disks as well as the onboard DVD and floppy disk drives. Also included on the front of the device are USB and VGA ports providing the ability to quickly attach a monitor and keyboard if necessary.

The rear of the box provides two further USB interfaces and a PS2 keyboard port, a VGA port, and three network connections. One of these NICs is reserved for a console connection.

The DP is physically smaller in size than the VnE, ideal for global based companies shipping a number of these units to a variety of locations. Similar to the VnE, the DP is also rack mountable. Connectivity is provided by a number of interfaces situated on the back panel of the unit, and include PS2, USB, RJ45, and VGA connections.

As a precaution against data theft, all information gathered by the DP is reported directly to the VnE Manager over a secure connection. Further to this, the DP contains no internal hard drive but boots directly from a front mounted Flash Disk. This adds yet another layer of security.

Multiple instances of each device can be deployed with the option either of having a series of DPs all reporting to the one VNE Manager or having clusters of DPs reporting to their own VnE Manager on a per site basis.

# TEST REPORT



## DEPLOYMENT - INSTALLATION AND CONFIGURATION

The initial setup and configuration of the VnE Manager may be performed either across a serial connection based console or by plugging a keyboard and monitor directly into the appliance. Upon connecting to the VnE Manager via the console port, the user is presented with a clean and easy to use interface and is asked to enter standard networking information including the addresses of the gateway and name server, as well as a private IP address.

There are a number of other options accessible from this console, including diagnostic tools. These tools provide the user with the ability to perform a basic set of network tests to check for connectivity, for example providing ping and traceroute functionality.

Also available is the ability to manage and update the applications within the IP360 solution. Updates can be performed from this console either via a live network connection or by manually downloading the updates onto CD/DVD and inserting the disc into the aforementioned drive.

Connecting to the DP, either via serial cable or plugging in a monitor and keyboard directly, gives access to a UNIX based console. This provides similar tools to those on the VnE Manager such as the ability to run pings and traceroutes along with diagnostic functionality to configure the local network address.

The time required for this phase is minimal and both appliances can be quickly setup and ready for further configuration.

# TEST REPORT

## THE MAIN INTERFACE AND SCANNING

On completion of the initial configuration, the user is then able to connect to the well-constructed and intuitive secure web interface for IP360. Within this interface the Administrator can complete the remaining configuration tasks such as the creation of user accounts.

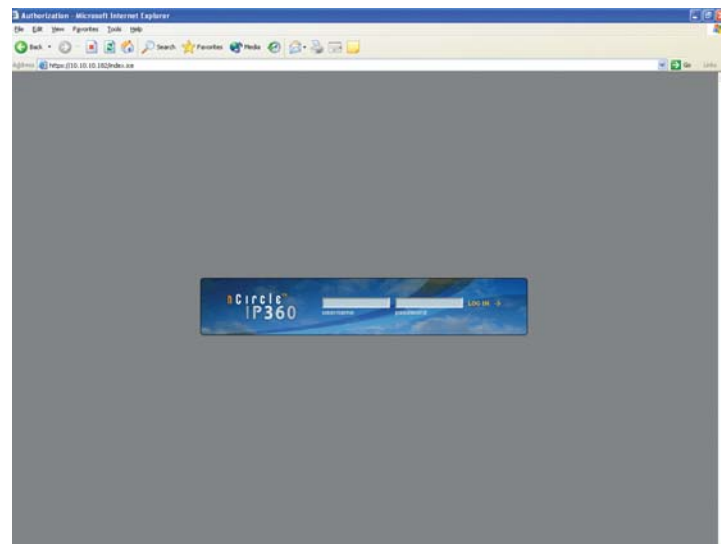
When creating user accounts, the Administrator can specify the individual time zone of the user along with the user group and the role that the user will fill. Assigning these users to groups and handing out specific roles allows for greater control over the management of IP360, whilst still allowing some of the responsibility to be devolved.

To assist with the construction of a user base, IP360 provides the ability to import a list of users directly from a .CSV file. Once the process of creating the users is finished, the status of each user can be ascertained with the help of coloured markers. These markers appear next to each name and are coloured green, grey, or red showing the user as online, offline, or locked out respectively.

User activity can be further monitored through the use of the audit tool that reports on any actions taken by each

of the individual users. The Administrator can select one or more of the created user accounts and search for entries relating to a host of different categories over varying time frames.

These searches can either relate to the more common login and logout events, or widened to include changes to specific system settings. With the use of this in-depth auditing tool, a very clear audit trail of events can be constructed that records the actions of every individual user.



# TEST REPORT

Networks may be created as either individual IP address ranges or, usefully for the larger companies working across multiple sites, as network groups. Those networks created as a group are shown in a network tree, clearly displaying which network belongs to which site.

As an example, an Administrator might choose to group all Linux based machines inside a particular office separately from those running Windows, and using IP360 they could be entered as different network groups that belong to the same site. This provides an Administrator with great help when dealing with an organization that uses hundreds of IP addresses across dozens of ranges and physical locations.

Before starting the first scan a Scan Profile must be created, and it is here that options relating to information including scheduling, credentials, and ports are configured. Also configured are options connected to the depth of scanning, most notably IP360's Application Scan. This tool can be used to accurately identify the specific applications in use on each machine, in turn this aids in the discovery of any associated vulnerabilities.

In order to mitigate the effect scanning has on a network, IP360 can be configured to limit the volume of network traffic being generated on a per second basis and scans can be set either to run at a specific time or to be run continuously. Using this latter option allows the administrator to constantly be aware of any new vulnerabilities that appear on the network.

A limit can be set on the number of instances per day that an individual scan can be run, while a time window can be designated for scans that create a high volume of traffic. The administrator is, however, still free to run an on-demand scan at any point using any of the created Scan Profiles.

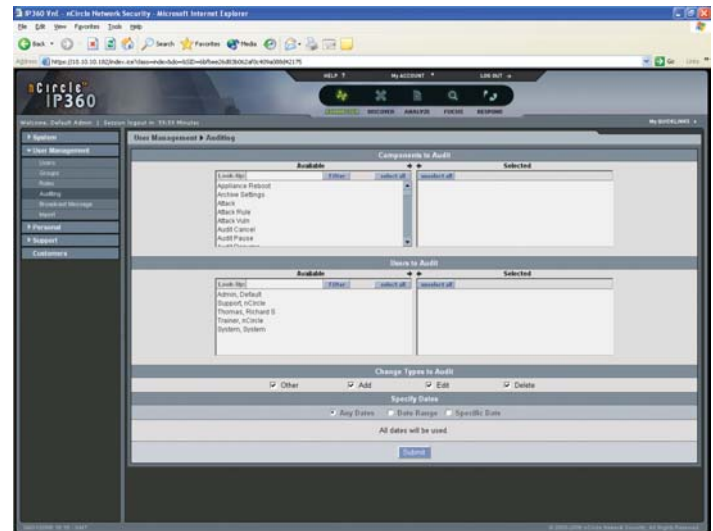


# TEST REPORT

One of IP360's key features is Host Policy Baseline, which is the ability to assign any given host as the standard to which all other hosts should be compared. In effect, this allows the user to spend time configuring one single machine to perfectly match their organization's security policy and then to scan the network or networks looking for those workstations that deviate from this standard.

The use of this feature can reduce the inherent risk of false positive results.

Host Policy Baseline will aid in immediately identifying programs and applications that are either installed by a user or any other means such as malware.

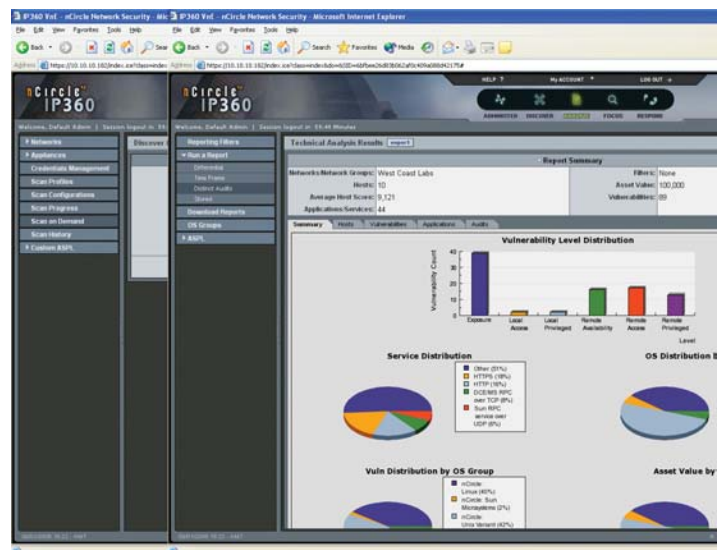


## REPORTING

Detailed reports can be created that include a wealth of information to aid the removal of vulnerabilities from a network environment. By clicking on the Scan History link, a list of every scan recently performed is displayed. This list can be sorted by various fields including the network group, the Scan Profile used, and the DP used.

The data generated in these reports includes a summary of the occurrences of each individual vulnerability, information about each discovered host, and a list of discovered applications. Also available is a list of every discovered vulnerability that are scored anywhere between 1 and 40,000.

Using this highly granular scale, the IP360 gives each discovered vulnerability a unique score. This is instead of a series of vulnerabilities all listed as critical, thus giving the administrator a clear indication of the most serious vulnerabilities.



# TEST REPORT

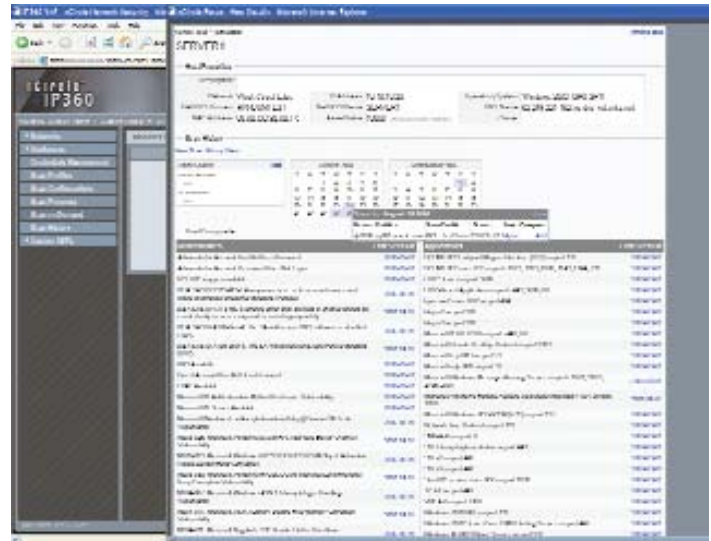
In all areas of use the IP360 endeavours to present as much information to the user as possible and nowhere is this more obvious than through the use of the solution's Focus feature, another technology unique to nCircle. This powerful tool allows the administrator to view and compare all data relating to their network and with proper use can greatly enhance the ability of a network security team to identify and remove network vulnerabilities.

One use of Focus is to display results for a specific machine. At the top of the page, basic information relating to the machine is displayed including the domain name, MAC address, operating system, network group, and network address.

Continuing down the page, a series of calendars display each month the machine was scanned; highlighting the specific dates. Clicking on these dates opens a small pop-up window that lists the DP and Scan Profile used to run the scan, along with the resulting vulnerability score. There is also an option for comparing the scan results from different dates to help detect any potential trends.

Tables containing lists of vulnerabilities and applications detected on the machine take up the bulk of the screen; each individual entry into these tables provides a hyperlink to further data relating to the item.

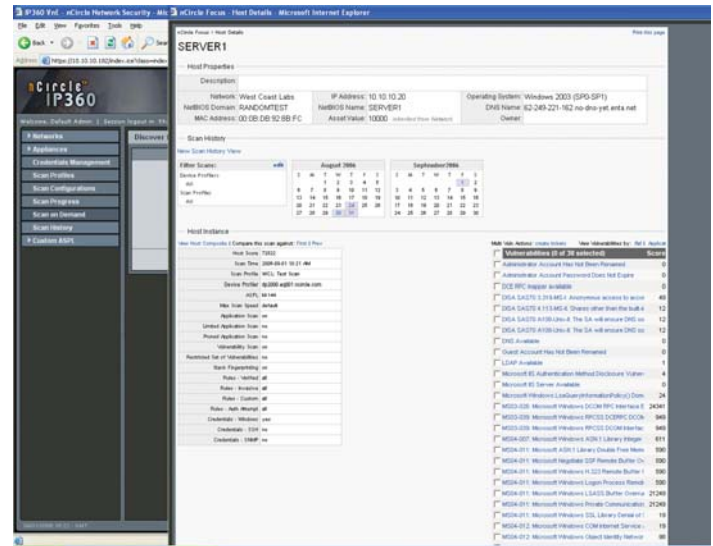
Clicking on an entry will display nCircle's ID for the vulnerability along with the score, approximate skill required to take advantage of the vulnerability, and the type of solution available. Following on from this information, nCircle presents a more detailed description of the solution along with a comprehensive solution to it's removal.



# TEST REPORT

A key feature of IP360 is its ability to assist first and second line support teams that use Remedy to manage support calls. Using the interface available on IP360, an Administrator is able to create a ticket relating to a specific vulnerability on a specific machine and IP360 can then automatically send this ticket on to Remedy.

If a support engineer then works on a specific vulnerability and closes the ticket, IP360 automatically scans the machine again looking for any trace of the vulnerability, re-opening the ticket if the fault is again found.



## TEST RESULTS

---

IP360 performed well during testing, maintaining a high degree of detection while supplying a vast amount of analytical data.

Of special recognition is IP360's Focus feature, use of which allowed data to be thoroughly examined during testing and would be a very useful tool for any network Administrator.

IP360 successfully detected 100% of the Critical vulnerabilities and over 90% of the Serious vulnerabilities on the West Coast Labs test network. The IP360 appliance has been awarded the Premium Checkmark Certification for Vulnerability Assessment.



## WEST COAST LABS CONCLUSION

nCircle's IP360 is a powerful vulnerability management solution providing strong security solution for any corporation looking to protect themselves in an increasingly hostile IT world.

IP360 provides a significant amount of information that is analyzed and categorized using powerful reporting and analytical tools unique to nCircle, allowing Security Administrators to quickly target, remediate or remove vulnerabilities.

The high level of scalability provided by the solution can help mitigate threats to even the largest of IT infrastructures.



# SECURITY FEATURES BUYERS GUIDE

## AS STATED BY nCircle...

- **nCircle Focus** – A new feature of IP360, nCircle Focus is a real-time data synthesis and active analysis tool that enables security professionals to immediately assess network risk and focus their actions. Focus is a unique tool and a major advancement that breaks from traditional reporting paradigms, offers security analysts instant and unparalleled insight into risks on their networks, enabling security professionals to take the most efficient actions to proactively reduce their network security risk.
- **Comprehensive Network Profiling** - IP360 discovers all hosts, applications, services, and vulnerabilities, providing a comprehensive view of your network and building the foundation for effective risk management and compliance processes.
- **Granular Scoring and Asset Values** – IP360 discovers a wealth of data about the hosts that reside on a network, but rather than provide that data in an endless list like traditional solutions, IP360 prioritizes remediation tasks, enabling users to focus on the items that will most effectively reduce risk on critical systems. IP360 utilizes a highly granular scoring methodology, system asset values, and optionally network topology information to provide true prioritization.
- **nCircle Topology Risk Analyzer™** - nCircle Topology Risk Analyzer™ incorporates network topology, or “line of sight”, risk analysis into nCircle IP360, providing an order of magnitude improvement in prioritizing vulnerability remediation. The Topology Risk Analyzer enables IT staff to identify the top few vulnerabilities from the thousands on their networks that will most effectively reduce risk on critical systems. Only nCircle offers this breakthrough technology as an integrated option in a vulnerability and risk management solution.
- **Integration/Open Architecture** - IP360 utilizes open standards, enabling the integration of vulnerability and risk management into existing business processes and IT systems such as help desk, asset management, and other security solutions. The comprehensive endpoint intelligence gathered by IP360 can be leveraged to enhance existing solutions and drive automation within the security ecosystem through nCircle’s command-and-control API.
- **Architecture** - IP360 was designed from inception for large, global deployments, centralized management, and maximum data security. A typical deployment consists of a central VnE Manager console appliance, and one or more distributed Device Profiler appliances allocated based on number of hosts and network layout. Device Profilers discover all IP-enabled devices on the network, profile the operating systems, applications, and vulnerabilities on each host, and communicate the information back to the VnE Manager for consolidation and centralized reporting.

# SECURITY FEATURES BUYERS GUIDE

- **Appliance-based** – All IP360 appliances employ a hardened (non-Windows) operating system with all non-essential services and hardware ports disabled to ensure that they introduce no new vulnerabilities to the network. All communication between the IP360 appliances is encrypted and authenticated using 128-bit SSL to protect the integrity and confidentiality of vulnerability information in transit. IP360 Device Profiler appliances use flash-based storage with no local hard drives to ensure that no vulnerability data is ever at risk on the distributed Device Profilers.
- **Centralized Reporting** – nCircle IP360 provides an easy-to-use Web interface for all functions including administration, configuration, reporting, and workflow. Customized reports are available for all audiences, from technically-focused security administrators to executives, providing an objective and comprehensive view of risk on the network.
- **Scalability** - IP360's distributed architecture enables scalability from small departmental networks to the largest global enterprise, delivering rapid deployment and automated product updates to eliminate the burdens of traditional software maintenance. This design also localizes audit traffic to reduce bandwidth consumption and avoid network bottlenecks. IP360's distributed architecture and centralized management enables organizations to rapidly and cost-effectively scale the system without further investment in IT resources.
- **Role-based Access Controls** - The industry-best Role-based Access Controls within IP360 enable customers to align remediation policies to internal security and ownership policies to ensure individuals can only remediate and report on hosts and networks assigned to them.
- **Host Policy Baselineing** - Using IP360, organizations may define a "gold standard" system based on the operating system, applications and vulnerabilities. They may then quantify the business risk associated with that host, and measure other hosts against that standard.