beyondsecurity
by HelpSystems

primenet

7 Best Practices for
Vulnerability Assessment & Management

A Guide for Effective Enterprise VAM

Table of Contents

Executive Summary

7 VAM Best Practices "In-A-Nutshell"

This eBook provides guidance on 7 best practices for getting the most value out of a vulnerability assessment and management program, including:

1. Developing a Vulnerability Assessment and Management Program	Why your organization needs a VAM plan and what it should include
2. Scan Broadly for Vulnerabilities	What systems should be scanned for maximum effectiveness
3. Ensuring Accuracy in Vulnerability Assessment and Management solutions	How to scan accurately, including minimizing false positives and to obtain actionable information
4. Scanning Frequently to Close the Door on Network Attacks	How frequent to scan assets for timely remediation of risks
5. Managing Vulnerabilities Based on Priority Versus Patching Everything	How to best prioritize and implement remediation steps to reduce risk to information
6. Leveraging the Best VAM Deployment Model for Your Organization	How to best align vulnerability scanning on a distributed and sometimes complex network
7. Ensuring the Leverage of High Impact Security Tools	How to leverage other security investments for maximum value

This eBook is sponsored by Beyond Security, a trusted vendor of vulnerability assessment solutions. To see how Beyond Security can help your organization feel free to contact them.

Best Practice 1
Developing a Vulnerability Assessment and Management Program

No single security solution can solve the entire security puzzle. Endpoint protection can't guarantee that workstations will be forever free of viruses and malware. Firewalls and IPS can't guarantee data on a database server won't be compromised. Access control can't guarantee the integrity of passwords. Etc. etc. So, information security becomes a constant balance of implementing information security technologies and processes with the broad goal of minimizing the risk of compromise to networked assets, while at the same time aligning with resources constraints of the business.

Prioritizing which information security technologies can seem overwhelming to even the most seasoned IT security professionals. Compounding the problem is that many industries have strict mandates on specific information security controls. Fundamental to any security program is having a proper information security plan in place that defines targeted security controls, and how to measure the success of the program.

VAM Is High Impact Security Control

Implementing an information security plan requires a commitment across the entire organization, including managers and senior executives. An effective security program requires dedication, by the organization at all levels, to put proper people, process, and technology in place to achieve the primary objective of reducing the risk of compromise to data.

The information security plan adopted by an organization will often align with one or more industry-specific regulations (e.g., HIPAA, PCI-DSS, SOX, etc.) and security best practices (e.g., the Center for Internet Security, ISO, etc.). A proper information security plan will contain multiple "security control" areas that outline a plan for implementing a specific information security concept. Although information security can often seem overwhelming, security practitioners have made great strides documenting security best practices that include excellent guidance for organizations, including providing guidance on security controls with the highest impact, like Vulnerability Assessment & Management (VAM).

VAM is a high priority security control across all compliance standards. At its core, VAM is an important data loss prediction tool. It will find the weaknesses that attackers will use to gain access to networked assets. Regardless of how an attacker may address your network or what means may be used to gain an initial foothold, every successful attack will use, at one stage or another of their journey deeper into the network, a KNOWN vulnerability that could have been found by VAM and that your security team could easily fix – with sufficient resources.

Any organization that is serious about information security should ensure a well-defined vulnerability assessment and management plan is in place and implemented to help ensure fixing vulnerabilities before hackers find them. A key consideration for any VAM plan is that it ensures all vulnerabilities are quickly discovered, prioritized, and documented.

VAM, an Essential Piece of the Security Puzzle

Almost every successful attack exploited known and well-documented security vulnerabilities in software, network infrastructure, servers, workstations, phone systems, printers or employee devices. Security flaws are constantly discovered and addressed by security patches and updates.

Even in modest networks, keeping all assets up-to-date on all security patches is difficult. A single host that is missing patches or that didn't get them installed correctly can compromise the security of the entire network.

There exists an element of balance and compromise as not all vulnerabilities are created equal, and not all assets are of equal importance or are equally available to a hacker's access. That is where good management comes in. No security effort has an unlimited budget, so VAM helps focus the available resources on the most serious issues that exist at any one moment. It is often much easier to fix a known vulnerability before the expense and effort incurred to react and respond to a breach after it occurs because of an unaddressed vulnerability.

Best Practice 2
Scanning Broadly for Vulnerabilities

Many vulnerability assessment and management deployments are more susceptible to being poorly implemented than most any other security solution. It is common for a company to implement their VAM solution to only a small portion of the network instead of all areas where a compromise would impact the integrity of corporate data. Scanning 10% of a network's hosts is like installing Antivirus on 100 endpoints out of 1000 or setting up just a subset of the firewall rules required for proper firewall security.

Organizations need to ensure vulnerability scanning is done broadly across all networked assets.

Don't be susceptible to the path of least resistance to achieve a VAM compliance checkbox by scanning only a minimum number of IPs as infrequently as possible. Get more out of your existing VAM. Use VAM broadly and frequently to find the vulnerabilities attackers are looking for and fix them, instead of purchasing layer upon layer of new security solutions with the intention of simply hiding vulnerabilities. Your network has known vulnerabilities. Don't try to hide them, but rather use VAM to find and fix them.

How Hackers Bypass Network Security

In almost all successful attacks, hackers bypass the network security perimeter to exploit existing vulnerabilities inside the network. The fact that all hackers consider breaking the perimeter to be job #1 and that most refer to it as being a trivial achievement should be a wakeup call.

In fact, most of the successful attacks are on networks whose admins (or entire security teams) were doing their best to maintain a tight perimeter! These breaches include the highly publicized break-ins at companies like Target and Equifax, and governments with large network security staffs and deep pockets. Apparently, something about the focus on perimeter defense is not working. Yes, the well-tended perimeter stops a great number of attacks, but the fact is, it only needs to be breached once.

Just because a vulnerability is blocked upstream in the network does not eliminate the risk of compromise by malware introduced into the network by the plethora of devices that may move in and out of the network daily.

Some political and financial high-value targets get bombarded with persistent planned attacks. However, most attacks are 'drive-by' in nature.

Attackers don't usually choose a target first and then spend time looking for a weakness. It is far easier to study up on a well-known vulnerability, scan broadly for ANY network that has this weakness and then exploit it to gain access.

From that beachhead, hackers expand their control through the network and then look for the most valuable data they can steal.

Prioritized vs. Full Coverage Scanning

Many organizations believe that only scanning high priority/sensitive systems is sufficient. However, considering that any device on a network can be subject to a compromise, it is important to mature VAM such that scanning of every device on the network occurs on a regular basis. As mentioned previously, scanning should not just include perimeter devices or high priority devices.

A proper VAM implementation should scan all networked assets including:

- devices that leave and rejoin the network (e.g., laptops, mobile devices, etc.)
- infrastructure devices (routers, switches, WAPs, etc.)
- network appliances (e.g., printers, IOT, cameras, etc.)
- servers (e.g., web, application, database, etc.).

A compromise to these systems can provide just as big a headache to an organization to a breach of the network perimeter. It is important to introduce priority concepts into a VAM implementation so that a proper assessment of impact can be measured both in the detection and remediation of vulnerabilities. For example, organizations will benefit from having a solution that incorporates scoring methods for things like asset business value and vulnerability risk scoring into the VAM capabilities.

Therefore, to better secure any network, these well-known vulnerabilities must be found, prioritized, and fixed regardless of ANY set of perimeter defense solutions being in place across all devices on the network.

Best Practice 3

Ensuring Accuracy in VAM Solutions

Accuracy is Vital in Vulnerability Assessment and Management

Testing for Behavior vs. Version

The primary benchmark for evaluating VAM solutions should be accuracy in testing. Ease of use and clear, actionable reports are important, but if accuracy isn't there, then little else matters.

Poor accuracy in VAM produces two kinds of testing error. Overlooking a vulnerability (a false negative) leaves an unaddressed security flaw. Reporting a vulnerability, when in fact none exists (false positive), sends you on a wild goose chase. Obviously, you don't want either. An inaccurate VAM will give you both and cost your team time, money, and valuable resources.

If the first four vulnerabilities reported by your solution didn't exist upon close examination, it becomes pretty difficult to take the 5th vulnerability it reports seriously. 'Crying wolf' creates complacency. A VAM report that says there are dozens of serious security issues when there are only 2 is more distraction than assistance. How valuable is your time? Your security budget doesn't get larger just because your VAM system says there "may be" dozens or hundreds of vulnerabilities on your network. The hidden cost of an inaccurate VAM system is the resource hours it takes to chase false positives, prove that they are false and check them off the list The total cost of ownership of a VAM system with a 5 to 8% false positive rate is double the cost of an accurate system when including the time to verify and eliminate false positives. Even a 2% error rate can be a headache.

Nearly all VAM solutions depend upon version checking as their primary method of assessing the relative vulnerability of network hardware or software. Most VAM solutions look at the response header and from the version data reported there they deduce whether the hardware or software has a vulnerability. If an old version is known to have five vulnerabilities and the header says that the old version is in use, then it is assumed that all 5 of those vulnerabilities exist.

Version Analysis Alone is Not Enough for Effective VAM

VAM solutions that only do version checking may look good on paper – but in practice will come up short. Version checking is easy to program so VAM solutions that don't have more advanced capabilities will often inflate the number of tests they can run. Unfortunately, this results in more noise than value for the company using the solution.

The disadvantage: Poor accuracy misses real problems and lists dozens if not hundreds of vulnerabilities that don't exist. Version information contained in a header doesn't reflect the presence or absence of a security issue with the accuracy you need.

Behavior Analysis

The most dependable and accurate indicator of a vulnerability is a specific response to a carefully crafted query. Vulnerabilities can be exactly and accurately identified by how the host responds.
In contrast to scanners that only rely on a version to assess a device's vulnerability posture, more advanced VAM solutions will deliver specially crafted queries and read the resulting response of network components and web applications as its primary indicator of whether a specific vulnerability exists or not. This strategy requires a great deal more effort in the programming of vulnerability tests but produces so few false negatives or positives that most of its customers never experience one.

Why is Behaviour Analysis Better?

The version number reported in the header is only a general indicator of potential vulnerability. It is not accurate enough for effective VAM.

Examples of false negatives (missed vulnerabilities):

- The header can be hidden or suppressed
- A firewall could be faking header information
- An update changed the version number in the header, but it failed to install completely
- A version update loaded, but the server never rebooted to complete the installation

Examples of False Positives (No Actual Vulnerability):

- Configuration settings can make the vulnerability unreachable
- The vulnerable service, feature or function may be turned off
- A workaround is in place which resolved the vulnerability
- A patch was applied that didn't update the version number

In all eight of these cases, the host response to a well-designed query would still identify the presence or absence of the vulnerability.

Why Is Accuracy in VAM So Important?

False negatives are a catastrophic failure in VA. All VAM vendors recognize this, and the broadly accepted solution is to declare every possible issue a vulnerability and let the network administrator try to prove otherwise. Unfortunately, false negatives and racing to claim "we ship the most tests" and "report the most vulnerabilities" has made false positives endemic to ineffective VAM solutions.

A 5% false positive rate may not be a problem for small networks - depending upon what your time is worth. If there are 15 false positives in a network of 300 IPs, that may not seem like a big deal. What if you have 1000 IPs with 150 high-risk false positives? It could take weeks to sort out.

Example of a Banner vs. Behavior Based Vulnerability Test:

The SOAP interface to the eMBox module in Novell eDirectory 8.7.3.9 and earlier, and 8.8.x before 8.8.2, relies on poorly executed client-side authentication. Poor design in this solution allows remote attackers to bypass authentication via requests for /SOAP URIs, and this can cause a denial of service (daemon shutdown) opportunity or allow arbitrary reading of files.

A Version-Dependent Test That Depends on Headers:

A beahviour-based test would look like this.

1. **Confirm it's an HttpStk server by sending it a request that triggers a pre-defined error page (basically an invalid HTTP request)**

2. **Then HTTP posts this to the server:**

```
<?xml version="1.0"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xml-soap.org/soap/envelope/"> <SOAP-ENV:Header/>
<SOAP-ENV:Body>
<dispatch>
<Action>novell.embox.connmgr.serverinfo</Action>
<Object/>
<Parameters/>
</dispatch>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

3. **If it returns:**
   novell.embox.connmgr.serverinf
   We know we're communicating with the right type of server.

4. **Send a follow-up request with:**

```
<?xml version="1.0"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xml-soap.org/soap/envelope/"> <SOAP-ENV:Header/>
<SOAP-ENV:Body>
<dispatch>
<Action>novell.embox.service.getServiceList</Action>
<Object/>
<Parameters>
<params xmlns:EMR="emtoolsmgr.dtd">
<EMR:NamesOnly>0</EMR:NamesOnly>
</params>
</Parameters>
</dispatch>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

5. **5) If it returns:**
   </EBX:XError>
   We know it's secure.

Any other response indicates the host is vulnerable regardless of what version number the header provides. The test itself makes no change to the host and doesn't interfere with any other traffic.

Ensure Accurate VAM Testing

Testing the behavior of hosts and applications is harder to program than just asking for the version number, but ensuring advanced behavioral tests are in place will deliver much more conclusive and actionable reports and a dramatic reduction in the time it takes to clean up network vulnerabilities.

Best Practice 4
Scan Frequently to Close the Door on Network Attacks

Your network is far, far more likely to be attacked with a known exploit than an unknown one. And the reason behind this is simple: There are so many known exploits with easily available, cheap and automated tools and one or more of these known vulnerabilities are probably present in your network. Because the introduction of vulnerabilities can occur on the network at any time, it is important to scan the network on a regular basis to ensure vulnerabilities are discovered and fixed promptly.

The number of networks with known vulnerabilities worldwide is so great and the number of new, yet undocumented and thus unknown exploits so small that your chances of being attacked with one are nearly zero - unless you have high- value network targets, or you are a particularly interesting target for deep pocket attackers. If you haven't attracted the attention of dedicated, well-financed attackers, then your primary concern must be to eliminate your known vulnerabilities so that a quick look by a bored passerby would not reveal an easy entry.

Network Security Defense Strategy

There are two roads to accomplishing excellent security. On one path you would assign all the resources needed to maintain constant alert to new security issues. You would ensure that all patches and updates are done at once, have all your existing applications reviewed for correct configuration, ensure that only proven security knowledgeable programmers do work on your applications and then have their work checked carefully by security professionals. You would also maintain a fiendishly restrictive firewall, antivirus and IPS/IDS.

Your other option: use a security scanning solution, test your existing equipment, applications, and website frequently to find the KNOWN vulnerabilities that exist on them and then fix them. While firewalls, antivirus, and IPS/IDS are all important, it is simple logic to fix the very issues that hackers are looking for rather than try to camouflage them. It is more effective to repair your relatively few actual risks than it is to build higher and higher walls around them.

Network VAM can be your most efficient security investment. Current guidance from most all information security practitioners is that scanning should occur as close to "continuous" as possible. Because vulnerabilities are so easily introduced – weekly, monthly and quarterly scans are no longer sufficient. At least once a day scanning should be considered.

If you must choose one or the other, diligent wall building or VAM, fixing your vulnerabilities instead of building higher walls around them will produce a better security posture on a dollar for dollar basis. The efficacy of higher walls is proven by the number of corporate and government networks with very high and thick walls that get hacked every month and then report that known and unaddressed vulnerabilities were key stepping stones used by attackers.

Best Practice 5
Priority in Patching

Are You Patching More but Feeling Less Secure?

Attacks on corporate networks result in hundreds of millions of records stolen every year. These networks have smart people administering them. A great deal of money is spent to ensure that patching programs are in place. However, each of them fall victim to one or several KNOWN vulnerabilities, meaning that the weaknesses hackers use are well-described and discussed in the public domain and that patches or workarounds existed.

The obvious lesson is that automated patching solutions are not keeping up. Apparently, neither were the enterprise- grade firewalls, antivirus programs, and IPS/IDS programs these major corporations had in place.

Patching Strengths and Weaknesses

Patching is vital. However, it has its costs, and as the number of vendors issuing patches, and the frequency of patch publication increases, it reaches a point where there just isn't enough money in budgets to keep up.

Microsoft alone releases over 300 patches a year. Altogether a network could need several times that many. Installing every patch issued by each manufacturer in every instance is common, but results in downtime and each patch runs a risk of breaking existing functionality. Additionally, many serious network vulnerabilities are not issues requiring a patch but are configuration issues.
Out of the 300 patches issued by Microsoft, a typical organization might need just half. Installing every patch from every vendor is an administrative headache.

Also keep in mind that most networks have accumulated applications and code that are no longer in constant use but are kept around, just in case. If not actively patched, these offer an easy avenue for entry to your system.

With complete and accurate VAM, it is possible to identify and prioritize the patches that are needed. Don't patch vulnerabilities that are not currently accessible due to configuration settings, or functions that are turned off.

"Closing the Door" - Dealing With Known Vulnerabilitiess

Almost all attacks are accomplished using known vulnerabilities. Even Stuxnet utilized a blend of known and 0-day vulnerabilities. If networks had no KNOWN vulnerabilities the risks from Stuxnet would have been minimized. So, making sure that every server, every workstation, and every device is free of known vulnerabilities is vital.

Unfortunately, reducing vulnerabilities to zero is typically not feasible. Many organizations need to deal with thousands of network assets, and even small networks often have hundreds. You might have every Microsoft patch in place, but there are dozens of products from other vendors, few of whom make patching easy. Moreover, most networks have accumulated applications and code that are no longer in regular use but are kept around, just in case. If these are not actively discovered and tested, then these offer an easy avenue for entry to your system.

A VAM solution must automate this process by identifying all the "known" vulnerabilities in your network and prioritizing them based on the importance of the asset and the criticality level of the vulnerability. With VAM you can gain certainty that your potentially small team is addressing the most critical vulnerabilities.

Is Security Pressured to Ignore Network Vulnerabilities?

Technical, organizational, financial and cultural forces in network security have combined to push the repair of known vulnerabilities, the single most important factor regarding network security, into the background.

Technical: Equipment and application vendors are under heavy pressure to release new products and versions quickly - but have less pressure during development to test their security. Thus, every developer/manufacturer generates a stream of updates to patch security issues after release. Even a modest network has hundreds of applications and appliances and has (or should have) thousands of patches in place. The challenge: Each patch has the potential for creating issues when installed and should be tested before being rolled out. The result is that unaddressed patches exist and the network ends up with unpatched, known vulnerabilities.

Financial: Security is difficult to fund without convincing proof of return on the investment. Installing every possible patch into every single host is budgetarily out of the question. The vulnerabilities left unpatched are hard to quantify as being a danger and staff is simply not available to track down every missing patch.

Organizational: Company executives want to see some evidence that the current security staff is doing something. So, you often get security theater. The perimeter solutions are great at reporting blocked attack volume, and the graphs they produce are great evidence that security is on the job and working hard. On the other hand, any security professional worth their salt might inquire 'Well, why did those issues exist in the first place?'.

Cultural: From the very earliest days of networking security has centered on a perimeter defense strategy. The arrival of smartphones, tablets, and cloud-based servers call into question whether a network "perimeter" even exists today. But there remains a powerful contingency in network security that still claims that they can keep all the bad guys away from the known but unrepaired vulnerabilities on your network via a strong "perimeter." Contemporary security wisdom thinks differently.

Because of these factors, security through the elimination of network vulnerabilities has become more of a compliance checkbox than a front-line defense strategy.

The truth is that the defense perimeter today is around each host, itself, therefore determining and prioritizing fixes to vulnerabilities at the host level can greatly reduce the risk of a data breach.

Best Practice 6

The Best VAM Deployment Model for Your Organization

A difficult reality for most every network and security professional is that network architectures are complex. A corporate network today will typically include user access to public, semi-private, and private networks. A company may leverage software or platform as a service (SAAS or PAAS or IAAS) architectures. A company may leverage VPN technology to allow users to connect to corporate or partner IT resources. Also, companies may have sophisticated access control systems. When implementing a VAM solution, it is important to choose a solution that has flexible deployment options to ensure proper scanning coverage across complicated, growing, or distributed networks.

Many organizations will attempt to use free, open source, vulnerability scanners, and security tools. Free scanners are great - up to a point. That point is when your network reaches a critical size, your assets have acquired a critical value, or your company, industry or Uncle Sam has set new compliance requirements. Unfortunately, many free tools are not conducive to effective VAM across a complex network – so organizations will attempt to cobble together multiple disparate solutions that are not optimal.

Running Multiple Tools is a Pain

If your network is small and you have time to configure and run multiple tools and then compare and resolve their potentially contradictory results, then great. If your organization has a larger, somewhat complicated, network and needs mission-critical reporting that is accurate and easy to produce? It's probably time to step up to an enterprise- grade VAM.

Ensure Flexible VAM Deployment Options

Networks come in many shapes and sizes. Your VAM solution should easily adapt to whatever network architectures your organization uses. If your network is hierarchical – your VAM should support a flexible, hierarchical scanning architecture. Also, the VAM solution should include modular, hierarchical and easily integrated scanning components. For example, scanners distributed packaged as a virtual machine can be invaluable when outfitting multiple smaller distributed networks. Similarly, plug and play hardware appliances can be invaluable when outfitting a large network backbone or DMZ.

Best Practice 7
Maximizing the Value of Your Network Security Tools

As discussed previously, an organization that is serious about information security will implement a comprehensive set of security controls that will be a combination of people, process, and technology. These investments will sometimes work independently; however real power can emerge when complementary systems can leverage the viewpoint of other relevant systems. For this reason, it is important that the VAM solution provides well-defined integration points for connecting other information security investments for maximum benefit.

Enabling SIEM to Leverage VAM data

SIEM systems have been shown to provide high value to a security program when the most relevant network and security data, including data from VAM solutions, is analyzed. SIEM systems have become good at comparing and contrasting signals from multiple viewpoints on the network to further prioritize potential risk to the network. For example, centralized analysis by a SIEM using both network activity from firewall or IDS logs and reported vulnerabilities from a VAM can be extremely valuable to assess not only that a system is vulnerable, but that actual network traffic exists on the network that might be underway to compromise the vulnerability.

When properly integrated and tuned the combination of VAM and SIEM has been shown time and time again to provide significant benefit to an information security program. In fact, an integration of VAM and SIEM is now recommended as part of the CIS information security control 4: "Continuous Vulnerability Assessment and Remediation." When implementing a VAM, it is important to ensure sufficient integration points with your SIEM.

Enabling Ticketing Systems to Manage VAM Incidents

Most all organizations with an information security program will implement some form of ticketing system to properly manage a broad range security concerns, including the remediation of vulnerabilities on the network. Key to integration between a VAM and ticketing system is the availability of APIs that allow sharing of vulnerability data with the ticketing system. When implementing a VAM, it is important to ensure sufficient integration points with your ticketing system.

VAM Past and Future
Conclusion

VAM: The Low Man on the Network Security Totem Pole

VAM was the new kid on the network security block 20 years ago. It was a short and unhappy childhood. Early tools were complicated, cumbersome and ill-suited for rolling into corporate networks. Admins that did install the early tools ran into huge reports filled with inaccurate results.

Accuracy has been the missing ingredient in many network security tools. Ask any admin who has tested several competitive VAM solutions side by side on a network. The variation in what each tool discovers and reports is enough to keep one up at night. This phenomenon applies to all security tools but particularly to VAM. Inaccuracy in a firewall, antivirus or IPS is nearly invisible. How do you know what risky traffic is traversing the network? On the other hand, an inaccurate VAM report is obvious, sending network staff searching high and low for things that don't exist. A VAM report that has a couple of errors on the first page is going to get tossed in the bottom drawer.

Most VAM systems sold today are now at 95% accuracy, which is a lot better than the early days. That still means one false positive for every 20 reported issues. And that is still enough to get the monthly VAM report relegated to the shred pile.

Breathing New Life Into VAM

VAM has grown up. Government and industrial security standards are requiring VAM as a component of constant network monitoring. VAM is now simple to install, easy to operate and should incorporate web application scanning and database scanning along with the traditional network scanning duties. Can your VAM solution assess asset value and vulnerability severity and so gives admins an accurate idea of remediation MUST have, NICE-TO have, and what might be done in the future to secure the network. And is it all done with accuracy and reliability.

VAM as Your Next Step?

We hope you will incorporate VAM into your network security strategy. If you are already using a VAM solution please seriously consider extending it to cover your entire network, including endpoints, test servers, phones, printers, etc. If you haven't invested in an effective VAM solution, now is the time. If you aren't happy with your current VAM solution now is a good time to start looking.

This eBook is provided by Beyond Security, a trusted provider of effective Vulnerability Assessment and Management solutions.
Our flagship VAM solution, beSECURE helps organizations:

1. Implement an Effective Vulnerability Assessment and Management Plan	Meet specific vulnerability assessment (VA) regulatory mandates, including PCI, HIPAA, SOX, NERC-SIP, among others Enables high impact vulnerability assessment and management program
2. Scan Broadly for Vulnerabilities	Automated, and easy to use security testing tools across entire network infrastructure Extensive vulnerability research and device scanning support
3. Obtain Accurate Vulnerability Assessment and Management	How to scan accurately, including minimizing false positives and to obtain actionable information
4. Scanning for Vulnerabilities frequently	Flexible scan scheduling options Timely vulnerability detection and reporting
5. Remediate Based on Prioritized Vulnerability Risk	Supports on-premise and SAAS vulnerability managementcAppliance or Virtual Machine scanning support
6. Deploy VAM Across Broad Range of Network Scenarios	How to best align vulnerability scanning on a distributed and sometimes complex network
7. Integrate With Existing Security Investments for Maximum Value	APIs for integration with existing and future IT investments Integrates with SIEM, ticketing systems,and other complementary security solutions

About Beyond Security

Leading Provider of Automated VAM Solutions

Beyond Security is a market leader in automated vulnerability assessment and compliance solutions - enabling enterprises across the globe to accurately assess and manage security weaknesses in their networks, applications, industrial systems and networked software at a fraction of the cost of human-based penetration testing.

Next Steps

Contact Primenet to discover how you can rest assured with a complete VAM Solution
marketing@primenetuk.com

beyondsecurity
by HelpSystems

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.

(bs-gd-ptr-pn-1021-r2-as)