2017

7 Best Practices for Vulnerability Assessments and Management

www.beyondsecurity.com

Table of Contents

Introduction

Many security tools are sold under the premise that they can be purchased, installed and then left to do their job with occasional review. Endpoint protection, firewalls, and IPS/IDS come to mind. They are sold with the promise that by putting them into play, your security is improved simply because they are providing a 24/7 barrier between attackers and the vulnerabilities the bad guys are looking for.

Vulnerability Assessment - not like that. A properly set up VA system is going to find and point out vulnerabilities and step back, its job done. Somebody must take action to fix the issues it found. This takes budget and man-hours. Short staffing in security departments and budgets that focus on purchase of tools, but not allowing additional head-count leads to over-dependence on adding more layers of theoretically hands-free defense applications, but precious little funding to fix the network vulnerabilities that make all those layers necessary.

Adding to that, VA implementation is more susceptible to being poorly done than any other security solution. It is common for Vulnerability Assessment and Management (VAM) to be applied to a small portion of the network instead of all of it, then to be rrun infrequently with insufficient man-hours dedicated to completing the necessary repairs. Scanning just 10% of a network's hosts is like installing Antivirus on 100 endpoints out of 1000, or setting up just few of the rules needed on a firewall. The VAM compliance checkbox often gets checked when the irreducible minimum of IPs get tested as infrequently as possible and then produce a report that gathers dust.

Get more out of your existing VAM. Use it 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 them. Your network has known vulnerabilities. No security tool will guarantee they will not be used against you. Find and fix them, however, and you are guaranteed that they *can't* be used.

Does that appear impossible or unlikely? Find a better VAM solution. Don't accept inaccurate or poorly organized reports. Find a tool that takes fewer man-hours to operate and put those hours into repairing the vulnerabilities discovered.

VAM is a data loss prediction tool. It will find the weaknesses that hackers will eventually use to gain access to your network. Use it to fix your vulnerabilities before they find them, or use it as a post mortem to identify what they used to take your valuables.

Best Practices

Getting right to the point:

1. Budget VAM correctly:
   1/3 of budget to purchase and manage the tool, 2/3 on the manpower to act on the reports.
2. Scan broadly:
   a. Scan everything.
   b. Prioritize – A high-risk vulnerability on a perimeter host is more important than a medium risk on a central host.
3. Scan accurately:
   Don't accept solutions that flag problems that don't exist.
4. Scan often:
   Scan weekly, (or even daily) instead of quarterly.
5. Compare change over time:
   Know that your network is gaining or losing.
6. Scan high value resources in authenticated mode (credentialed)
   Test configuration settings on key hosts
7. And last but best:
   Fix the high-risk vulnerabilities on your network.

Why is Vulnerability Management Necessary?

No single security solution can solve the security puzzle. Endpoint protection can't guarantee that workstations will be forever free of viruses and malware. Firewalls and IPS can't guarantee protection of data on a database server. Access control can't guarantee that a password won't be stolen. Etc., etc. So, it's a matter of balancing multiple solutions.

Peripheral Solutions

These focus on the attack itself, network traffic and preventing unauthorized access to network assets and their known vulnerabilities.

- Firewall - performing access control at the network border. Challenged by hosts that move in and out of the network
- Endpoint protection - Exponential increase in signatures is pushing AV toward the limit.
- Intrusion Detection and Prevention Systems - IPS and IDS at its most secure settings produces some degree of access limitation for authorized users.
- Access control…
- Etc.

Internal Solutions

Attackers are looking for network weaknesses, and these solutions focus on finding the weaknesses first and fixing them.

- Vulnerability Assessment - Network scanners, port scanners, IP scanners and network mappers can all assist in the detection of network assets and weaknesses.
- Vulnerability Assessment and Management (VAM) - Solutions that assess the network, then prioritize the repairs needed and in some cases provide the tools to do the repairs.

VAM, an Essential Piece of the Security Puzzle

Attacks resulting in data loss are usually performed by exploiting known and well-documented security vulnerabilities in software, network infrastructure, servers, workstations, phone systems, printers and 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 that is missing patches or that didn't get them installed correctly can compromise the security of the entire network.

As not all vulnerabilities are created equal and not all assets are of equal importance or are equally available to a hacker's access, there is a compromise. 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.

How Does VAM Complement Other Security Solutions?

Every known peripheral security solution can be bypassed under the right circumstances, but with proper VAM in place, the attacker who gains access to an endpoint will not find internal weaknesses to step deeper into the network. Here are some examples:

Firewall - Attackers will always try to use (steal) a legitimate network access, and will bypass the firewall by hacking an endpoint or stealing credentials. VAM finds and helps repair the vulnerabilities that attackers are searching for. If you have no serious vulnerabilities on important assets and have kept endpoints clean as well, then your chances of data loss and dependence on perfect firewall assessment is reduced.

Intrusion Detection and Prevention Systems - The ideal IPS installation, with careful maintenance and using the strictest rules possible, will stop nearly all malicious packets. Given that the average network gets thousands a day, that means that few get through under even these ideal circumstances. However, strict settings also capture many valid packets and this gets pushback from users. The nearly universal solution is to dial back on the rules to ensure valid packets pass and accept that IPS will stop fewer attacks. In real-world IPS installations, internal network assets will get many attack attempts a day and ensuring that they are free of vulnerabilities though VAM is vital.

Antivirus - Antivirus studies incoming traffic, and is not primarily focused on the system itself to see if there is a weakness that malicious code can exploit. VAM is so focused and will find the vulnerabilities there and help you eliminate them. As such, VAM complements anti-virus software in protecting the system.

It is important to understand that all the perimeter security solutions can be bypassed under relatively common circumstances. Those circumstances include incomplete or improper installation or settings.

Only by hardening each individual network asset using VAM can network security be improved with confidence.

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 errors. Overlooking a vulnerability (a false negative) leaves a security flaw you don't know about. Reporting a vulnerability as present when in fact none exists (false positive) sends you looking for something that can't be found. Obviously you don't want either. An inaccurate VAM will give you both and is more trouble than it's worth.

If the first 4 vulnerabilities reported by your solution didn't actually 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. Also, 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 man-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 the time to verify and eliminate false positives is included. Even a 2% error rate can be a headache.

Version Analysis

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 5 vulnerabilities and the header says that the old version is in use, then it is assumed that all 5 of those vulnerabilities exist.

Version checking has many advantages for the vendor and one key disadvantage for the customer. It is easy to program them and claim '45,000 tests'. Also, a version analysis scan that finds an old version can produce a long and impressive list of vulnerabilities. This makes the solution look good.

The disadvantage: Poor accuracy misses real problems and lists dozens if not hundreds of vulnerabilities that don't actually 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.

Beyond Security's AVDS, for example, delivers specially crafted queries and reads 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 Behavior Analysis Better?

The version number reported in the header is only a general indicator of potential vulnerability. It is not accurate enough for 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 was used 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 clearly a catastrophic failure in VA. All 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. This and the race to claim having the most tests and report the most vulnerabilities has made the false positive endemic to VAM.

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 may 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. This 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 files to be read.

A version-dependent test that depends on headers:

1) Check the version of eMBox. Is it 8.7.3.9 or earlier or 8.8.1 or earlier?
2) If yes, then report it as a high-risk vulnerability.

A behavior 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 POST this to the server:

```
<?xml version="1.0"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.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 talking to the right type of server.

4) Send a follow-up request with:

```
<?xml version="1.0"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.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) 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.

Accurate VAM Testing

Testing the behavior of hosts and applications is harder to program than just asking for the version number, but doing tests like that produces accurate testing, conclusive and actionable reports and a dramatic reduction in the time it takes to clean up network vulnerabilities.

Network Security Scanning - Closing 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 tool sets and one or more of these known vulnerabilities are probably present in your network.

The number of networks with known vulnerabilities worldwide is so great and the number of new, as of yet undocumented and thus unknown exploits so small that your chances of being attacked with one is nearly zero - unless you have network assets of truly great value, or you are a particularly interesting target to deep pocket attackers.

If you haven't attracted the attention of a dedicated, well-financed attack, 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 accomplish excellent security. On one path you would assign all of 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 of 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 to test your existing equipment, applications and web site to find the KNOWN vulnerabilities that actually exist on them and then fix them. While firewalls, antivirus and IPS/IDS are all important, it is simple logic to also 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 is your most efficient security investment.

If you have to 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 status on a dollar-for-dollar basis. This is proven by the number of corporate and government networks with very high and thick walls indeed, which get hacked every month and then report that known and unaddressed vulnerabilities were key stepping stones used by attackers.

Network Security Using a Security Scanner

Beyond Security has been accumulating a library of known issues for many years and has compiled what is arguably the world's most complete database of behavior-based tests in existence.

In a matter of hours, a security scanner can run through its entire database of tens of thousands of tests and can report on which vulnerabilities are present and better yet, confirm the thousands that are not. With that data in hand, you and your staff can address your actual security vulnerabilities and after retesting, confirm that your network is completely free of known issues.

Security scanning should then be run on a regular basis so that your network will be tested against new vulnerabilities as they become known and provide you with solid data as to whether action is high or low priority. You will also be alerted if new equipment has been added, a new port has been opened that was unexpected, or a new service has been loaded and started that may present an opportunity to break in.

In complex, large systems, weekly (or daily) scanning is the only way to ensure that none of the many changes made to network equipment or applications may have created a weakness that a determined hacker could exploit.

Why Patching Everything Fails

Are You Patching More But Feeling Less Secure?

Attacks on corporate networks result in hundreds of millions of records stolen every year. These networks had smart people administering them. A great deal of money was spent to ensure that patching programs were in place. Yet each of them fell victim to one or several KNOWN vulnerabilities, meaning that the weaknesses hackers used were well described and discussed in the public domain and that patches or work-arounds 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, a point has been reached 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 on 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 configuration issues.

Out of the 300 patches issued by just 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 these are not actively patched, then these offer an easy avenue for entry to your system.

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

Scanning for Complicated, Growing or Distributed Networks

VAM Getting to be a Chore?

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. AVDS is a step up into the corporate VAM arena, but with the simplicity you are used to with your favorite freeware scanner.

Running Multiple Tools is a Pain

You may have a half dozen network scanners sitting around. If your network is small and you have time to configure and run multiple tools and then compare their often contradictory results, great. Got a somewhat complicated network and need mission critical reporting that is accurate and easy to produce? Time to step up to an enterprise grade VAM.

When a Network Scanner is Just Not Enough

On top of having many things you would like to be doing, compliance requirements are coming to your network soon (if you aren't already coping with them). You need a single, solid, common-sense solution to find and handle the nasty vulnerabilities when they happen. Got credit card data? Medical records? Financial records, or are you a publicly held company? Get a VAM system that includes all compliance reporting at no extra cost.

Vulnerability Assessment

Why VAM Got a Bad Rap

The number of desktops, laptops, phones and personal devices accessing network data is constantly growing. The number of applications grows exponentially. And over the years, as known vulnerabilities grew in number, IT managers found that traditional VAM solutions could easily find more problems than could be fixed.

One solution has been to concentrate on building better walls around the network to keep attackers from accessing these known weaknesses. Vulnerabilities have been ignored, or addressed only when and if there are resources available.

Another solution: scan just the most important network resources, so that limited resources could be applied to fixing just those hosts that were most likely to carry vital data.

Neither of these solutions are working very well. Unsophisticated attackers are routinely bypassing antivirus, firewall and IPS to find and exploit vulnerabilities on systems deemed unimportant, or vulnerabilities that were left unrepaired because they weren't high risk.

Most successful attacks are accomplished using well-known, easily discovered and easily exploited vulnerabilities. Most attackers get good at attacking one or two specific vulnerabilities and they then search broadly for networks that have that weakness. From that beachhead they expand their control through the network.

Vulnerability Assessment's Black Eye

The VAM industry fell from grace in the 2000's because its solutions failed on two fronts. Their reports were riddled with errors and its vendors got into a race of which report could list the most vulnerabilities. VM reports became so long and inaccurate as to be un-usable.

If resources are unlimited then every vulnerability found by a traditional VAM system could be validated by additional tools and then fixed. But few have that much time and patience. And so the decade of building better walls by adding more layers, more solutions was launched.

And now we are faced with running multiple, overlapping and complex systems that still can't keep the attackers out.

We propose that it is time to revisit VM, but this time focus on accuracy and usability.

"Closing the Door" - Dealing With Known Vulnerabilities

Almost all attacks are accomplished using known vulnerabilities. Even Stuxnet utilized a blend of known and 0-day vulnerabilities and would have been severely limited in its scope had there been no KNOWN vulnerabilities in the networks it attacked. So, making sure that every server, every workstation and every device is free of known vulnerabilities is vital.

Unfortunately this is not so simple. 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 limited resources are being applied to the most serious network issues.

Network Security

Network Security and Vulnerability Assessment and Management

Antivirus, access control, firewall and Intrusion Prevention Systems are failing to keep attackers from reaching vulnerable systems. Network administrators may have budget to add yet more security layers, but little budget to actually fix the vulnerabilities. This is a problem because successful attacks are often done with layer upon layer of security solution in place. Something about these common perimeter guards isn't getting the job done.

How Hackers Bypass Network Security

In 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, all the successful attacks we hear about were done on networks whose admins (or entire security teams) were doing their best to maintain a tight perimeter! This includes the highly publicized break-ins at Fortune 500 companies 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, they don't stop enough.

Some political or financial high value targets get attacked with persistence – with planning and investment of time. 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.

Therefore, to better secure any network, these well-known vulnerabilities must be found and fixed regardless of ANY set of perimeter defense solutions being in place. VAM is the solution that achieves this goal.

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 not all patches are installed and every network ends up with unpatched, known vulnerabilities.

Financial: Security is difficult to fund with any convincing proof of a 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 get security theater. The perimeter solutions are great at reporting how many attacks were blocked and the graphs they produce are great evidence that security is on the job and working hard. On the other hand, reports to execs about finding and fixing serious vulnerabilities can be met with a 'Well, why did those issues exist in the first place?'.

Cultural: From the very earliest days of networking, security has been fixed on a perimeter defense strategy. The arrival of smartphones, iPads and cloud based servers finally marked 'paid' to the idea that a perimeter can be held, or that it even exists. 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. If that were only true.

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.

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 competing 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 applies to all security tools but particularly to VAM.

Inaccuracy in a firewall, antivirus or IPS is nearly invisible. How do you know what is getting through? On the other hand, an inaccurate VAM report is really obvious, sending network staff searching high and low for things that don't exist. A VAM report that has a couple of errors in 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. It assigns asset value and vulnerability severity and so gives admins an accurate idea of what MUST be done, what should be done and what might be done in the future to secure the network. And it is 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 don't have VAM installed on your network, now is the time. If you aren't happy with your current system, now is a good time to start looking.

About Beyond Security

Beyond Security is a leading worldwide security solutions provider. It's testing tools accurately assess and manage security weaknesses in networks, applications, industrial systems and networked software. Beyond Security's product lines include, AVDS for network vulnerability management and beSTORM for software security testing, which can help secure network and applications and comply with the security policy requirements that exceeds industry and government standards.

Founded in 1999, Beyond Security's solutions are essential components in the risk management program for many organizations worldwide. With the headquarters located in Cupertino, California, Beyond Security's distributors and resellers can be found in North and South America, Europe, Asia, Africa, the Middle East and Australia.

For more information, please contact – Sonia Awan at 747-254-5705 or at soniaa@beyondsecurity.com

Or visit us at www.beyondsecurity.com and https://blogs.securiteam.com/