Information Security (INFOSEC) Best Practices for Data Protection and Compliance

by Gary S. Miliefsky, CEO, SnoopWall, Inc.

SnoopWall

The State of Network Security Today – Reactive and Slow

Network breaches are in the news every day. In the US alone, there have been over 900,000,000 – that's 900M records of personally identifiable information (PII) stolen over the past few years. While most organizations are running the latest corporate firewalls – also known as UTMs – unified threat management systems or NGs – next generation firewalls and the latest and greatest antivirus products, they are still breached. Over 95% of breaches happen behind these corporate firewalls on these endpoints that appear allegedly to be secured by antivirus. So, it seems, the hackers have leap-frogged most INFOSEC countermeasures. Yes, that's what the tools you've been buying to protect yourself are – just reactive technologies, countermeasures, that usually react too late – causing a ransomware payment decision, data theft, downtime or even much worse.

The Way to Win the Battle – Proactive, Offensive, Fast and Semi-Automated

While not all of your defenses can be automated, I do like to focus on more proactive approaches to the problem of being breached. If you do a root-cause analysis, you will discover your weaknesses in advance of their exploitation. For example, let's say you buy the latest and greatest antivirus software, keep it always up to date and then get infected. The infection exploits a fairly new but known vulnerability in the Microsoft Windows RPC protocol, which can be found in the nvd.nist.gov database on common vulnerabilities and exposures (CVEs). While your antivirus software focuses on reacting – scrubbing and cleaning up after you've been infected, it's still reactive technology. The Offensive security model suggests you should find out which systems have the RPC vulnerability, contact Microsoft for a patch and fix this hole quickly. If there is no patch available, maybe you could turn off the RPC protocol for a few days or a week until next week's Patch Tuesday from Microsoft. This may cause a minor disruption in network service access or Remote Help Desk software, however, your Windows computers won't be getting infected with this new virus. So, simply put, finding the leak and patching it or hardening the system is a lot better than bailing out water from a sinking ship because you never noticed it had this hole allowing the ship to fill with water.

Let's explore the 7 secrets of Offensive Security and learn a new, more proactive approach to dealing with protection of PII, keeping networks running and employees productive. We'll dig into ideas and methods that, while they sound so simple and easy, sometimes to implement them, you'll be dealing with corporate politics, budget issues, resource issues and time constraints.

I'll go into a deep dive for you on each of these seven secrets, however, let's get started right away, here are my seven secrets:

1. Demand Executive Support – Funding, Training, Etc.
2. Deploy Continuous (Or Daily At Minimum) Backups And Test Them – Does The Restore Even Work?
3. Deploy Corporate Wide Encryption
4. Create A "living" Corporate Security Document
5. Train (And Retrain) All Employees On Best Practices Infosec Policies (ISO27001, COBIT, NIST– Choose One You Like)
6. Manage The Bring Your Own Devices (BYOD) Dilemma By Assuming All Mobile Devices Already Infected
7. Deploy And Manage A Breach Prevention Solution (We'll Quickly Show You Ours) That Helps…

   a) Document and mitigate RISK, especially serious vulnerabilities (CVEs)
   b) Provide Network Access Control (NAC)
   c) Quarantine high-risk, rogue and infected devices

What is the real cost of a Breach?

Recently, the Ponemon Institute concluded it's 2016 Data Breach report. According to this report (excerpted under fair use of the US Copyright Act, source: http://www.ibm.com/security/data-breach):

The cost of data breach sets new record high. According to this year's benchmark findings, data breaches cost companies an average of $221 per compromised record – of which $145 pertains to indirect costs, which include abnormal turnover or churn of customers and $76 represents the direct costs incurred to resolve the data breach, such as investments in technologies or legal fees.

The total average organizational cost of data breach reaches a new high. In the past 11 years, the most costly organizational breach occurred in 2011, when companies spent an average $7.24 million. In 2013, companies experienced a net decrease in total data breach cost to $5.40 million. This year, the total average cost is $7.01 million.

Measures reveal why the cost of data breach increased. The average total cost of a data breach grew by 7 percent and the average per capita cost rose by 2 percent. Abnormal churn of existing customers increased by 3 percent. In the context of this paper, abnormal churn is defined as a greater than expected loss of customers in the normal course of business. The average size of a data breach (number of records lost or stolen) increased by 5 percent.

Certain industries have higher data breach costs. Heavily regulated industries such as healthcare, life science and financial services, tend to have a per capita data breach cost substantially above the overall mean of $221. In contrast, public sector (government), hospitality and research had a per capita cost well below the overall mean value.

Malicious or criminal attacks continued to be the primary cause of data breach. Fifty percent of incidents involved a malicious or criminal attack, 23 percent of incidents were caused by negligent employees, and 27 percent involved system glitches that included both IT and business process failures.

Malicious attacks were most costly. Companies that had a data breach due to malicious or criminal attacks had a per capita data breach cost of $236, significantly above the mean of $221. In contrast, system glitches or human error as the root cause had per capita costs below the mean ($213 and $197, respectively).

Certain industries were more vulnerable to churn. Financial, health, technology, life science and service organizations experienced a relatively high abnormal churn and public sector, media and research organizations tend to experience a relatively low abnormal churn.
The more records lost, the higher the cost of data breach. This year, companies that had data breaches involving less than 10,000 records, the average cost of data breach was $4.9 million and those companies with the loss or theft of more than 50,000 records had a cost of data breach of $13.1 million.

The more churn, the higher the per capita cost of data breach. Companies that experienced less than 1 percent churn, or loss of existing customers, had an average organizational cost of data breach of $5.4 million and those experiencing churn greater than 4 percent had an average cost of data breach of $12.1 million.

Certain industries were more vulnerable to churn. Financial, health, technology, life science and service organizations experienced a relatively high abnormal churn and public sector, media and research organizations tend to experience a relatively low abnormal churn.

Detection and escalation costs are at a record high. These costs include forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and board of directors. Average detection and escalation costs increased dramatically from $0.61 million to $0.73 million, suggesting that companies are investing more heavily in these activities.

Notification costs increased slightly. Such costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary mail contacts or email bounce-backs and inbound communication set-up. This year's average notification costs increased slightly from $0.56 million in 2015 to $0.59 million in the present year.

Post data breach costs increased. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. These costs increased from $1.64 million in 2015 to $1.72 million in this year's study.

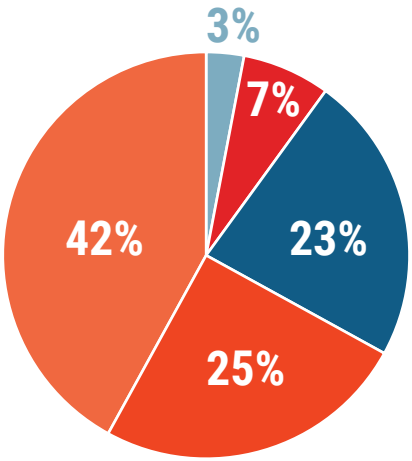
Lost business costs increased. Such costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. The current year's cost of $3.97 million represents an increase from $3.72 million in 2015. The highest level of lost business cost was $4.59 million in 2009.

Companies continue to spend more on indirect costs than direct costs. Indirect costs include the time employees spend on data breach notification efforts or investigations of the incident. Direct costs refer to what companies spend to minimize the consequences of a data breach and to assist victims. These costs include engaging forensic experts to help investigate the data breach, hiring a law firm and offering victims identity protection services. This year the indirect costs were $145 and direct costs were $76.

The bottom line is this: Breaches are EXTREMELY costly and may put your organization out of business and you, out of a job. Isn't it time to take an Offensive approach to cyber security? Aren't you tired of reading about breaches in the news, wondering if your organization will be next?

Are Insider Threats Really That Serious?

According to the Insider Threat Report of 2016, by Crowd Research Partners, Seventy-four percent of organizations feel vulnerable to insider threats - a dramatic seven percentage point increase over last year's survey. Even though only 42 percent of companies feel they have appropriate controls to prevent an insider attack, only three percent of companies feel they are not at all vulnerable to an insider attack.



74%
feel extremely vulnerable to insider threats

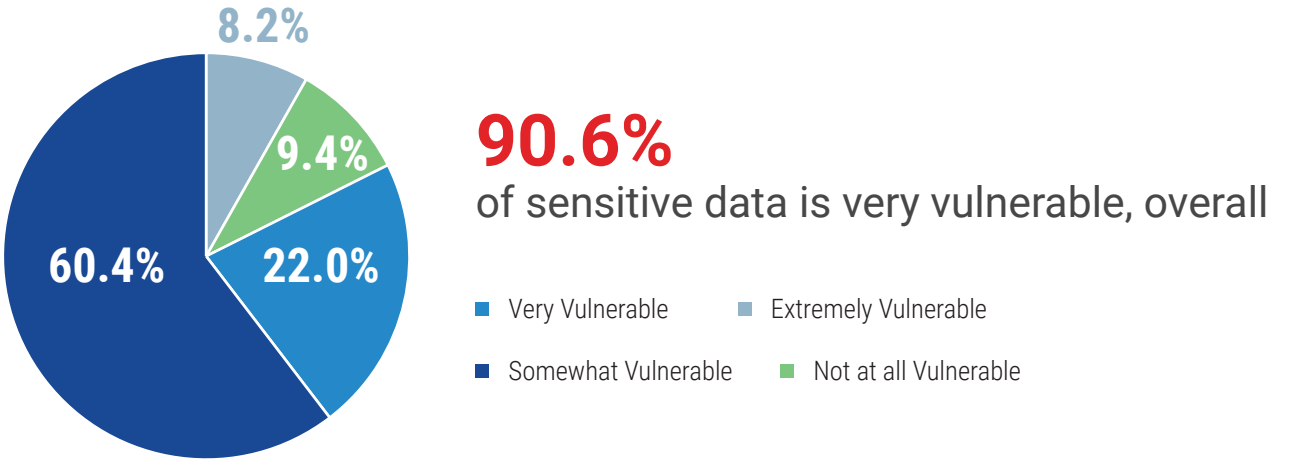
Extremely Vulnerable
Slightly Vulnerable
Very Vulnerable
Moderately Vulnerable
Not at all Vulnerable

What most organizations don't realize is that most employees have no malicious intent – they just aren't properly trained to handle Spear Phishing, Remote Access Trojans and Ransomware, among other cyber threats. In addition, highly vulnerable systems as well as infected (including mobile, through spyware and creepware apps) systems are wide open doors. Most antivirus software misses at least 50% of the latest malware while firewalls have no intelligence to block the cleaning company from plugging in a rogue laptop at midnight, for example.

In addition, the detection of a breach which usually begins BEHIND the firewall is much more difficult to discover than the traditional breach attempt coming from the outside-in. The main reason is that most organizations have not deployed agentless, non-inline Network Access Control (NAC), have not documented their internally exploitable Vulnerabilities known as Common Vulnerabilities and Exposures (CVEs) as defined by http://NVD.nist.gov in the National Vulnerability Database, updated very frequently, and have no way of quarantining, nearly instantly,

infected, soon to be infected or rogue network assets, behind the corporate firewall. Also, the Bring Your Own Device (BYOD) dilemma has left the corporate 'backdoor' wide open to data leakage through mobile devices loaded with creepware, spyware and very powerful data leakage ports – webcam, Bluetooth, nfc, microphone, keyboard, wifi, 3g/4g, gps, etc.

From the Vormetric 2016 Global Data Threat Report, when it comes to the risk of personally identifiable information (PII) or mission critical confidential data being stolen or at risk, the numbers are astoundingly high:



And, the proof is in the pudding – according to PrivacyRights.org we've seen nearly ONE BILLION PII RECORDS stolen in the USA alone (see http://www.privacyrights.org and click on 'chronology of data breaches'). You'll see most of these breaches are starting to happen on Small to Medium Sized Enterprises (SMEs) more than ever before. SMEs have become the #1 target of cyber breaches because they are easier targets than those like a Bank of America who has a $400M per year Cyber Security budget and a huge INFOSEC team protecting their networks 7x24x365 and who can weather a major breach, as they manage over $4 TRILLION US DOLLARS.

The only way to get ahead of a breach is to not let it happen and if it does, to instantly, quickly, automatically isolate it and minimize the impact. So, now that you've seen how costly breaches are and you've also now know my 7 secrets of Offensive Security, let's discuss each one in more detail.

Here they are:

1 Demand Executive Support

This may not be easy, however, you will have to get the Board of Directors, the CEO, CFO, CIO, etc., all top level executives to agree that, fiduciarily, the right thing to do to avoid a breach is to have an annual budget, agree that training of all employees is important, that a corporate security policy is a must have and how the corporation will react if and when a breach actually does happen.

Steps involved:

1) Schedule a meeting with key executives (Board Members, CEO, CFO, CIO, etc.) and explain that you want to share a way to dramatically reduce the risk of the corporation suffering a major outage, fines, penalties, lawsuits, business disruption and possibly going out of business. That will get their attention.

2) Present the typical costs of a Breach and why you think your organization is at risk. Try to cover what you think your organization is missing from my 7 Offensive Security Secrets – funding, training, frequently tested backups, corporate security plan, fuel for the backup diesel generator, corporate wide encryption, etc. Whatever the infosec gaps and related issues that are on your mind should be presented in an organized and thoughtful fashion. If you could sum up the costs in people/time/money that you need vs the cost of a breach, you'll probably find that your requests are 1/10th or less than the cost of a breach.

3) Explain that this is an ongoing process, you'd like to document steps being taken and results on a mutually agreeable frequency and then schedule your first followup meeting with them to present the ongoing risk reducing results.

2 Deploy Continuous Backups and Test Them Regularly

When is the last time you tested a 'restore' of a backup file? When did you most recently backup employee desktops, laptops, servers and other critical infrastructure? While there are numerous and very solid backup products in the market, some even open source (free), there is a smaller list of continuous data protection products that are doing backups in real-time.

Continuous data protection (CDP),also called continuous backup or real-time backup, refers to backup of computer data by automatically saving a copy of every change made to that data, essentially capturing every version of the data that the user saves.

Steps involved:

1) Inventory all network attached assets throughout your entire organization – in particular, the operating systems you are running.

2) Find a CDP product that runs on all the operating systems where you value data – laptops, desktops, servers, etc. If they have a client for smartphones, that would be a plus however, at the time of this writing, it's doubtful. If that's the case, look for an additional backup product or consider Google or Apple's hosted offering such as Google+ and the iCloud.

3) Test your backup solution and make sure it can restore properly on a few key test platforms such as windows and linux. If it meets your needs, deploy it corporate-wide.

3 Deploy Corporate-wide Encryption

Encryption is one of the most powerful ways to protect personally identifiable information (PII). There's encryption for data in transit, encryption for entire hard drives, databases and file systems. If you have employees who travel frequently, if there were a way to encrypt their smartphone, tablet, laptop, netbook and notebook hard drives and file systems that would be the best place to encrypt first – in many cases employee traveling equipment are lost or stolen and without encryption, whatever corporate records, data, passwords, VPN client or other confidential information could end up in the hands of criminals or other preying eyes. There are some excellent encryption technologies on the market – some encrypt chat sessions, instant messaging and SMS as well as telephone or voip communications. These are great for data in transit. There are numerous free and open source tools like Stunnel, OpenSSL, OpenSwan and TrueCrypt (v6 or earlier) that will provide you with a high level of encryption. If there's ever a breach either on portable equipment or behind the corporate firewall, you can mitigate data theft risk, if the data that's accessible to the hackers and cyber criminals is encrypted and they don't have the keys.

Steps involved:

1) Inventory all network attached assets throughout your entire organization – in particular, the operating systems, file systems and databases you are running.

2) Find encryption solutions that will protect these operating systems, file systems and databases. You'll probably end up with multiple solutions from a mix of open sources or different vendors. So, you won't end up with a single dashboard to manage all the encryption but even so, it's worth the effort.

3) Test and deploy the encryption across your organization. The biggest headache will be multi-factor authentication and key management so make sure you picked the most manageable solution with the ability to recover keys or reset passwords without losing access to the data.

4 Create a "Living" Corporate Security Document

A 'living' corporate security policy is your documentation that states in writing how your organization plans to protect the company's physical and information technology (IT) assets. It's a living document because it's never final – you should be continually updating it based on geographic risk, people risk, physical and network resources risk and other forms of risk that might be changing or evolving over time, affecting your organization.

As new threats arrive, such as Ransomware, you'll want a corporate security anti-phishing policy and a policy on how to deal with ransomware, for example. Most corporate security policies include acceptable use, password management, network access control, bring your own device policies, encryption policies and others with descriptions on mitigating risk and how policies are to be enforced. You'll also want to deploy policies that help you prove due care and due diligence in compliance with regulations that affect your organization (FISMA, EU GDPR, GLBA, SOX, HIPAA-HITECH, VISA PCI, etc.).

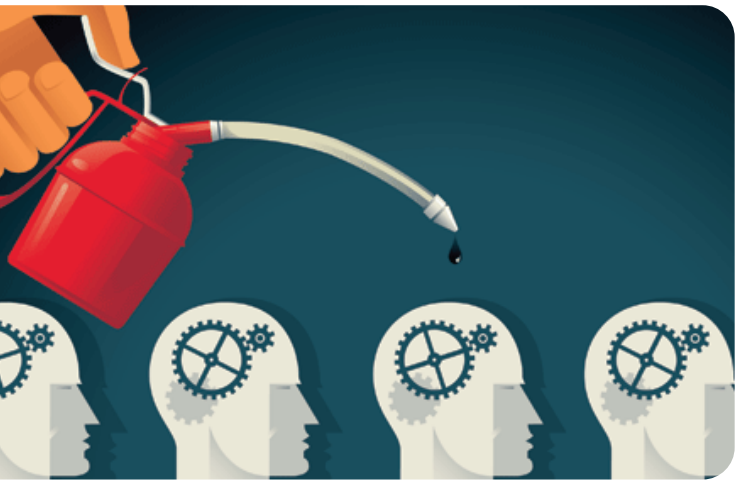
Steps involved:

1) Review various corporate security models and find one you like – most are inexpensive and even freely available such as ISO27001, found here: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm,ISACA's COBIT, found here: http://www.isaca.org/cobit/pages/default.aspx, or the NIST cybersecurity framework, found here: http://www.nist.gov/cyberframework/.

2) Explain to key executives and employees how important this document and their acceptance is for protecting the organization from regulatory compliance pressures, to maintain compliance and reduce the risk of a breach. Have them look at this one story to see what happens when a regulator (over-reaches) gets involved: http://michaeljdaugherty.com it won't be the breach that puts you out of business, it might actually be a government regulator.

3) Roll it out and update it as necessary. Test the controls in each policy section. For example, test password management as well as backup/restore.

5 Train and Retrain All Employees on Best Practices INFOSEC Policies



So, now you have a great 'living' corporate security policy. Do your fellow employees from the "C" levels down to the receptionist understand these policies? Are they helping you implement them or are they becoming difficult and a hindrance to your documented regulatory compliance and best practices? Of all the policies you're implementing, which one's will most likely cause a breach or data theft, if an employee violates the policy?

The most important would be a Bring Your Own Device policy (BYOD) as it's a network asset that you are allowing to cross the bounds, outside of your firewall and then returning, most likely in a different (maybe infected, maybe more insecure) state. Others include ensure devices have the latest patch and application updates, as well as proper configuration and system hardening, to reduce the risk of Common Vulnerabilities and Exposures (CVEs) that get exploited by hackers, cyber criminals and malware. Antivirus software should be up to date but it won't stop the latest exploits – especially Spear Phishing, Remote Access Trojans (RATs) and Ransomware. This requires a better educated employee population who understand that sending and receiving un-encrypted emails is a big risk, emails with attachments and being too trusting to click links and open attachments without verifying the senders' true identities. This leaves them wide open to being socially engineered and victimizing your organization.

Steps involved:

1) Train employees about the risks of BYOD, lack of updated systems, traveling with laptops using weak passwords, no encryption and the biggest risks of being spear phished, then being infected with nearly invisible malware.

2) Schedule these training sessions using statistics, graphics, memes and other tools to make it 'pop' – it should be fun and visual so they will enjoy the learning experience. You could even make it a game. Whatever it takes, get the employees engaged and understanding the value of best practices – stronger passwords, strong encryption, regular backups, safer BYOD, etc.

3) Send out INFOSEC updates. Give out awards. Keep the employees engaged. The more aware they become, the lower the risk of victimization.

6 Manage the Bring Your Own Devices (BYOD) Dilemma

Bring your own device (BYOD) has become pervasive. Most companies are being pressured by their executives for cost reduction and productivity boosting, to allow employees to bring their personally owned devices (laptops, tablets and smartphones) to work. They are asking for privileges to, either behind the firewall over corporate wifi, or over the public internet using 3G/4G or public wifi, to be able to VPN into corporate resources from these traveling devices. There could not be a riskier thing to do, when it comes to corporate security.

The main reason is that the state of these devices is ever changing – applications, emoji keyboards, vpn clients and even productivity sinkhole games like Pokemon Go have taken over the mindset of end-users. Most employees have 30-50 unmanaged apps running on these devices and many are freeware given away in return for access to their personally identifiable information – phone identifiers, contacts list, email information, social media passwords, geolocation and much more – turning these devices into fully loaded creep ware and spyware platforms.

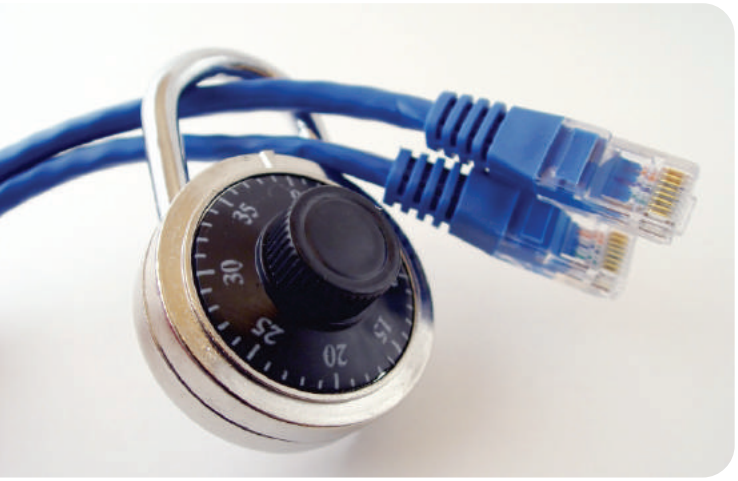
Steps involved:

1) Create a 'living' BYOD policy and make sure everyone who is allowed to leverage their own devices agree to the policy.

2) Train them as to the risks inherent in the free apps they already have on their devices. Explain to them that their Emoji Keyboard is probably a keylogger and it should be deleted if it didn't come with the phone from the operating system vendor – Microsoft, Google, Apple or RIM. The same holds true for all of their other free apps. It's time to do a spring cleaning – remove all the unused apps. Evaluate the rest for their affect on privacy and data leakage risk. What hardware ports do they use? Do they really need to access Keyboard, Microphone, Webcam, Bluetooth, Wifi, NFC, 3G/4G, GPS, etc. Does their privacy policy look onerous? If so, convince the employee to find a safer replacement app.

3) Enforce rules through BYOD agent-based software to prevent Data Leakage. Make sure these rules protect the corporation and are enforced during working hours, through geolocation and/or VPN remote access.

7 Deploy and Manage a Breach Prevention Solution



You have a firewall. Check. You have anti-virus. Check. Ok, so now you are about 5% protected. Now is the time to deploy a breach prevention solution because over 95% of breaches happen behind the corporate firewall on systems running the latest antivirus software. Can you tell if a system has a critical vulnerability that is easily exploitable? Do you know if the Cleaning Company is plugging in a rogue device on your network this evening?

What about an employee who forgot about your spear-phishing policy and just clicked a link leading to an installation of Locky Ransomware that will probe your corporate network to attempt to encrypt not only the employee desktop but all of your fileservers? How do you get one step ahead of these threats? With a breach prevention solution.

Steps involved:

1) Find a breach prevention solution that you can afford and that you like. There are many new ones on the marketplace today. Some are called internal intrusion prevention devices, others are called anti-malware gateways and anti-phishing email systems but these are all point solutions. You'll need to focus on those that help you do the following three things:

a) Document and mitigate RISK, especially serious vulnerabilities (CVEs)
b) Provide Network Access Control (NAC)
c) Quarantine high-risk, rogue and infected devices

2) Selfish-plug: While we at SnoopWall make NetSHIELD as affordable, cost effective and easy to deploy breach prevention solutions, you could also look into Forescout, Fireeye, IBM and/or a mix of point solutions like Qualys, Rapid7, better managed switches, Cisco's 802.1x NAC solution, etc. Ultimately, it's up to you to find the best tools you can work with to help you find and fix your vulnerabilities, manage access to your network and quarantine rogue and/or infected devices.

SnoopWall's Award Winning, Affordable Breach Prevention Solution:

SnoopWall, Inc. proudly manufactures in the USA, the patented NetSHIELD appliances for intranet breach prevention, shipping them worldwide, (see: https://www.youtube.com/watch?v=fDO3dkOV-1M) receiving numerous awards and the award winning WinSHIELD and MobileSHIELD endpoint data leakage prevention technology based upon AppSHIELD SDK, SnoopWall's patented mobile security toolkit that has already been used to protect hundreds of thousands of financial transactions that take place through mobile banking applications. To learn more about these products and services, visit: https://www.snoopwall.com/products-services/

Third-Party Evaluations & Awards

"Full dynamic access control and auditing of network devices."
- Peter Stephenson, SC Magazine

Features	★★★★★
Ease of Use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for Money	★★★★★
Overall Rating	★★★★★

SC MAGAZINE RECOMMENDED

Info Security Products Guide GLOBAL EXCELLENCE AWARDS ★★★★★

NETWORK PRODUCTS GUIDE PRODUCT INNOVATION ★★★★★

SC MAGAZINE Top Product 2020 PRODUCTS YEARS

For: Full dynamic access control and auditing of network devices.

Against: None that we found.

Verdict: A solid suite of hardcore NAC products with a clear focus on keeping unauthorized systems and users off the network.

About SnoopWall

SnoopWall is the world's first breach prevention security company delivering a suite of network, mobile and app security products as well as cloud-based services protecting all computing devices from prying eyes and new threats through patented counterveillance cloaking technology. SnoopWall secures mission critical and highly valuable confidential information behind firewalls with our award winning patented NetSHIELD appliances and with WinSHIELD on windows and MobileSHIELD on Google Android and Apple iOS mobile devices with next generation technology that detects and blocks all remote control, eavesdropping and spying. SnoopWall's software products and hardware appliances are all proudly made in the U.S.A. Visit us at http://www.snoopwall.com and follow us on Twitter: @SnoopWallSecure.

About the Author

Gary Miliefsky,
fmDHS, CISSP®,
CEO, SnoopWall

Gary is the CEO of SnoopWall, Inc. and a co-inventor of the company's innovative breach prevention technologies. He is a cyber-security expert and a frequent invited guest on national and international media commenting on mobile privacy, cyber security, cyber-crime and cyber terrorism, also covered in both Forbes and Fortune Magazines. He has been extremely active in the INFOSEC arena, most recently as the Editor of Cyber Defense Magazine. Miliefsky is a Founding Member of the US Department of Homeland Security (http://www.DHS.gov), the National Information Security Group (http://www.NAISG.org) and the OVAL advisory board of MITRE responsible for the CVE Program (http://CVE.mitre.org). He also assisted the National Infrastructure Advisory Council (NIAC), which operates within the U.S. Department of Homeland Security, in their development of The National Strategy to Secure Cyberspace as well as the Center for the Study of Counter-Terrorism and Cyber Crime at Norwich University. Previously, Gary has been founder and/or inventor for technologies and corporations sold and licensed to Hexis Cyber, Intel/McAfee, IBM, Computer Associates and BlackBox Corporation. Gary is a member of ISC2.org and is a CISSP®. Email him at ceo@snoopwall.com.

Learn more about SnoopWall's cybersecurity expert CEO at:

http://www.snoopwall.com/media/

For CEO interviews and Press Inquiries Contact:

Brittany Thomas
News & Experts
727-443-7115 Ext: 221
Email: brittany@newsandexperts.com

Mark Bermingham,
Vice President,
Worldwide Channels,
SnoopWall

Interested in Breach Prevention?

Please contact Mark Bermingham, Vice President, Worldwide Channels, SnoopWall

markb@snoopwall.com, 1-800-991-3871 x1001