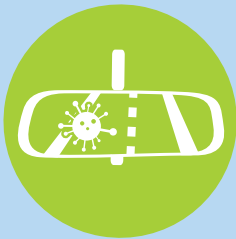
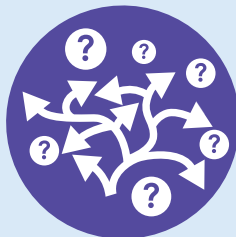






Mitigating Gartner's Network Security Worst Practices

An AlgoSec White Paper

Share on   

 **algosec**



| | | |
|---|---|----|
|  | Shiny New Object Syndrome | 3 |
|  | Culture of No..... | 4 |
|  | Insufficient Focus on Users and Business Requirements | 5 |
|  | Suboptimal Branch Architecture | 6 |
|  | Organizational Misalignment | 8 |
|  | Uncoordinated Policy Management | 10 |
|  | Defense with Inadequate Depth | 12 |
|  | Security Blind Spots..... | 13 |
|  | Hazardous Network Segmentation | 14 |

Introduction

Over the course of more than 3,000 client interactions in the past year, Gartner observed several common network security “worst practices.” These worst practices were documented in a great research paper titled “Avoid These “Dirty Dozen” Network Security Worst Practices”* which was released in early 2015.

According to the report Gartner’s clients “often underestimate, or are even unaware of, the potential negative impact of these practices. CISOs should assume that their organizations suffer from at least some of these issues and work to avoid them. Avoiding these practices will improve security posture and increase network availability and user satisfaction. Furthermore, most of these practices can be achieved without making large capital investments.”*

Here at AlgoSec, we’re no strangers to observing the network security practices of the world’s leading organizations. We have been fortunate enough to work alongside our customers to not only understand their challenges, but also to develop solutions that help them mitigate and even completely avoid these common pitfalls.

Through this collection of articles by AlgoSec experts, we’ll take a deeper dive into nine of Gartner’s network security worst practices, and examine how they can be mitigated using automated security policy management.

* Throughout, asterisks refer to this source: Gartner, “Avoid these “Dirty Dozen” Network Security Worst Practices,” by Andrew Lerner, Jeremy D’Hoinne, January 8, 2015.





Shiny New Object Syndrome

You Can Resist the Temptation of the Shiny New Tools

By Joanne Godfrey

Driven by market hype many IT security professionals and their CISOs believe that they must have the latest and greatest new tools to win the battle against cybercrime. But just look at one of the most discussed breaches of 2014. Target had a variety of tools and services already in place to detect and potentially block attacks. These existing tools did sound the alarm. But the company was too focused on its investment in new tools, instead of paying attention to their existing ones. This came back to bite them and millions of their customers, whose records were stolen.

Target is not alone: Most companies don't need to invest in yet another shiny new technology. In fact according to leading industry research, upwards of 95% breaches can be prevented by better managing existing technologies and making sure to cover the [security basics](#), such as removing unused firewall rules, ensuring systems are patched, removing unnecessary admin rights, etc. – all tasks that AlgoSec's [automated security policy management suite](#) can help with.

As Gartner says “changes to policy/process, leveraging an existing technology and/or simply waiting will achieve a similar impact. In many instances, avoiding acquiring new products can simplify the technical environment and reduce operating expenditure/capital expenditure.” *

Furthermore, it's important to note that only a handful of attacks (which are disproportionately amplified by the media) really use sophisticated attack tactics that the 'shiny new toys' can help protect against, and most organizations are not a target for those types of attacks.

In fact these tools can do more harm than good. First, precious IT time is needed to learn, deploy and adapt these tools to your environment – time that could be better spent on maximizing the benefits of your existing tools. Second, as with Target, these new tools will likely overload your staff with even more alerts and anomalies, and your overwhelmed staff may not have the skills and certainly not the time to analyze, prioritize, and address them.

So focus on what you already have first, and invest your time and expertise in covering your security basics, and optimizing your existing security technologies, processes and people. With a little polish and attention, your current tools will work even better than the “technology du jour.”



Culture of No

Saying No to the Culture of No

By Nimrod Reichenberg

According to Gartner, “Many Gartner clients make statements along the lines of “those IT folks prevent us from doing our jobs.” They specifically cite that security departments implement policy and controls without regard for business function.” * Does this sound familiar to you?

The solution to this network security worst practice is twofold, as is often the case. We know the first step requires a change in culture and attitude. One CISO I recently spoke with forbids his team from using words such as “no” and “can’t” and makes them replace these words with “how?” Surprisingly, this isn’t just the right thing to do from a business enablement standpoint; it’s also the right thing to do from a security standpoint. Users who are constantly blocked by security from doing their work will find ways to bypass those controls — most likely using less secure platforms. Just in case you have been sleeping under a rock for the past 5 years, anyone with a credit card can now spin up their own machine on Amazon Web Services (AWS) in minutes, away from IT’s prying eyes. And of course there are readily available services such as Dropbox for storing information.

But there is another reason why security and IT often stand in the way of business — and that is lack of visibility and control over how their actions impact

business functions. Without such visibility, it’s easy to revert to the lowest common denominator – forbid it. This is where security policy management solutions can help. With relatively new and innovative solutions that offer *visibility and control of application connectivity* requirements, network and security practitioners can rise above the bits, bytes and IP addresses and see how enabling (or removing) access impacts business services. This visibility can also take the security and compliance mandates of your organization into consideration.

Sometimes a good reason for saying no may exist, such as a PCI-DSS violation, but with the right solution, security will have the data in its hands to explain and justify the decision, as opposed to just being a naysayer.

With proper visibility and control, most business requests can be safely enabled, moving your business forward, and making you more popular at the next office party.



Insufficient Focus on Users and Business Requirements

Taking Care of Your Business

By Nimrod Reichenberg

According to Gartner, "Security projects that are owned exclusively within the security team face the risk of neglecting business and user requirements, which are too often seen as constraints." *

Security teams are often guilty of taking this concept to the extreme, assuming business users will do stupid things which only a strict security policy can prevent. However, as crazy as this notion may sound, security is here to enable business, and not the other way around. While not always easy, I believe this worst practice can be much improved by taking the following steps:

1. Put yourself in the business users' shoes. Retail companies have been conducting mystery shopper exercises for years, in order to understand the shopping experience from the shopper's perspective. Try and go through the same steps a business user would to perform a certain task. If you are frustrated by the experience, chances are the user will be as well. See if you can remove obstacles without sacrificing security.

2. Collaborate early with business users. Unfortunately, security is all too often an afterthought which is bolted on once an application or business process has been finalized. Forward looking organizations are extending the DevOps model to include security, a practice often dubbed DevOpsSec.

Call it what you like, it basically means security teams are involved early in development projects so that they can see how these applications should be secured while still in the design phase.

- 3. Ensure visibility into the business impact of security operations.** With the complexity of today's networks and applications, it's very difficult to understand the impact of a security change (such as adding a firewall rule) on business applications. This can have some serious implications including:
- Business services outages caused by misconfigurations.
 - Weak network access lockdown since access is never removed for decommissioned applications for fear of breaking something that is working.
 - Slowing down or even blocking productivity because of an inability to understand how business requirements translate at the network level.

To summarize, security teams should ensure they adopt the right mentality, incentivize the right actions and make sure to have the right solutions to align security operations with the business.



Suboptimal Branch Architecture

Finding the Right Notes for Your Network Security: The Trombone Effect

By Edy Almer

Global organizations today face some big challenges when it comes to figuring out the best architecture for their networks. On the one hand they need to get their applications closer to their users for better performance, but on the other hand they need to centralize security in order to leverage new features and capabilities that are continuously being released onto the market and therefore require specialized management by a bunch of highly trained and knowledgeable security analysts. This is what Gartner has coined “the trombone effect.”*

I believe the trombone dilemma is applicable to at least two additional core scenarios: The first is Internet access within branch offices, and the second is your basic data center architecture where multiple boxes reside physically near each other inside the data center. In this scenario traffic must flow through multiple ports before it can benefit from the huge, advanced firewalls at the edge of the data center.

To address the first scenario — internet access at the branch office — companies often route risky traffic back to the heavy guns for security, or deploy multiple boxes at the branch office. But both of these options have significant downside: latency and/or high cost.

In their research note, Gartner recommends that “Organizations should look to build hybrid WANs, which combine Internet and Multiprotocol Label Switching (MPLS)/Ethernet”* as a solution for “tromboning.” I believe that there are some additional solutions that should be considered. For enterprises not in the process of fully moving to the cloud just yet (which is essentially the vast majority of organizations) one option is to use trailblazing solutions such as zScaler. zScaler has proved that security delivered via a cloud offering can be as good, or in fact even better, than an on-premise internet access security architecture.

For internal applications that need to be deployed close to the end-users for performance as well as for internal data center security — i.e., the second scenario — utilizing a private or public cloud deployment architecture is a possible solution to alleviate “tromboning.”

In addition, today most firewall vendors, and increasingly many other security vendors offer virtualized versions of their kit with pricing models to match an enterprise’s needs. These pricing models are as important as the virtualization itself. The ability to run tens or hundreds of small firewalls wherever you need them, instead of one big box at the edge, without losing functionality, enables the deployment of security close to the applications that need it, and reduces ‘tromboning’ and associated latency — although it also adds management overhead (which

is something that AlgoSec's security policy management capabilities can help alleviate). This deployment model enables you to match firewall capabilities to required functionality and allows you to have firewalls embedded in the fabric of your network.

But this does come at a price: now both your security analysts and your network analysts need to have a comprehensive understanding of your entire network topology. As Gartner says, "To build the ideal balance between security controls and WAN performance, networking and security teams must work together."* And as these two teams collaborate, both will need a solution, such as AlgoSec, that will enable them to speak the same language and manage their security policy across their entire hybrid environment.



Organizational Misalignment

All War and No Play: Align Your IT Organization to Eliminate End-User Frustration

By Nimrod Reichenberg

In my previous *article* I discussed the problem of insufficient focus by IT teams on users and business requirements. In addition, it's also important to remember that groups within the IT organizations are often misaligned as well, which Gartner refers to as "warring factions" and "us versus them."*

According to the research, "Within many IT organizations, security is seen more as a bolt-on appendage to IT rather than an integral component that should be baked into all architectures. This leads to end-user frustration and fosters kingdom-building versus deep integration between teams."* "The end results of both intrasecurity and IT organizational misalignments are unhappy users; reduced security; and architectures that are more complex, costly to operate and difficult to scale."*

One area where this misalignment is clearly visible is between the networking and security teams. Many of our customers report frequent 'blaimstorming' meetings where these two teams blame each other when things are not working or not progressing quickly enough.

I am a big advocate of examining solutions from both a processes and a tools perspective. However, while AlgoSec is a software provider, I am the first to acknowledge that a good tool will not fix a bad process

(a well designed software solution can however, force you to rethink and redesign your processes). On the flip side, a good process which can't be enforced will not go very far either.

So let's first examine what you can do from a process perspective to address organizational misalignment:

- 1. Align incentives.** Aligning incentives to create shared goals may be common knowledge, but it's hardly common practice. In many organizations there is an inherent conflict between the goals of networking team and the goals of the security team. The networking team may be concerned with maintaining network availability which is obviously hindered as security and access restrictions pile up, while the security team resists any architectural changes if they can potentially introduce new risk. So consider defining both security and networking goals for both teams.
- 2. Align reporting structures.** In some organizations, the CISO reports outside of the IT department (e.g., to the CFO). In the absence of a common boss inter-team tension can quickly escalate.

3. Foster collaboration. There are many ways an organization can foster better collaboration between teams. Simple things such as joint social events or locating the teams in close proximity can go a long way. Another common approach is to have “overlays” where the networking team has a representative in the security team and vice versa.

From a solutions perspective, here are some things you should look at to improve alignment:

1. Single pane of glass. All too often the security team’s view of the network and risk are different to those of the networking team due to different tools that are used by each team. It is imperative that both teams use the same solution for provisioning and making changes to network security devices.

2. Holistic process analytics. Without good data and visibility it’s not easy to understand where you may have made mistakes or introduced bottlenecks. Tracking each stage of the network change process (which team requested the change, how long did it take to analyze it, approve it for risk, provision the change, etc.) can help you identify and resolve inefficiencies.

3. Automation. First and foremost, automation can eliminate mistakes which reduces tension. Automated tools are also better than human beings at translating requests that may be communicated in one language (e.g., the language of networking) into another language (that of security). Finally, whenever a person has to say no to a request, there is a potential for friction. However, if an automated solution does not allow something, it creates a sense of fairness: “the system won’t let me approve this” rather than “I don’t allow you to do this.”

With the speed of today’s business, and with increased focus on automation, the lines are quickly blurring between operations and security teams. Aligning these teams is therefore quickly becoming an imperative. If your factions are warring, don’t delay doing something about it.



Uncoordinated Policy Management

Who Put That in Here? (And Who's Going to Take It Out)

By Nimrod Reichenberg

Helping organizations improve security policy management is obviously at the heart of what we do at AlgoSec. In many ways, I feel this Gartner worst practice is really the aggregated result of many of the worst practices we have already covered, such as [*insufficient focus on business requirements*](#) and [*organizational misalignment*](#). But at the end of the day, most of the ailments that result from poor security policy management are, according to Gartner, due to the “use of unsustainable and nonscalable tools and processes such as spreadsheets”* to address an increasingly complex task. As a result, the network security policy is cluttered, and processes to add and remove rules are inefficient and error prone.

Here are just some questions we ask organizations that we work with. The reply is usually a nod ... and a sigh.

- What happens to firewall rules when an application is decommissioned from the network? Do you safely remove them knowing that no other application is going to break?
- Have you ever suffered an application outage due to a firewall rule change gone wrong?
- Do you have difficulty understanding what the application team requires from the networking perspective when they deploy a new application or update an existing one?

- Do you have a good understanding of the business reason for each firewall rule in place? How good is your documentation?

Notice that the words business or application appear in every question. We have talked about the divide between operations and security teams. A potentially bigger divide exists between IT and application teams. This is the root cause of uncoordinated policy management.

Here's what you can do to transform the way you manage your security policy:

1. Adopt an application-centric approach. Instead of focusing on ports and protocols, make sure you can understand and map the firewall and router access rules to the business application they support. This is not an easy exercise, an innovative solution for [*application connectivity management*](#) can greatly simplify this process.

2. Automate change control and documentation. Leverage [*security policy change automation*](#) solutions to process changes more quickly and accurately. One often overlooked benefit of these tools is automatic documentation. As you are making each change, each step of the change, including the business reason for the request, the risk implications, and even the date it needs to be recertified is documented. This not only simplifies your next audit, it also makes information readily available to all, improving coordination.

3. Extend DevOps to network security. The DevOps movement is continuing to gain traction and for good reason. Better aligning IT and developers has many benefits. Look to extend the DevOps model to include security so that security people are involved early in the development process to better understand how to provision security for applications.

Policy management is uncoordinated at most organizations, but it doesn't have to be. With the right tools and processes and, more importantly, with the conviction that things must change, every organization can take steps to make policy management a much more seamless process.



Defense with Inadequate Depth

More Vendors, More Security?

By Avishai Wool

For several years security teams have viewed the defense in depth network security strategy as akin to building castle walls, with each wall providing an additional layer of protection. In theory, multiple protective layers should make a network more secure — if they're done right. But somewhere down the line, confusion has developed over what a layer really means, with many companies thinking that using multiple vendors for the same type of task provides an additional layer of security. Not only do redundant layers which provide the same kind of protection from different vendors not increase your security, they may actually impair it.

You may think that by using firewalls from two or more vendors you'll have overlapping protection, where the weaknesses of one vendor solution is compensated by the strengths of the other. However, industry research shows that the vast majority of firewall-related incidents are not caused by vulnerabilities introduced by the firewall vendors; they are caused by administrator misconfigurations.

Your real risk with using multiple vendors comes from your staff, or more specifically their skills and time. If your staff has to work with multiple vendor solutions it will likely make things less secure. With two (or more) vendor solutions, the networking and security staff need twice the training. Yet in real life, they usually receive the same amount of training regardless of the number of vendor solutions they have to manage, so they have less competence than had they focused on just one solution.

Less familiarity leads to more mistakes, which leads to greater vulnerability and risk. In addition, multiple vendor solutions increase costs by eroding volume discounts. As a result, the company suffers a double whammy — less security and higher costs. In practice it is much more efficient, cost effective and secure to standardize on one vendor for each specific function.

For real defense in depth, each layer must do something functionally different. If, behind the firewall, you have a DLP solution or a web filter, you now have two different dimensions and additional security that's structured in a tiered way. You can also achieve true defense in depth protection through network segmentation, using just one vendor solution. In this scenario, you could have outer and inner firewalls plus specialty firewalls that protect high security data, and a variety of internal "choke points" to protect access to this data.

Whichever way you go, security policy management solutions can provide the critical visibility and automation needed to achieve your defense in depth goals. It can help with defining and enforcing network segmentation, automating firewall change management processes, and maintaining compliance. The AlgoSec solution is vendor agnostic so we can support your environment however many vendor solutions you use or however you structure it. But for your sake, keep the number of vendor solutions down so you stay more secure.



Security Blind Spots

Mind the Security Gap – It Is Your Job

By Joanne Godfrey

We all know that managing security is more demanding than ever before. We're being bombarded with cyber threats, our highly complex environments are constantly evolving, and we face relentless demands to deploy or update enterprise applications impossibly fast in order to maximize our business' productivity and ensure that it remains competitive.

So it's no surprise, as Gartner says, that "most security gaps are already known by the security team, but have not been addressed because of other priorities."* But claiming that it's "not my job"* or that you don't have the time to address security gaps is not good enough anymore and isn't going to hold water when you've been breached or when a critical business application suffers an outage — as many CIOs who have recently lost their jobs will testify.

One solution is to use automation. Automation frees up time — so automate as many security functions as much as possible. Automation also reduces errors, streamlines processes, and aligns IT teams towards common goals, which goes a long way to identifying and bridging security gaps. And with automation you can build critical steps into security management processes that will plug known gaps — steps which might otherwise be overlooked or forgotten if security professionals are too busy to do them manually.

Another way to help "mind the gap" is by unifying security management as much as possible. Having a single solution that provides holistic, real time visibility and enables unified security management across your entire on-premise, virtual and cloud environment makes it much easier and quicker to identify and address gaps, risks and opportunities within your security strategy.

A unified approach to security management also helps plug security gaps created by "shadow IT," i.e., when R&D groups bypass IT and security to spin up servers and applications in the cloud, usually for development and testing purposes. With a unified approach to security policy management, everything is seen and nothing can slip under the radar — and IT will no longer be responsible for mitigating risks for applications it doesn't know exist.

In the report Gartner specifically calls out application security, mobile security, and public cloud platforms, among others, as examples of where security is "too thin"* and therefore creates blind spots. And in a [recent AlgoSec survey](#), two-thirds of organizations said that security across the public cloud poses a significant challenge due to lack of visibility, tools and workflows. Automation and a unified approach to security management will go a long way to addressing these risks and strengthening the security posture of companies with hybrid environments.



Hazardous Network Segmentation

When More Isn't Better

By Avishai Wool

Both under and over-segmentation of networks are extremes that pose different challenges to organizations. Finding the right balance is essential to providing security while supporting business agility.

The risks posed by under segmentation are clear enough. In the “old days,” organizations established a perimeter firewall to keep the bad guys out and that was it. We called it “crunchy on the outside, chewy on the inside.” As a result, many companies found their networks chewed up and key data breached. Obviously, the problem here is that a single breach of the outer firewall makes the entire network vulnerable.

So in order to block free access to all the organization’s goodies — credit card information, patient data, intellectual property and such — security teams implemented network segmentation. By creating zones or segments with their own additional protection or layers of defense, they limited the ability for “nefarious actors to access systems via lateral movement in the environment,”* as Gartner puts it.

But there can also be too much of a good thing — in this case microsegmentation. I suggest that we think of microsegmentation as analogous to micromanagement: good intentions that can sometimes create an unworkable situation. With an excessive level of segmentation, the costs and time required for day-to-day management make it unmanageable, and both business agility and security suffer.

To get an idea of the scope of work involved in maintaining microsegmentation, consider that you have to define what you want to allow between each pair of zones. If you have 50 zones in a network, you have 50 x 50 or 2,500 policy choices to make. That’s quite out of control. Now imagine what could happen if you had a zone for every few servers: the calculations and policy maintenance are far beyond human capabilities. In real life, you want to maintain fewer than 15 to 20 zones. If you get much beyond 30, you’re deceiving yourself in thinking you can manage them.

So what can you do? Network segmentation is a significant, wide-reaching undertaking that requires considerable planning and ongoing management, and there are technology solutions that can help. AlgoSec’s security policy management suite can simplify the complexity involved in defining, deploying and enforcing the security policies that are at the core of your network segmentation strategy. Furthermore it can help avoid disruptions and limit the risks caused by accidental firewall misconfigurations. And as your business needs evolve, AlgoSec’s unique visibility and automation will help you effectively ensure the integrity of your network segmentation strategy while responding to business initiatives.

About the Authors



Avishai Wool, AlgoSec's CTO, is a frequent speaker at industry conferences and has published more than 90 research papers and holds 13 US Patents with more pending. He is also an associate professor in the School of Electrical Engineering, Tel Aviv University. When he's not busy evangelizing AlgoSec's solutions, Avishai enjoys tinkering with all sorts of computer and network security technologies. [in](#)



Edy Almer runs Product Management for AlgoSec. A user-oriented craftsman with forays into marketing and business development, Edy cares about the customer first. He has presented sessions at Infosec UK, RSA, Cebit, IT-SA and many other industry events, and has published articles in Network World, eWeek, Forbes and other leading industry and business publications. [in](#)



Nimmy Reichenberg heads Global Marketing for AlgoSec and surprisingly actually understands what he markets. Originally a software engineer with security focus, Nimmy designed and developed security products before switching over to the dark side and becoming a marketer. Nimmy has published many articles in security publications such as SC Magazine, Dark Reading and Network World and has presented at leading security conferences. [in](#)



Joanne Godfrey is a hands-on marketer with a passion for communications. Joanne has marketed a wide range of enterprise technologies over the years including networking, security, application performance management, data management and virtualization, and published many articles in industry and business publications. [in](#)



Global Headquarters

65 Challenger Road, Suite 320
Ridgefield Park, NJ 07660
USA
+1-888-358-3696

EMEA Headquarters

80 Coleman Street
London EC2R 5 BJ
United Kingdom
+44 207-099-7545

APAC Headquarters

10 Anson Road, #14-06
International Plaza
Singapore 079903
+65-3158-2120

