AXIM™ | SentryWire PACKET CAPTURE PLATFORM

5 ways to sweat network security budgets

Security spending is no longer a bottomless pit. The greatest challenge for IT and network teams is not the next WannaCry, negligent or malicious insiders, or even needle in a haystack searches – it will be delivering a sufficiently deep security posture with insufficient budgets. How do you square the circle? Here are 5 ways to sweat your network security budgets.

How do you make network security budgets go further?

Here's a worrying thought: security spending is no longer a bottomless pit. Businesses are losing more than they are spending and by 2021 $6 will be lost for every $1 spent[1]. The result? More and more boardrooms are becoming involved in security budget setting and there are clear signs that the open checkbook is closing: organizations need to spend up to 50% more on security this year, on average they'll get 10%.

Network and IT professionals will have to make less go further by acting differently, seeking technologies that combine incident response and network troubleshooting, and by harnessing lower cost network packet capture tools.

Arguably the greatest challenge will not be the next WannaCry (what a great name), negligent or malicious insiders, or even needle in a haystack searches – it will be delivering a sufficiently deep security posture with insufficient budgets.

For those who will have to square this circle, here are five strategies that could just help:

5 ways

to make network security budgets go further.

- one: Think just enough and accept there will never be enough.
- two: Focus more on the everyday and less on zero-day.
- three: Look backwards not forwards.
- four: Invest in transformational technologies.
- five: Prioritize hybrid security solutions.

1. Ernst & Young

one:

Think just enough and accept there'll never be enough

The big driver of an open checkbook is the relentless innovation in cybersecurity threats and breaches. 75% of organizations would likely increase their cybersecurity resources following a breach (thanks again Ernst & Young).

It's creating a corporate culture that fights every fiber of good governance: a be-safe-after-the event culture and a corporate acceptance that there will never be enough security in place.

A security budget ceiling will force a culture change, a culture of realism that may not be good news for the security industry but will be great news for compliance teams and shareholders. At its heart are three core elements:

1. An acceptance that protecting all aspects of security at all costs is unrealistic and ungovernable.

2. A realization by network managers that although in many ways they are gods, they cannot hold back the tide of security breaches: organizations will and are being breached almost continuously.

3. A focus on 'just enough': that identifies and secures the most critical elements of an organization, maximizing investment against these rather than spread it thinly across more and more security demands

two:

Focus more on the everyday and less on zero-day

One of the big reasons organizations need a big increase in security spend is the growth in internal and external threats and breaches. Clearly the threats won't lessen so the challenge is to identify the biggest volume of most critical threats and focus spend on them.

One decision organizations will have to make is to spend more on defending against zero-day attacks or the everyday attacks. It's a no-brainer: Gartner says zero-day accounts for just 0.4% of all vulnerabilities in the last decade. The 99% of vulnerabilities are the real challenge: those insidious actions of organized crime and employees that only occasionally create media noise (sorry for reminding you Equifax and Facebook). Over half of IT decision-makers are kept awake at night by insider threats. That's a lot of sleepless nights, it says to me where the emphasis should be. But whilst prioritizing the everyday will help focus budgets, it will also create some big challenges for network management:

Managing the digital transformation double whammy.

Digital transformation won't just create UX and CX challenges, it will fuel threats that have never been seen or thought of. Cybercrime will create new weapons, whilst new technologies will make employees more careless and negligent and help malicious insiders to be even more vengeful.

Going beyond technology.

Network professionals will have to think beyond technology and look to the entire digital security chain. They will have to focus on managing and communicating risk and go beyond restrictive controls to user behavior monitoring and analysis. And they will have to drive process and cultural change management.

three:

Look backwards not forwards

As network teams focus security budgets on their greatest threat and breach risks there's an obvious starting place: the past. It seems counter-intuitive as we are constantly looking to the next new network intrusion, but the logic is compelling. Most network breaches have already happened. They're not zero-day, they're the ones that normally take between 146 to 191 days to detect, and another 60 or so days to contain. These are the ones that can truly decimate businesses.

Just in case you needed reminding. The recent massive breach at Dixons Group in the UK happened almost a year ago. Equifax still has over 240 class actions. Home Depot is still paying out 3 years and $180m later. Whilst Facebook lost $50bn of its market capitalization in two days.

Detection and remediation will increase.

Doesn't it then stand to reason that concentrating more budget on identifying solutions that most effectively manage what's already happened will be more important than protecting against what is yet to happen. Gartner sees it as the future, predicting that by 2020 60% of information security budgets will be allocated to reducing the time to detect and accelerate recovery and remediation – a 200% increase on 2016.

Smarter management of ransomware attacks.

Won't this strategy increase your potential exposure to ransomware at a time when one business will be attacked every forty seconds? (it will be every fourteen seconds by 2019). And won't it expose organizations to even greater costs? (WannaCry was estimated at $8bn). The answer is yes. But there are less costly strategies to manage ransomware. Like educating employees on the techniques the distributors of ransomware use is a critical first step, as is good network and security hygiene measures and routine and frequent back up.

From the IT room to the boardroom.

The bottom line is that prioritizing investment will require hard decisions and smarter thinking. Network professionals won't have to do this alone. The cost of breaches to a business and the limited effects of high security spending are bringing the boardroom into the IT room. Research by PWC suggests 40% of boards are now involved in security budget setting, and 43% partake in the strategy. An unwanted influence? Maybe. But it will bring network professionals a new perspective when making tougher decisions.

We will see a greater use of infonomics to analyze data assets and liabilities, and security outcomes will be more strongly connected to business outcomes. Management will bring new evaluative criteria to security investment, like competitive advantage, growth and brand trust. And there will be a more strategic approach to spending budgets, informed by improving security posture and better protection.

four:

Focus on the transformational technologies

Leveraging finite budgets and resources to contain exponential security threats will undoubtedly put technology front and center. The adoption rate of more sophisticated security technologies is accelerating. Real-time change auditing solutions and analytics will help secure critical assets. 'Remote browsers' adoption will isolate a user's browsing session from the network and deception technologies will become more commonplace. Endpoint Detection and Response (EDR) solutions, will monitor endpoints and alert to suspicious behavior. And, Network Traffic Analysis (NTA) will monitor network traffic to help determine the type, size, origin, destination and contents of data packets.

But what happens when budgets come under greater scrutiny? The question will become 'which technologies will deliver a 'just enough' strategy, help accelerate detection and remediation, and secure the maximum number of everyday vulnerabilities?' The answer lies squarely with the transformational technologies, and the list reads like a game of buzzword bingo.

AI will become a linchpin.

AI and machine learning will come to define the 'normal' state of systems: monitoring networks and the deviation that will accurately identify attacks, getting breach updates in real-time, and, better chasing down yesterday's attacks. AI will help network professionals more intelligently manage budgets; especially the growing managed security services, incident response services and detection and remediation services.

Solutions are adapting to hybrid cloud.

Monitoring hybrid cloud architectures has caused network professionals' real headaches, an inability to predict resource utilization or support dynamic environments. But network performance monitoring players are now releasing solutions that provide end-to-end visibility for business-critical applications.

Analytics are becoming integral.

Increasingly data analytics are being built into network performance monitoring software. It's bringing new opportunities like collection, analysis and the prediction of network trends, the transformation of data into insightful information and the management of API interfaces.

Software-defined solutions are crossing-over.

Arguably the top of any marketing hype list is software-defined anything. But when applied to networking it makes sense, especially as organizations seek to cap costs and manage multiple types of connections. They seem to be buying it. Gartner predicts that 25% of users will manage their WAN through SD by 2019, and by 2020 it will be a $1.3 billion market.

Transformational technologies will be an ally and an enemy.

It's clear the transformational technologies will be a powerful ally to network professionals as they do more with less. They would be wise to look at these technologies as enemies as well.

AI will also power more sophisticated attacks: by automating data collection, cracking passwords, utilizing chat bots and committing cryptographic attacks. As the cloud grows so does the cyberthreat. Increased cloud security will become a top priority. Adding telemetry to cloud workloads will better manage security failures, allowing organizations to see the danger signs and enabling a quick, and possibly preventative response. Security experts will have to decide who to trust and not, whilst companies will develop security guidelines for private and public cloud use - utilizing a cloud decision model to apply rigor to cloud risks.

five:

Look to hybrid security solutions

The headline from these strategies is that in a do-more-with-less security landscape network and IT professionals must look to security solutions that can do more: hybrid not point solutions that can deliver a depth of functionality, but not compromise on efficacy. The currency becomes utility but how do you identify the utility value? One way is to develop a utility checklist. What would one look like? Based on the strategies outlined above, here's a starter for ten:

1.	Will it deliver a 'just-enough' security and secure a critical element of security?
2.	Can it help accelerate detection and remediation, can it help to better and more speedily mitigate a breach that's already happened? Will it fuel prediction?
3.	Will it secure the maximum number of everyday vulnerabilities and counter zero day ones as well?
4.	Can it look into the past?
5.	Will it integrate the critical transformation technologies?
6.	Can it deliver a value proposition that will satisfy the board?

As network and IT teams begin to assess the potential technology solutions against a different corporate, financial and security environment, one technology stands tall above others: network packet capture.

It's time to recognize the value of network packet capture

What places it above the other defining network security solutions: VPNs, network analyzers and packet sniffers and deceptive network technologies?

First it is a real hybrid solution, it can bridge network intrusion and network monitoring. Network packet capture can accelerate incident response through unlogged activity detection, data and malware exfiltration detection, phishing preparation detection and indicators and signature alerting. Network packet capture can also enable network troubleshooting through forensic traffic analysis, Network Access Control analysis, user anomalous behavior, network behavior anomaly detection and encryption visibility.

But when you assess network packet capture against the utility value checklist, it comes into its own:

Deliver 'just-enough' security.

The hard edges of a firewall can no longer protect against external access: the traditional network confines have been splintered by personal devices, remote working, visitors and the Internet of Things. Defining the organization's perimeter virtually impossible, and it makes the network one of the critical focal points in a 'just enough' strategy.

Accelerate detection and remediation.

The new network packet capture tools can search petabytes of network traffic in minutes, making long detection and containment times history. Their architecture can scale search as it scales computation and storage. They search over smaller data stores, dramatically increasing search results. And they manage very large PCAP files reducing them to digestible bites so that search results are streamed almost immediately and don't bog down the network.

Secure the maximum number of everyday vulnerabilities.

Full network packet capture goes beyond metadata to high fidelity traffic records. It offers the fastest capture speeds up to 100Gpbs. Unlike network sniffer tools it inspects packets and retains the metadata, captures and stores all network IP packets, filters them against known signatures, and continuously inspects and analyzes them for signatures that materialize once the traffic is filtered, collected and stored.

Full packet capture can also help network and IT teams manage zero-day threats by analyzing the network history around the breach to see how they got in and what has been compromised.

Look into the past and present.

The latest tools can packet capture tens of petabytes of network traffic data, massively extending the timeline of data capture. They offer enough to meet the average 146-191 days it takes to detect a breach, to get to the root of the problem and determine which data was accessed and exfiltrated.

Integrate the critical transformation technologies.

Network packet capture can bring AI and machine learning to identifying out of normative security threats and data breaches, as well as application and network performance monitoring. Network packet capture can also enable organizations to extend existing enterprise network and security policies into their cloud environment.

Deliver a value proposition that will satisfy the boardroom?

Based on the above, absolutely. The clincher is that the cost of network packet capture has tumbled, it can be less than 25% of the cost of traditional network packet capture, and it can cut the cost of massive data storage by up to 80%.

A parting thought

The big threat to your network is not cybercrime or negligent and malicious employees, it's an insufficient budget and it will open-up network threats and breaches. But that's only one of the network-related challenges that network and IT professionals will face. Network continuity and complexity will be up there. As will alignment of networks with public cloud, the fragmentation of NetOps and its convergence with IT security, then there's the increased outsourcing of network management. What's the answer? Focus on solutions that can help more facets of your network management strategy, from security to monitoring and troubleshooting. At the heart of these is real-time and real depth network visibility, and the ability to speedily and efficiently respond to what you see – at lower cost of course!

Author

Dan Davies is CMO of Axim. Axim helps organizations better manage the big risks their data, infrastructures, technologies and service delivery bring to their users, their customers, their business performance and their corporate reputation. Axim is a distributor of SentryWire, the newest and most advanced network packet capture tool.

Discover more visit www.aximglobal.com/sentrywire

Or email sentrywire@aximglobal.com

About Axim

Axim is a global partner for SentryWire, a next generation full network packet capture tool. It's just one of the solutions we bring to help organizations better manage CX risk, and protect their customer loyalty, corporate reputation and commercial bottom line. Learn more about our data and technology risk-management solutions, and our range of CX governance offers and platforms.

AXIM™

www.aximglobal.com