WHITE PAPER

proofpoint.

FLIPPING THE SCRIPT ON SECURITY SPENDING

INVESTMENT STRATEGIES TO PROTECT AGAINST ADVANCED THREATS AND TARGETED ATTACKS

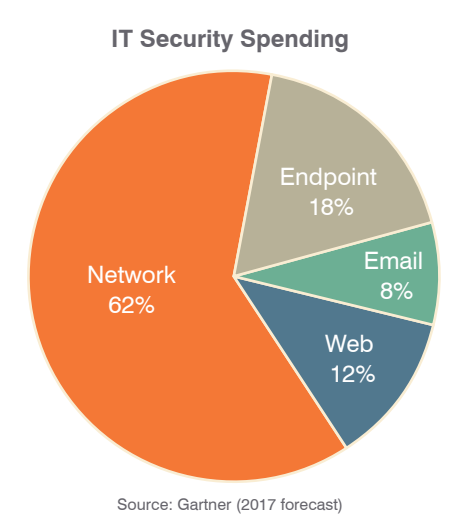
TABLE OF CONTENTS

INTRODUCTION

Cyber criminals target your company because that's where the money is. It's just that simple. Security budgets should be that simple and fund security controls in the vectors where the threats come from.

But the question of how to spend a security budget is a complex one. More than 95% of cyber attacks arrive through email.[1] Yet 92% of the average 2017 security budget will go toward non-email defenses such as network, endpoint and web security tools.[2] The remainder—a mere 8%—will be used for email security.

Equally perplexing is the criteria used to evaluate and purchase new security solutions. Performance and cost is cited as top reasons for purchasing a new solution. Yet complexity and operational difficulties are leading reasons security tools are scrapped before or soon after deployment, according to a recent Ponemon Institute study.[3]



Other studies show similar challenges. Everyone surveyed in a recent Cloud Security Alliance poll—a full 100% of participants—expressed significant challenges rolling out and managing endpoint agents.[4] Yet, endpoint security receives the second highest number of security dollars according to Gartner spending forecasts.

[1] Verizon. "Data Breach Digest." February, 2017
[2] Gartner. 2017 Worldwide Spending on Information Security Products, August, 2016
[3] Ponemon Institute. Risk & Innovation in Cybersecurity Investments, April, 2015
[4] Cloud Security Alliance. IT Security in the Age of Cloud Survey Report, October, 2016

TODAY'S SECURITY MUST EVOLVE WITH THREATS

While network and endpoint security solutions get the majority of the security budget, threats evolve and the challenge of securing the business has changed:

- The traditional corporate network perimeter is quickly dissolving. Mobile and cloud solutions are being used for everyday business.
- Exploit kit activity that dominated the threat landscape a year ago has slowed to just a trickle of its former volume
- Ransomware, Trojans and rootkits that once were distributed via exploit kits are now being spread via email
- Macros are back in style and document-based attacks are replacing what exploit kits used to do

Seismic shifts in advanced threats and targeted attacks leave no room for security teams to wait around. A successful credential phishing email can bypass most perimeter and endpoint defenses. That's because credential phishing does not contain any malware that network defenses can detect and attacks using stolen passwords is not easily detectable by endpoint security controls. These solutions leave security teams with no way to tell if a credential phishing attack occurred without an employee call to the help desk.

Advanced threats are just as challenging to conventional security approaches. These threats include ransomware, business email compromise (BEC), zero-day threats, polymorphic malware, and credential-stealing threats.

What was once good enough is no longer enough to protect your organisation. You need a different approach security—one that directs your existing security budget to protect the way employees work.

This paper weighs the merits and drawbacks of current approaches and recommends a better way to invest your security budget to defend against the complex nature of today's threats.

SECURITY INVESTMENT STRATEGIES

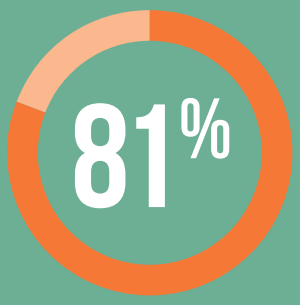
Security teams typically invest their security budget in one or more of the following ways:

- **Baseline security**—Employ patching, asset management and keep signatures and anti-virus (AV) definitions up to date
- **Network security**—Improve IPS defenses, detect and block malware using analysis of network-based traffic
- **Endpoint security**—Add endpoint security management to enforce policy
- **Email security**—Block unknown malware and credential phishing attacks before they reach employee inboxes

BASELINE SECURITY INVESTMENTS

Security teams continually invest in their baseline security measures. They provide foundational security controls every company needs. Unfortunately, security efforts often stop there and does not progress beyond the basic security measures of patching and asset management.

Some companies take a wait-and-see approach and rely on hope as a security strategy—call it the "I hope we don't get hacked" approach. One in five security practitioners surveyed at the 2015 Security BSides conference said their management relied on "hope" as a security strategy. A full 35% said management "lacks a healthy paranoia about cyber threats."[6]

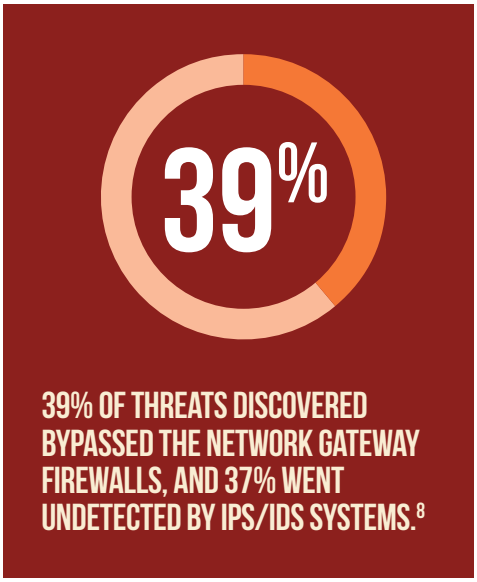


81% OF CIOS, CISOS, CTOS AND CIOS SURVEYED BY KPMG ADMITTED TO A RECENT BREACH—BUT LESS THAN HALF SAID THEY'D INVESTED MORE IN SECURITY AS A RESULT.[5]

[5] KPMG. "Consumer Loss Barometer." August, 2016
[6] DomainTools Survey. "Security Pros Concerned Their Organization Lacks A 'Healthy Paranoia." August, 2015

Some companies stay stuck maintaining basic security controls. Others recognise the opportunity to move beyond a baseline strategy and enable new security protections that reduces risk in the organisation. Beyond the pain and loss of experiencing a major breach, there are few ways to pull management away from an engrained "hope for the best" approach.

To justify an investment, security teams are left in the difficult position of needing to demonstrate the caliber of advanced threats aimed at the company so that they can get the funding to implement preventative measures. If you currently work with limited threat intelligence and visibility into your attack surface, it can feel like you are stuck in a catch-22 situation.



NETWORK SECURITY INVESTMENTS

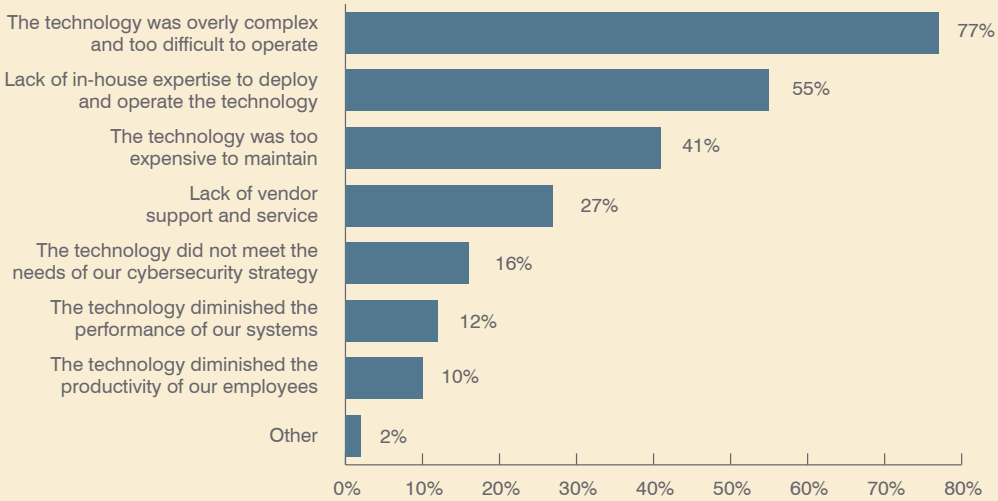
For years, network-driven approaches have been the go-to solution for combating advanced threats and targeted attacks. This is changing as security teams recognise new ways that attackers are able to bypass perimeter defenses.

For example, BEC and credential phishing are malware-less threats that easily bypass network and endpoint security controls. Network tools can be useful for detecting some attacks already in your environment. But they don't stop the threats from getting there in the first place.

The sheer number of shelved network security tools strongly suggests that organisations realise they need a better defense. While there are dozens of ways to improve network and perimeter defenses, they tend to fall into one of these categories:

- Intrusion and perimeter tools
- Heuristic detection
- Network sandbox analysis

WHY SECURITY TECHNOLOGIES ARE SCRAPPED BEFORE OR SOON AFTER DEPLOYMENT



Source: Ponemon Institute Risk & Innovation in Cybersecurity Investments survey, February 2015

[7] SANS Institute. "Exploits at the Endpoint: SANS 2016 Threat Landscape Survey." September, 2016

INTRUSION AND PERIMETER TOOLS

Depending on the maturity of your investment in intrusion prevention systems (IPS), you may have deployed this capability with next-generation firewalls (NGFW), secure web gateways, or standalone appliances. You have several options to defend your company from advanced threats using IPS technology. Inline IPS systems, secure web gateways, and SSL network proxy tools are the more common.

Inline IPS deployments

When an IPS is deployed out of band or set to an audit mode, the next logical step is bringing your IPS inline on your network or web gateway. This step provides the benefit of real-time detection and monitoring. But the technology relies on file signatures so it can only detect and block only known malware. More importantly, it is not equipped to inspect and block SMTP traffic or provide off-network protection.

NETWORK BASED DEFENSES

Pros

- Detection and blocking of threats in real-time
- Protection from malware downloaded via the web
- Blocking of malicious websites

Cons

- No protection for users working off the network
- No inspection of SMTP traffic
- No forensic data on threats

Secure web gateway and SSL network proxy

If you have already gone through the work of baselining your environment to deploy inline IPS protections, you may be looking at adding a secure web gateway (SWG) or an SSL network proxy. These technologies enable the inspection of encrypted web traffic and can actively block employees from visiting malicious websites.

But these preventative efforts are limited. For one, they can't detect and block malware in SMTP traffic. And in the case with network based IPS deployments, it does not detect and block threats when employees are working off the network.

Heuristic detection

Heuristic technologies are another way security teams attempt to combat advanced threats and targeted attacks. Often they are deployed to complement network and endpoint signature-based defenses. Heuristic scanning is often included with signature-based defenses in IPS, NGFWs and endpoint behavioral analysis solutions. Heuristic scanning uses rules not signatures to look for malicious commands, behaviors, and anomalies in network traffic. By using rules, not specific signatures, it can catch new variants of malware that exhibit similar behavior to known malware.

Heuristics will catch more malware than signature-based defenses, but it usually produces more false-positives. A key difference to consider between heuristic detection solutions and signature-based solutions is that heuristics does not detonate malware or use specific signatures, so it does not provide useful forensic information on attacks.

As with all network or endpoint-driven strategies, adding a heuristic based analysis does not protect employees from malicious websites and downloads off the network. And unless heuristic scanning is deployed at the email gateway, it does not block malicious attachments and URLs delivered by email.

Network Sandbox Solutions

Sandbox analysis is another technology deployed at the network perimeter to complement a NGFW, IPS, or a SWG system. It provides a self-contained environment—virtual, physical, or cloud-based—to run suspect code and observe its behavior.

The ideal sandbox analysis tool also inspects URLs that lead to malicious websites and downloads. Once the system verifies a threat, it can block the URL using inline protections of an NGFW, IPS or SWG.

Sandboxing does not rely on rules or signatures. Instead, it extracts rich forensic information as it analyses malicious URLs and code. This information helps enrich threat intelligence so that new forms or malware are more easily recognised.

Where you deploy your sandbox determines how effective it is. When deployed with a NGFW, it mainly provides file-based analysis but is less able to analyse web objects such as JavaScript and HTML. Sandbox analysis also can slow network performance and throughput. To avoid this hit, many security teams limit analysis to only header information. Sandboxing at the SWG has similar problems; it cannot process huge volumes of suspicious web objects without slowing overall network performance.

Network-deployed sandboxing has other limitations. First, it is not built to inspect SMTP email traffic. And any protection it offers for malware and weaponised files does not extend to employees' off-network interactions.

ENDPOINT SECURITY INVESTMENTS

New security capabilities via endpoint detection and response is the next bright and shiny silver bullet promising to bring order to chaos when threats bypass network security controls.

Security teams looking to invest in next generation endpoint solutions find themselves wadding through a plethora of data telling you that no matter what you do, the threats will get through, so you better be equipped to detect and respond. This notion has a grain of truth. And with roughly 20% of the security budget dedicated to the endpoint, security vendors have aggressively responded with next-generation endpoint solutions. Popular solutions include endpoint protection platforms (EPP) and endpoint detection and response (EDR) systems.

These tools promise to give security teams more visibility into potentially malicious processes on endpoints. And they're supposed to help teams respond to them faster using automation and endpoint tracking. Malware analysis features can include:

- Pre-execution prevention
- Micro virtual machines that act as a one-sample sandbox on the endpoint
- Behavioral detection methods
- Cloud-based malware analysis

These are improvements. But in all cases, the endpoint solution still blocks malware only when the malicious programme tries to load into memory—after it is already active on the endpoint. The malware may spread through email and other channels until it can execute on an endpoint and then it may be recognised as malicious.

This post-execution detection may seem good enough. But it does not prevent malware from getting into your environment in the first place. Even if a malicious process is blocked, you still need to clean-up residual traces. Malware artifacts may include LNK files, cookies, temporary files, steganography images, malware-linked executables, keyloggers, and so on.

While some solutions have automated capabilities to help clean up malware artifacts after the fact, they require bulky agents to manage and keep up to date. It's no wonder that 67.5% of IT pros don't want a corporate agent on their personal device.[9]

Endpoint security can help reduce your attack surface. As with network security, endpoint controls will prevent some attacks and block some malware by isolated infected endpoints.

But, you need to ask yourself, how effective are these solutions at preventing a credential phishing attack or a new strain of malware from getting inside your company in the first place? Do these approaches prevent users from clicking on a link or attachment and infecting themselves?

[8] Verizon. "2016 Data Breach Investigations Report." April, 2016
[9] Cloud Security Alliance. IT Security in the Age of Cloud Survey Report, October, 2016

EMAIL SECURITY INVESTMENTS

Anti-virus, spam reputation services, email classifiers, and mail routing capabilities are an important part of managing your email. But they cannot protect against malicious links and attachments, zero-day threats, ransomware, polymorphic malware and credential phishing attacks.

Email is by far the most popular way for attackers to distribute malware, and social engineering is the top method used to entice users to click. A well-crafted email to the right recipient in your organisation can cause a user to click, infecting a device or exposing account credentials. Social engineering gets employees to, in effect, do the work of keyloggers, information stealers, and other automated malware.

MORE THAN 90% OF TARGETED ATTACKS ARE LAUNCHED THROUGH EMAIL, EXPLOITING THE WEAKEST LINK IN THE SECURITY CHAIN: PEOPLE. NEARLY A THIRD OF PEOPLE WHO RECEIVE A MALICIOUS EMAIL OPEN IT—ON OR OFF THE NETWORK. AND ABOUT 12% CLICK THE MALICIOUS ATTACHMENT OR LINK.[10]

The only way to prevent these attacks is by deploying advanced protection at the email gateway. It should provide protection that goes beyond AV and filtering. Signature- and heuristic-based solutions can protect your company from only known forms of malware. Given how quickly attackers create new malware, that's not enough to protect your organisation.

An effective approach uses sandbox analysis at the email gateway to inspect the full attack chain with a combination of static and dynamic techniques. Cloud-based sandbox solutions enable you to detect and block the newest forms of malware and attack campaigns.

A cloud-based analysis environment is constantly updating and adapting to detect new attack tools, tactics and targets. And email is the most effective and strategic place you can aim sandbox analysis. At the gateway, it can and stop attacks before they reach the network or your employees.

Besides being able to scale to handle large influxes of email traffic, cloud-based analysis is able to extract detailed intelligence from attacks. Paired with a cloud–based threat intel platform, organisations can quickly connect the dots of an attack. They can correlate intelligence about patterns, behaviors and tradecraft used in each attack. With this insight, your defenses can adapt to better detect future attacks.

FLIPPING THE SCRIPT ON THE 8%

Taking a closer look at email's 8% share of security budgets illustrates the disparity between security spending and the vectors used to target organisations and privileged users.

Why does advanced protection in the No. 1 attack vector receive so little attention and security budget? Causes include organisational silos, hype over new malware variants, and security tools that use the majority of a security budget but are never fully deployed or ultimately are scrapped.

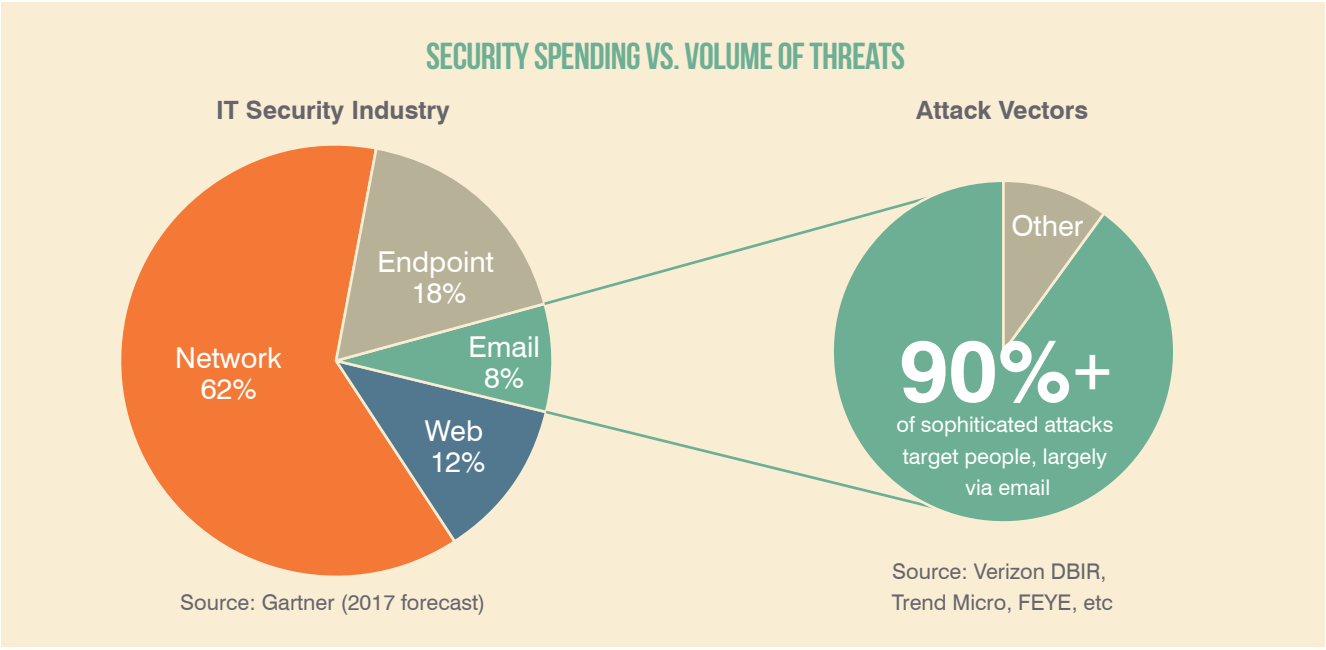
Dynamics that can pull security teams away from considering advanced protections within the flow of email include:

IT silos
When the messaging works separately from the security group, there are too competing priorities that make it difficult to implement security controls in the flow of email.

The belief that traditional AV and email filtering is "good enough" when used in with network and endpoint security solutions can prevent the search for a more effective solution.

Malware Hype
The hype surrounding new malware bypassing network security controls has reached epic levels. It can paralyse security teams from seeking out new ways to approach preventing the problem in the first place. Instead, security teams are relegated to reactive solutions that keeps them doing what they always did before.

[10] Verizon. "2016 Data Breach Investigations Report." April, 2016.



RECOMMENDATIONS

Security teams have many potential approaches to cloud-based sandbox analysis for email gateways. Not all vendors operate with the same level of threat intelligence or infrastructure. We recommend evaluating sandbox analysis solutions that have these key capabilities:

Scale
You need cloud-based analysis that can accommodate the ebb and flow of corporate mail volume. Your solution should be able to scale, offering for extra capacity when needed.

Automation
An effective solution automatically analyses attachments and URLs rather than waiting on someone to manually submit them. It should also manage and update the sandbox automatically to lift the burden from IT administrators. Automated updates shouldn't require restarting security services.

Forensics
Knowing that something was blocked is not enough. Security teams need real-time information on campaigns and targeted attacks aimed at their company.

Look for a management interface built for security teams, not for Microsoft Exchange admins or messaging crew. Without detail on threats, prioritising your response is impossible. At a minimum, a dashboard for security team should organise threat data in coordination with information on targeted people or systems. A dashboard view should enable security teams to answer these questions in real-time:

- Is this a broad campaign or targeted attack aimed specifically the company?
- Are executives and other high-value employees being singled out?
- Who is behind the attack? Where else has this attack been seen? What infrastructure is being used in the campaign or targeted attack?

URL and Attachment Inspection
Analysis capabilities for attachments and URLs are essential. Protection must extend from the time the email is delivered to time it is actually clicked; a seemingly benign website can go bad or be compromised later.

Threat Intelligence
Subscribing to one or more threat services is not enough to detect new malware. Look for a platform that has rich extraction services that can derive as much intelligence as possible from attacks. Ideally, it should correlate all aspects of attacker tradecraft and reputation— not just IP addresses and domains and use the details to learn from each new attack to better detect future attacks.

GET STARTED TODAY WITH A FREE THREAT ASSESSMENT

Learn more about the risks you may not be seeing by scheduling a free threat assessment from Proofpoint. Our simple, non-invasive process will help you assess your security posture. You'll get a clear picture of threats and vulnerabilities in your environment.

EMAIL

Our email risk assessment shows you who is being targeted and how (though ransomware, credential phishing, BEC, and more).

MOBILE

Our mobile defense risk assessment shows you what mobile applications your users have on their phones and what each of those apps is doing.

SOCIAL

Our social risk assessment provides a snapshot of all accounts associated with your brands. You'll see corporate, unauthorised and fraudulent accounts.

DATA DISCOVER

A Data Discover risk assessment shows you where sensitive data lives within your environment.

To schedule an assessment, visit proofpoint.com/us/cybersecurity-assessment

ABOUT PROOFPOINT TARGETED ATTACK PROTECTION (TAP)

Proofpoint Targeted Attack Protection (TAP) helps detect, analyse and block advanced threats that target people through email. Our solution protects users on any network or device, regardless of where and how they check their email.

We detect known and new, never-before seen attacks that use malicious attachments and URLs to install malware on a device or trick users to share their passwords or other sensitive information. TAP is unmatched in stopping targeted attacks. These include attacks that use ransomware, polymorphic malware, weaponised documents and credential phishing to access sensitive information or steal money.

Proofpoint TAP is easily configured as add-on modules to the Proofpoint email security platform. It can be deployed as a cloud service, virtual appliance or hardware appliance.

[1] footnote goes here

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.