The Hidden Costs of Detect-to-Protect Security
Executive summary

Today, large enterprise organizations spend an average of $16.7 million every year on security tools and people power to manage cybersecurity, detect threats and prevent data loss. But it simply isn’t working; if anything, the problem is getting worse. Research shows that cybercrime damages will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015\(^1\).

Mobile and cloud have changed how we do business, yet our approach to security remains unchanged. The perimeter has shifted from the network, to the endpoint and ultimately to the application. Combined with soaring volumes of phishing attacks, ransomware, Trojans, APTs, and more, this has helped to create what SANS Institute describes as a “perfect storm”\(^2\), threatening to compromise key data, IP, and systems on an ever-growing scale.

Even as threats grow increasingly sophisticated, and the number of endpoints and applications multiply, we continue to rely on detect-to-protect tools focused on detection techniques. The continued failure of this approach is validated by the fact that breaches continue to rise. Risk Based Security’s Annual Data Breach QuickView Report\(^3\) showed there were 4,149 data breaches reported during 2016, exposing over 4.2 billion records—the highest number on record.

This independent research uncovered the surging hidden costs of reactive detection-based security. The initial, upfront investment in security tools and licenses is dwarfed by the cost of human labor needed to manage the millions of alerts generated by those same tools.

This report provides business and security leaders with a better understanding of the total costs of ownership for detection-based security. It is designed to assist CIOs and CISOs with building a business case for change; going beyond IT service deployment to operational scalability and long-term business growth, by exposing the reality of detect-to-protect security.

About the research

This research is based on a survey of 500 CISOs from large enterprises across the USA (200), UK (200) and Germany (100), at organizations sized from 1,000 to 5,000+ employees. The research was carried out by Vanson Bourne, an independent market research organization.

---

\(^1\) Cybersecurity Ventures 2017 Cybercrime Report
\(^2\) Exploits at the Endpoint: SANS 2016 Threat Landscape Survey
\(^3\) Risk Based Security Annual Data Breach QuickView Report 2017
Introduction

Attackers see applications—in particular, email and browsers—as a favorite target, because they present the best chance of tricking users into helping bypass corporate defenses.

Current tools are not working. In 2017, we saw a steady stream of major data breach incidents—such as Equifax and Deloitte—with huge implications for consumers, and potentially even national security.

The WannaCry and NotPetya ransomware campaigns showed us that cyber-threats are not all about data theft. WannaCry infected more than 250,000 endpoints in 150 countries in a matter of hours, causing scores of National Health Service (NHS) Trusts in the UK to cancel patients’ operations and appointments.

NotPetya is still being felt even by large multi-national companies, with Danish shipper Maersk and FedEx both revealing losses of up to $300 million apiece.

The impact of these security incidents extends way beyond direct financial costs such as industry fines, legal bills and falling share prices. Brand and reputational damage can have a much longer-lasting and serious impact on customer attrition.

Reported incidents are likely to be just the tip of the iceberg, given that many info-stealing attacks slip quietly past defenses without raising the alarm. Research shows the median number of days that attackers stay dormant within a network before detection is more than 200. This tells us something very important: detect-to-protect solutions are falling at the first hurdle and can’t hope to provide effective threat defense.

According to SANS, hackers most commonly gain entry to endpoint devices in the following ways:

- **75% of identified, impactful threats initially entered via email attachment**
- **46% of attacks were executed by users clicking web links in email**

---

1. Exploits at the Endpoint: SANS 2016 Threat Landscape Survey
2. BBC News: Ransomware cyber-attack threat escalating – Europol
3. ZDNet: Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk
4. The Register: FedEx: TNT NotPetya infection blew a $300m hole in our numbers
5. M-Trends® 2015: A View from the Front Lines
The human cost: $16 million annually

Detection tools are drowning security teams in alerts. Every cybersecurity system—endpoint and network threat detection, anti-virus, intrusion detection systems, firewalls, etc.—unleashes a flood of alerts that must be addressed daily. However, 70% of these alerts are false positives. Our research found that the average security operations center (SOC) receives 4,146 alerts every single day, but more than 2,900 of these are actually false positives (fig. 1).

70% of security alerts are false positives

SOC teams must investigate each and every alert to determine which are legitimate, then determine what triggered the alert. Because detection tools do not allow malware to fully execute, SOC teams must piece attacks together retrospectively; working backwards to try and understand how a hacker gained entry, what they did once they had access, and what actions they took. It’s often impossible to understand the nature of an alert until it has been triaged and checked, making this an inefficient and time-consuming task for overstretched teams.

Alert fatigue setting in….

Nearly two-thirds (63%) of CISOs said they were concerned their SOC teams may be getting alert fatigue. This can have a serious impact on organizations: the security team at US retailer Target reportedly missed a crucial alert that could have saved the company hundreds of millions of dollars in breach costs, because they were drowning in this kind of data.

© Bromium, Inc. 2018
How time consuming? Well, on average SOC teams triage 796 alerts per week, taking an average of 10 hours per alert—that's 413,920 hours across the year. When you consider that the average hourly rate for a cybersecurity professional is $39.24, that's an annual average cost of more than $16 million each year (fig. 2).

Organizations spend $16 million per year triaging alerts

Detect-to-protect security tools often only detect threats after the fact, when the endpoint is owned. So after triage, organizations spend even more hours rebuilding compromised devices.

On average, organizations rebuild 51 devices every month, with each taking four hours to rebuild—equating to 2,448 hours each year. When multiplied by the average hourly wage of a cybersecurity professional, $39.24, that's an average cost of $96,059 per year (fig. 3).

Figure 2: Organizations spend $16 million per year triaging alerts.

Cybersecurity skills will be hard to hire

Research suggests there will be 3.5 million unfilled cybersecurity positions by 2021. This skills shortage is likely to impact costs and increase pressure on understaffed teams.

Cybersecurity Ventures: Cybersecurity Jobs Report

$16,242,220.80 is calculated as follows: the hourly rate for a cybersecurity professional is $39.24. This was then multiplied by 796, the number of threats triaged per week. The result was multiplied by the 10 hours spent triaging each threat on average, and then multiplied by the 52 weeks in a year.

$96,059 is calculated as follows: The hourly rate for a cybersecurity professional is $39.24. This was multiplied by the 2,448 hours.
Organizations spend $96,000+ rebuilding 600+ devices per year.

![Bar chart showing costs in different regions](image)

**Patch-to-protect giving CISOs a headache**

More than half (53%) of CISOs say crisis patch management is a major disruption to their teams.

**According to some estimates**, 15,000 vulnerabilities were disclosed in 2016.

Emergency patching is another cause of the detect-to-protect time drain. According to some estimates, 15,000 vulnerabilities were disclosed in 2016. Each patch must be tested prior to implementation in mission-critical environments. By itself, this is a significant challenge for IT departments.

Yet increasingly, major vendors—including the likes of Microsoft, Adobe and Oracle—are forcing businesses to break their regular patching cycles by issuing emergency fixes on top of regular patches; such as the Windows SMB server update for legacy OS versions issued in response to WannaCry, and the 2018 emergency patch issued by Microsoft to correct the Intel chip vulnerability.

---

**Fig. 3**

[Risk Based Security’s 2016 Year End Vulnerability Quick View Report](#)
Our research showed that enterprises issue emergency patches five times per month on average, with each fix taking 13 hours to deploy. That’s 780 hours a year, which—multiplied by the $39.24 average hourly rate for a cybersecurity professional—incurs costs of $30,607 per year (fig. 4).

**Emergency patching costs $30,000+ per year**

![Bar chart showing patching costs](chart)

Fig. 4

Added to this, our research shows that more than half of CISOs pay overtime, or bring in a third-party response team, to issue patches or fight a security issue. They estimate the cost at $19,908 per patch (fig. 5).

**$19,900+ per patch for 3rd-party expertise and overtime pay**

![Bar chart showing patch costs](chart)

Fig. 5

---

13$30,607 is calculated as follows: the hourly rate for a cybersecurity professional is $39.24. This was then multiplied by the five patches per month, and then multiplied by the 12 months of the year. The result was multiplied by the 13 hours per patch.

14CISOs surveyed, estimate that the average cost per patch of overtime and third party resources was $19,908.
Organizations are spending a large amount of money and time to manage alerts, triage security events, rebuild compromised machines, and patch on the fly. Excluding the cost of using third parties or overtime, each year this equates to:

- $16,242,220 to triage threats
- $96,059 to rebuild compromised devices
- $30,607 to issues emergency patches

That’s a **total spend of $16,368,886 every year** (fig. 6).

**Over $16 million: the average combined cost of triaging threats, rebuilding compromised machines and issuing emergency patches**

---

**Top Tips**

It doesn’t have to be this way. With a fresh approach, you can eliminate false positives, reduce alerts and rebuild rates, and ease the burden of emergency patch management:

- Isolate applications within virtualized environments, rendering malware harmless
- Allow malware to fully execute to track the full kill chain
- Produce high fidelity alerts so that SOC teams only receive real threats
- Deliver forensics in real-time and sharing threat intelligence to protect the enterprise at large
- Protect at the point of infection, so that machines do not get owned
- Do not rely on patch-to-protect, so emergency patches can be updated within regular patch cycles
The Technology Burden: $345,300 per year

Advanced Threat Protection (ATP) and prevention solutions, used by 92% of respondents, still typically rely on the detect-to-protect approach. These tools largely uncover threats by identifying indicators of compromise, applying behavioral analysis and increasingly using Machine Learning (ML) or Artificial Intelligence (AI). Essentially, if something seems unusual then an alert will be created.

This approach relies on the system being able to determine what is and what isn’t normal behavior—and hackers know this. As a result, many forms of malware will delay execution, so that the host application or document appears to be innocuous; that is until the monitoring tool moves on. This means that such systems often miss malware or can be fooled into believing it is benign.

Organizations spend an average of $79.61 per user each year for ATP tools. For an average 2,000-person organization, this equates to an annual spend\textsuperscript{15} of $159,220 (fig. 7).

Nearly $160,000 is spent per year on ATP

\textsuperscript{15}$159,220 is calculated as follows: The average spend on advanced endpoint detection solutions per user is $79.61 per year according to data from Vanson Bourne. This was then multiplied by the average number of employees (2,000) in a large organization.
Nearly all respondents, 98%, have invested in traditional or next-gen anti-virus solutions. Although this is useful for stopping commodity malware and the most elementary attack types, it’s too basic to spot or block advanced threats, such as those featuring polymorphic techniques, which are becoming increasingly common.

Businesses spend an average of $22.10 per user, each year, on anti-virus—that’s an average annual cost of $44,200\(^{16}\) for a 2,000-person organization (fig. 8).

### $44,000 for next-generation or traditional anti-virus

If you’re detecting ransomware, it’s already too late

Ransomware is in the headlines a lot. In fact, reports\(^{16}\) show the number of ransomware attacks targeting businesses tripled last year.

Detecting ransomware after the fact means you’ve already been owned. It’s too late and there is no way to turn back the clock.

---

\(^{16}\)Kaspersky Security Bulletin 2016. The ransomware revolution

\(^{17}\)$44,200 is calculated as follows: The average spend on Next Gen or traditional AV per user is $22.10 per year according to data from Vanson Bourne. This was then multiplied by the average number of employees (2,000) in a large organization.
A similarly large number, 92%, said they use a whitelisting or blacklisting endpoint security solution. Whitelists require a significant investment of time to develop and can often lead to usability issues if legitimate apps and executables are blocked. On the other hand, blacklists are only as strong as the list they’re based on, which means they can only block known threats. With each solution costing an average of $14.77 per user, per year; that’s an average annual cost of $29,540 for an average 2,000-person organization (fig.9).

**Nearly $30,000 is spent on whitelisting or blacklisting**

---

Fig. 9

**Defense against advanced threats—leave your AV at the door**

AV, blacklisting and whitelisting largely rely on businesses knowing what is coming. They are signature-based, and useful in filtering out known threats. Yet in today’s security climate, this is not enough.

Research\(^\text{19}\) shows that in Q3 2016 alone, 18 million new malware samples were captured. That’s an average of 200,000 per day. As these threats have never been seen, there is no way that these tools can detect them.

Application isolation and containment protects against the unknown, as all activity takes place in a micro-VM, separated from the rest of the device and network. This means that if a user is hit with polymorphic malware or a Zero-Day attack, then it cannot cause any damage.

\(^\text{19}\)$29,540 is calculated as follows: The average spend on whitelisting or blacklisting endpoint protection solutions per user is $14.77 per year according to data from Vanson Bourne. This was then multiplied by the average number of employees (2,000) in a large organization.

\(^\text{19}\)Panda Security report: Cybercrime Reaches New Heights
Around 75% of respondents claimed they’re planning to create a separate detonation infrastructure, so that risky-looking links can be checked in a safe and isolated environment. This approach requires each link to be checked, and can be costly. CISOs have spent, or intend to spend, on average $56.17 per user, per year. When deployed across all users in a 2,000-person organization, this would cost\(^2\) an average of $112,340 per year (fig. 10).

$112,000+ is spent annually on detonation environments

While it is advisable to have layered defenses, and security investment is vital, the costs are mounting up:

- $159,220 on advanced threat detection and prevention
- $44,200 on AV (including next gen)
- $29,540 on whitelisting/blacklisting
- $112,340 on detonation environments

\(^2\)S112,340 is calculated as follows: The average spend on detonation environment per user is $56.17 per year according to data from Vanson Bourne. This was then multiplied by the average number of employees (2,000) in a large organization.
That’s a whopping $345,300 each year for detection-based security tools. When added to the $16,368,886 in indirect costs\(^{21}\) outlined in the first section, companies are spending an average of $16,714,186 every year (fig. 11).

**Over $16.7 million: the total cost of detect-to-protect for a large, global enterprise**

![Bar chart showing the total cost of detect-to-protect for a large, global enterprise.](image)

**Make smarter investment choices**

Security is vital to business health and operations. But it is equally important that money spent does make the business more secure. As such, IT leaders need to calculate the total cost of ownership of security solutions before making choices, asking questions like:

- Where are most of the attacks happening?
- Are advanced threats getting through current defenses?
- Is employee productivity negatively impacted by current security measures?
- How many alerts are being generated? Of those, how many are false positives?
- Is it likely that machines will still get compromised and need to be rebuilt?

\(^{21}\)$16,369,728 is calculated as follows: The average cost of $16,242,314 for triaging alerts (footnote 1), added to average cost of $96,807 for rebuilds (footnote 2), added to average cost of $30,607 for emergency patching.
Conclusion

Detect-to-protect has been the de facto standard in security for close to two decades—at a huge cost to organizations. Major data breaches, ransomware-related outages, and other cyber incidents show no signs of stopping. Despite bold promises around the power of AI and behavioral analysis, hackers keep getting through.

As businesses consider the changing threat landscape, accurately understanding the costs of your detect-to-protect security will help you counterbalance the value of protecting against malware. With a full understanding of the total cost of detection-based security, you can make smart, sustainable business decisions.

Organizations of all sizes, across all industries, are moving away from detection and are now protecting their assets with application isolation and control. With application isolation, end users perform untrusted tasks—anything that could be ingress points for malware—in an isolated environment. If malware is present, it completely plays out in the isolated environment, with no access to the protected host operating system. It’s the classic “honey pot” scenario, where malware believes it’s fully running and executing, yet only damaging a disposable environment.

With application isolation and control:

- False-positive detections no longer require the expenditure of scarce resources to track down
- False negatives (missed detections) cause no harm because the threats are isolated
- Endpoint remediation and reimaging due to malware infections become practically non-existent
- Security patching for applications and operating systems can be planned, eliminating crisis patching
- Separate detonation environments are no longer needed

Combined, these help businesses to drastically reduce the cost of cybersecurity, while also ensuring systems and data are protected.
Protect before you detect with Bromium

Bromium protects your brand, data and people using virtualization-based security. We convert an enterprise’s largest liability—endpoints and servers—into its best defense. By combining our patented hardware-enforced containerization to deliver application isolation and control, with a distributed Sensor Network to protect across all major threat vectors and attack types, we stop malware in its tracks.

Unlike traditional security technologies, Bromium automatically isolates threats and adapts to new attacks using behavioral analysis and instantly shares threat intelligence to eliminate the impact of malware. Bromium offers defense-grade security and counts a rapidly growing set of Fortune 500 companies and government agencies as customers.

Contact Bromium for more information about how application isolation and control can help you protect before you detect, and turn around your approach to security.

- Visit our website: Bromium.com
- Speak to a solutions expert: https://learn.bromium.com/contact-us.html

ABOUT BROMIUM

Bromium has transformed endpoint security with its revolutionary isolation technology to defeat cyber attacks. Unlike antivirus or other detection-based defenses, which can’t stop modern attacks, Bromium uses micro-virtualization to keep users secure while delivering significant cost savings by reducing and even eliminating false alerts, urgent patching, and remediation—transforming the traditional security life cycle.