Report

Bromium: Endpoint Protection Attitudes & Trends 2015

Increasing Concerns Around Securing End Users

Bromium®

Table of Contents

AUTHOR

Clinton Karr

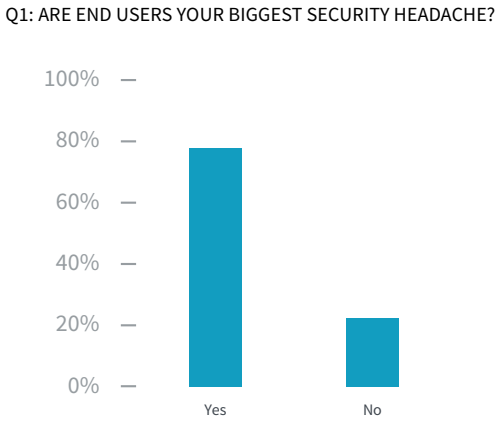
Introduction

"NOT ONLY DO AN OVERWHELMING NUMBER OF INFORMATION SECURITY PROFESSIONALS BELIEVE THAT END USERS ARE THEIR BIGGEST SECURITY HEADACHE, BUT THE NUMBER HAS ACTUALLY BEEN INCREASING OVER TIME."

In January 2015, Bromium conducted a survey of more than 100 information security professionals, focused on the greatest challenges and risks facing their organizations today. The results indicate that end users continue to remain the greatest security risk, thanks to their tendency to click on suspicious and malicious e-mail and URLs. Additionally, the survey highlights the operational challenges information security professionals face as they struggle to manage multiple point solutions, to respond to the security alerts generated by their users on a daily basis, and to detect and remediate compromised endpoints.

End Users Remain Greatest Security Risk

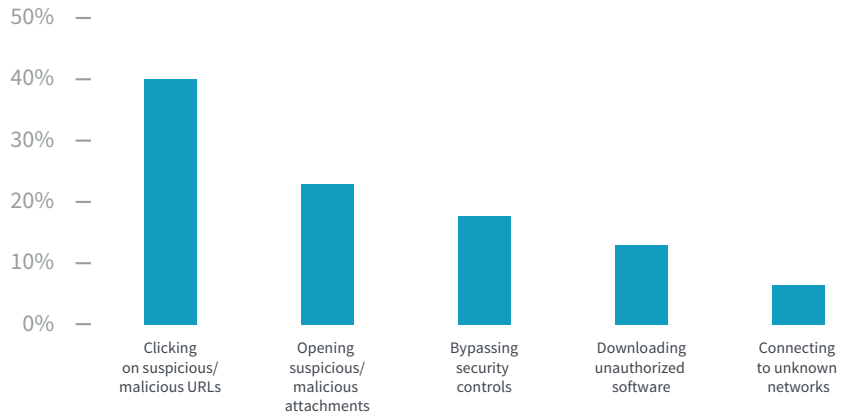
Bromium published similar research in June 2014, which determined that 72 percent of information security professionals believe end users are their biggest security headache. Today, 79 percent of information security professionals believe that end users are their biggest security headache.



"CLICKING ON SUSPICIOUS AND MALICIOUS URLS AND E-MAILS CONTRIBUTES TO THE MAJORITY OF SECURITY RISK (63 PERCENT)."

We can see from these results that not only do an overwhelming number of information security professionals believe that end users are their biggest security headache, but the number has actually been increasing over time. Why is it end users are the biggest security headache for so many information security professionals?

Q2: WHICH OF THE FOLLOWING END-USER BEHAVIORS IS THE SOURCE OF THE MOST SECURITY RISK?



From these results, we can see that information security professionals believe that clicking on suspicious and malicious URLs is the end-user behavior that introduces the most security risk (40 percent). Additionally, information security professionals believe that opening suspicious and malicious attachments is the end-user behavior that introduces the second most security risk (23 percent). Together, these behaviors contribute to the majority of security risk (63 percent).

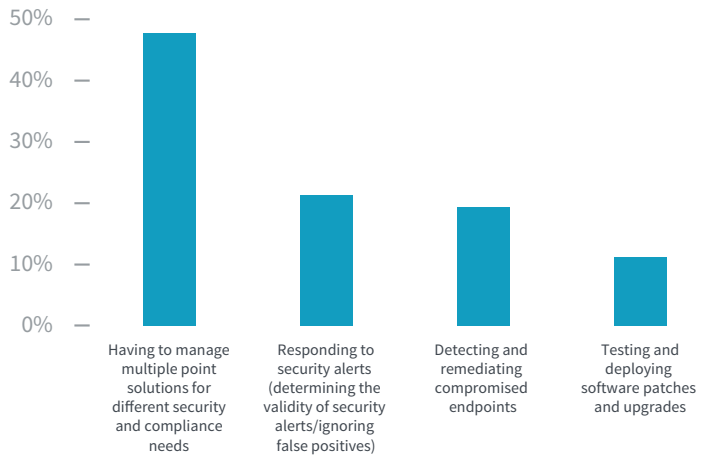
These results should come as no surprise because it has become so trivial for a determined attacker to circumvent detection-based solutions, such as antivirus, application white listing, or malicious behavioral blocking. Previous Bromium research indicates that more than 80 percent of information security professionals do not believe their existing endpoint protection can prevent all infections, APTs or spear phishing. We will explore this sentiment in more depth later in this report.

Secondarily, bypassing security controls is the major source of risk for 17 percent of information security professionals, downloading unauthorized software is the major source of risk for 12 percent of information security professionals, and connecting to unknown networks is the source of security risk for 6 percent of security professionals. Therefore, we may conclude that many organizations are grappling to maintain control over its users.

Operational Impact of Security

In addition to struggling to maintain control over their users, many information security professionals are struggling to maintain control over their current security systems. In this survey, Bromium sought to determine the greatest operational challenges facing information security professionals and the impact of security alerts generated by detection-based security solutions.

Q3: WHICH OF THE FOLLOWING CHALLENGES INTRODUCES THE MOST COST AND COMPLEXITY INTO YOUR SECURITY PROGRAM?



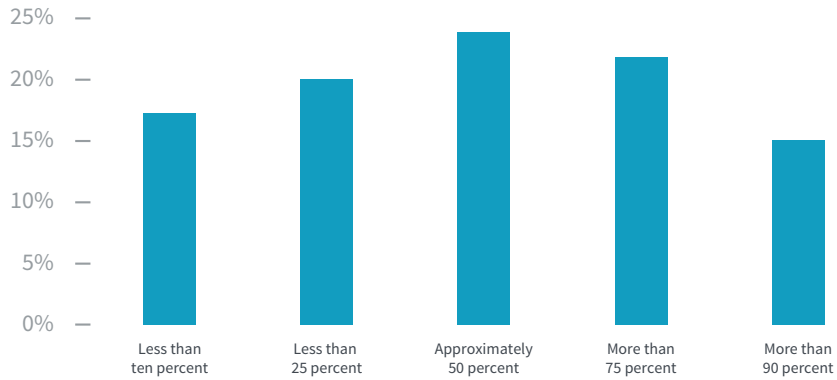
It may seem obvious, but nearly 48 percent of information security professionals believe that having to manage multiple point solutions, many of which are redundant, introduces the most cost and complexity into their security. Logically, more solutions cost more money and take more time to manage. Unfortunately, previous Bromium research has demonstrated that deploying multiple solutions—a "defense-in-depth" architecture—may still leave organizations vulnerable to attack if they are based on the same foundation of traditional pattern-matching or detection.

However, one conclusion we may draw from these responses is that information security professionals could reduce the cost and complexity of their information security programs by reducing the number of point solutions they have to manage by considering new ways to automate or eliminate time-consuming processes, such as responding to security alerts, detecting and remediating endpoints, and testing and deploying urgent patches.

"ONLY 15 PERCENT OF ORGANIZATIONS INVESTIGATE OR RESPOND TO 90 PERCENT OR MORE OF THEIR SECURITY ALERTS."

In fact, approximately 20 percent of information security professionals believe that responding to security alerts introduces the most cost and complexity into their security program, while an additional 20 percent believe it is detecting and remediating compromised endpoints. The results suggest that reacting to manual processes that emerge from managing detection-based solutions, such as antivirus or intrusion detection, is the source of considerable frustration for a significant number of information security professionals. As the next questions demonstrate, some information security professionals have given up on keeping up with security alerts.

Q4: WHAT PERCENTAGE OF SECURITY ALERTS IS YOUR ORGANIZATION ABLE TO INVESTIGATE AND/OR RESPOND TO?

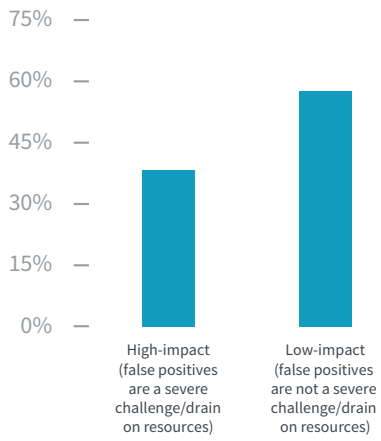


When we asked information security professionals what percentage of security alerts their organization is able to investigate and respond to, the results were returned as a normal distribution—or a bell curve. However, a closer analysis reveals an alarming response: 62 percent of organizations investigate or respond to 50 percent or less of their security alerts, and only 15 percent of organizations investigate or respond to 90 percent or more of their security alerts.

This represents a huge security gap. What is the value of a security alert if information security professionals are not taking the time to investigate and respond to them? Just ask Target. There is no value! Detection is worthless without action, yet the overwhelming majority of information security professionals are unable to respond to all of their security alerts.

"EACH EMPLOYEE GENERATES 4.5 SECURITY ALERTS EACH MONTH—MORE THAN ONE EACH WEEK."

Q5: WHAT IS THE IMPACT OF "FALSE POSITIVE" SECURITY ALERTS ON YOUR ORGANIZATION'S RESOURCES?



One surprising result is that only 41 percent of organizations believe that false positives are a severe challenge or drain on resources—although this may be less surprising when we consider that 62 percent of organizations respond to 50 percent or less of their security alerts.

Additionally, Bromium asked each information security professional how many employees were in their organization, and separately asked how many security alerts their organization generates each month to determine how many security alerts each employee generates each month, on average. The result is that each employee generates 4.5 security alerts each month—more than one each week.

Waning Confidence in Legacy Security Solutions

One of the most interesting and most telling questions explores the confidence information security professionals have in various security solutions for their ability to prevent zero-day and advanced targeted attacks.

Q6: FOR EACH OF THE FOLLOWING SOLUTIONS, HOW CONFIDENT ARE YOU IN ITS ABILITY TO PREVENT ZERO-DAY AND ADVANCED TARGETED ATTACKS?

	NOT CONFIDENT	UNSURE OF CAPABILITIES	CONFIDENT	TOTAL	WEIGHTED AVERAGE
Firewall	**43.38%** 59	**19.85%** 27	**36.76%** 50	136	1.93
IDS/IPS (Intrusion Detection/ Prevention Systems)	**28.47%** 39	**33.58%** 46	**37.96%** 52	137	2.09
SWG (Secure Web Gateway)	**28.57%** 38	**40.60%** 54	**30.83%** 41	133	2.02
AV (Antivirus)	**51.45%** 71	**16.67%** 23	**31.88%** 44	138	1.80
NGFW (Next-generation Firewall)	**19.40%** 26	**43.28%** 58	**37.31%** 50	134	2.18
Advanced Threat Protection Appliances	**14.18%** 19	**46.27%** 62	**39.55%** 53	134	2.25

It should not be surprising that the majority of information security professionals are not confident in antivirus solutions (51 percent). Similarly, 43 percent of information security professionals are not confident in firewalls. This demonstrates that information security professionals have lost faith in traditional/legacy information security solutions.

Interestingly, there are no information security solutions that truly instill confidence in information security professionals. While only 37 percent of information security professionals are confident in firewalls, information security professionals are only slightly more confident in next-generation firewalls (37.31 percent) and advanced threat protection appliances (39.55 percent). In fact, more information security professionals responded that they were unsure of the capabilities of secure Web gateways, next-generation firewalls, and advanced threat protection appliances than they were confident.

Conclusion

Information security professionals have lost faith in the traditional approaches to securing the network and the endpoint, yet are unaware of the capabilities of the emerging breeds of next-generation solutions. Simultaneously, information security professionals are overwhelmed managing multiple point solutions, responding to security alerts, and remediating compromised endpoints. Traditional solutions are simply not working, so a new approach is needed.

It is a challenging time for information security professionals because the traditional security model has been unable to scale with the volume of transactions generated by the modern enterprise. For some organizations, its information security program has become a big data problem, always a step behind, always reacting to a new threat or a new alert.

One issue that almost all information security professionals can agree on: end users are their biggest security headache because of their tendency to click on suspicious and malicious URLs and e-mail attachments.

Moving forward, information security professionals should seek proactive protection for the endpoint that eliminates the tedious manual processes that introduce cost and complexity into their information security programs: responding to security alerts, remediating endpoints, and patch management.

One approach is isolation, such as the micro-virtualization delivered by Bromium vSentry. By isolating user tasks in disposable micro virtual machines, Bromium enables a dynamic security model that prevents malware from establishing persistence, eliminating the need for detection, response, and remediation.

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.

Bromium, Inc.
20813 Stevens Creek Blvd
Cupertino, CA 95014
info@bromium.com
+1.408.213.5668

Bromium UK Ltd.
Lockton House
2nd Floor, Clarendon Road
Cambridge CB2 8FH
+44.1223.314914

For more information go to www.bromium.com
or contact sales@bromium.com

RPT.SurveyReport.US-EN.1510