Survey: Endpoint Security Concerns 2014

The issues keeping IT admins awake into the New Year

Intro

2014 has created uncertainty for those in charge of IT security. Not only is the threat landscape advancing at a fast pace, leaving traditional antivirus behind, but high-profile breaches have put data security firmly on the map in the boardroom. Previously, this would have been a problem resolved by deploying a single vendor who promised a catch-all solution. However, in today's world of advanced malware, zero-day exploits and endless data breaches, what's on the minds of those tasked with IT security?

Overview

The research interviewed 685 IT decision makers at businesses in a range of sectors. To reflect the non-discriminatory nature of threats, companies of all sizes were surveyed[1].

The objectives of the research were:

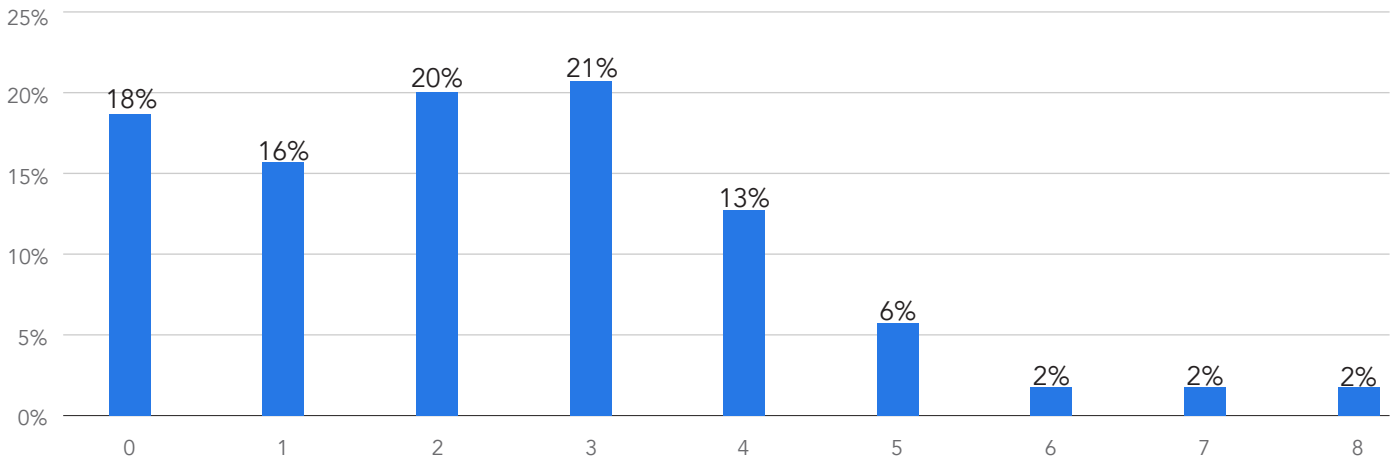
1. To understand the prevalence and impact of different types of online attack or threat.
2. Rank the biggest challenges faced by security professionals.
3. Determine the percentage of firms that employ multiple AV and anti-malware solutions and identify the top reasons for doing so.
4. Rank the top selection criteria for endpoint security solutions.

[1]See appendix for outline methodology details

Malwarebytes

Contents

Number of types of infections, threats, and attacks experienced in the last 12 months by companies with 50+ employees



Attacks are commonplace

The results showed a high number of businesses had experienced an online attack or threat in the last year. 82% of all organizations questioned had faced at least one. This means that, of the sample base of 685, only 124 had made it through the year.

The figures also showed a trend for businesses experiencing multiple infections, threats and attacks, with the average company being subjected to three types of attack in total. Some organizations were the target of as many as eight types of attack in the last 12 months alone.

Severity

Despite its relatively low frequency of attack by comparison with other threats, the data clearly showed that where ransomware was present, the impact was very severe. This potentially speaks to the real-world drain on IT teams struggling to decrypt, recover, or suffer the consequences of data loss.

		How severe were they?		
In the past 12 months, did your company experience the following infections, threats or attacks?	**Total** N=685	**Low Severity**	**Medium Severity**	**High Severity**
Ransomware	15%	23%	39%	38%
Advanced Persistent Threat (APT, a targeted attack aimed at your organization)	17%	28%	35%	37%
DoS or DDoS	16%	25%	51%	24%
File infector virus	40%	36%	41%	23%
Hacking or network intrusion	29%	31%	46%	23%
Drive-by download	19%	40%	40%	20%
Malware (viruses, worms, spyware and other malicious programs)	67%	40%	42%	18%

Given their sophistication and highly tailored nature, the targeted APT threat also scored highly in terms of severity of impact, again out of proportion with the numbers of companies experiencing such an attack. This speaks of a low volume, yet highly impactful attack. Conversely, despite having a high incidence of penetration, the burden of infection from Potentially Unwanted Programs, such as adware and toolbars, on IT teams was relatively low.

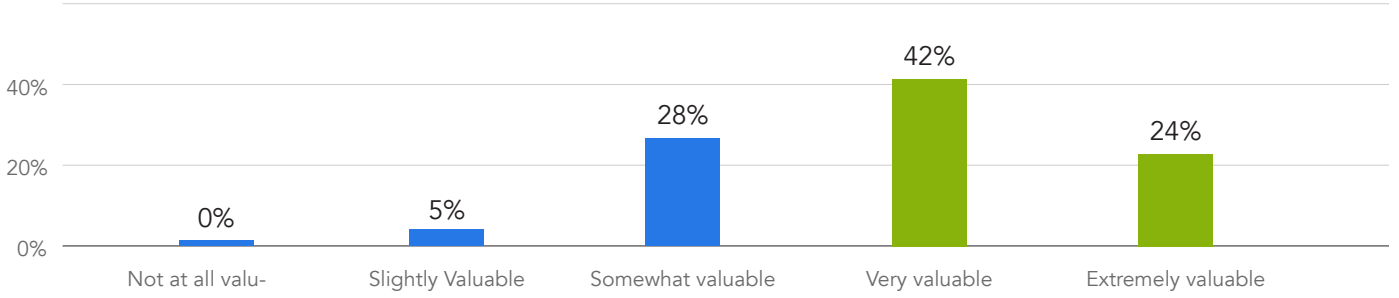
2015, the year of the vulnerability?

As we move into 2015, the data identified that browser vulnerabilities are making endpoint security most challenging. Flaws in popular browsers such as Internet Explorer, which can be exploited as part of advanced attacks, were identified as the threat which is currently making endpoint security most difficult for organizations, indexing 10 points higher than the next nearest answer and 13 points higher than the

	Total Number of Endpoints			
Which of the folowing make endpoint security difficult for your organization	**1-99**	**100-999**	**1000+**	**Total**
Browser vulnerabilities	70%	73%	76%	72%
Mobile device vulnerabilities	54%	65%	68%	62%
Advanced Persistent Threats	55%	57%	69%	59%
Cleaning infected endpoints	54%	60%	56%	57%
OS security bypasses	51%	54%	59%	55%
Zero-day malware	44%	57%	57%	53%
None of the above	0%	3%	3%	2%

The growth in awareness around this issue could be linked to the increasing number of updates for browser vulnerabilities, with more in 2014 than previous years[2]. This could also be tied to the increasingly popular use of vulnerabilities as a part of the advanced attack chain, or the growing use of exploit kits. In response to this threat, 94% of all businesses questioned said they would find a purpose-built exploit mitigation tool valuable in some form. This was especially true in organizations which have to manage more than 1000 endpoints. The most valuable feature of such a tool, according to those questioned, was that it should be compatible with existing antivirus and anti-malware products, highlighting a desire to operate it in tandem on the endpoint.

How valuable would an exploit mitigation tool be?



[2]'Why are there more browser vulnerabilities these days?' – Larry Seltzer, ZDNet Nov 11, 2014

The real world impact

The impact of enterprise threats is still not gauged by in-house teams in terms of the data being stolen or intellectual property compromised. Rather, the data shows that it is largely in the resource outlaid directly resolving and remediating the threat. This is evidenced by the fact that the most common impact cited by IT leaders suffering from attack is the increased help-desk workload it generates. This front-line thinking carries into the fact that the next largest effect is seen to be with the reduction in productivity suffered by the impacted employee.

	Total Number of Endpoints			
What impact did the threats or attacks have on your organization?	**1-99**	**100-999**	**1000+**	**Total**
Increased help-desk time	12%	25%	40%	24%
Reduced employee productivity	13%	31%	37%	20%
Difficult to remediate	18%	37%	32%	13%
Customer data lost or compromised	50%	22%	19%	9%
Intellectual property lost or compromised	49%	24%	19%	8%
Negative effect on reputation or sales	51%	25%	18%	6%

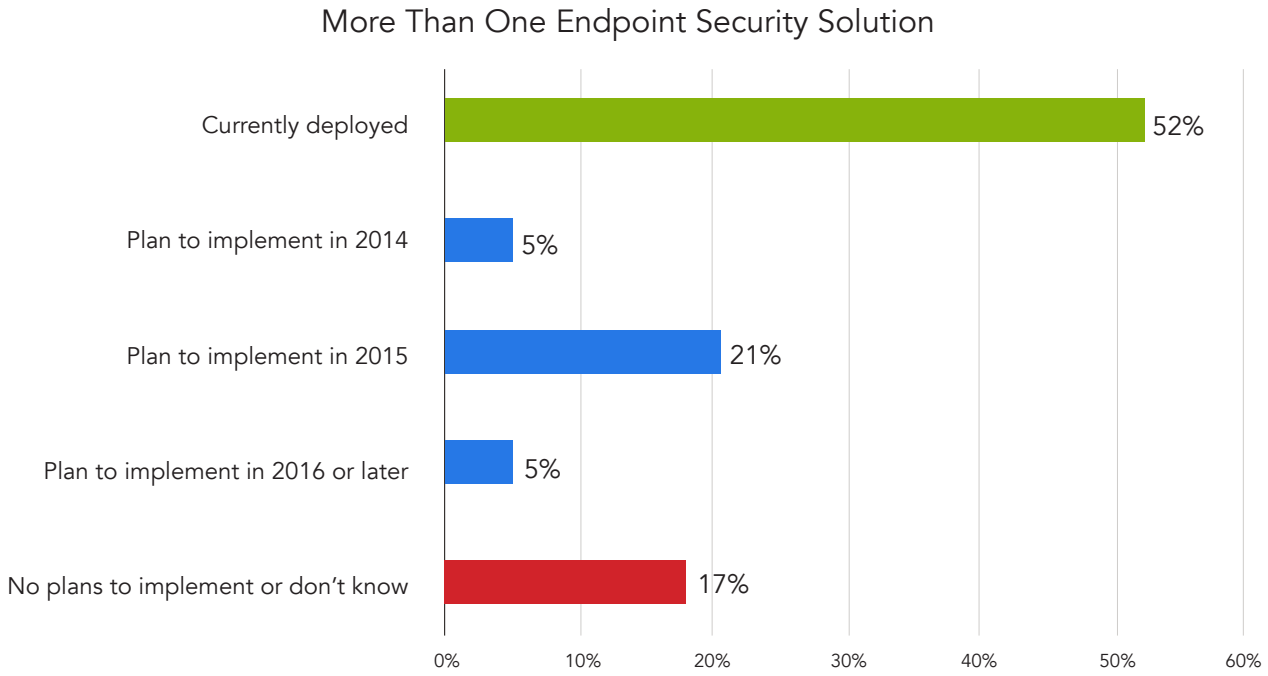
Traditional antivirus typically tends to struggle to remove today's advanced malware. In response, those surveyed said they normally either undertake the lengthy process of quarantining the machine and reimaging, or contacting the vendor of the failed endpoint solution for advice.

Layered endpoint security enhancing failing AV

84% of all of those questioned agreed that advanced malware has made traditional endpoint antivirus less effective and the majority, 80%, plan to purchase an endpoint security solution in the next 12 months.

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
Traditional AV has become much less effective at countering the latest malware.	2%	5%	9%	20%	37%	27%
Having two or more endpoint anti-malware products provides better protection.	4%	8%	10%	21%	32%	25%
The weakest security link is the endpoint.	3%	6%	10%	23%	36%	21%

Awareness of the fading efficacy of traditional AV is accompanied by a move towards layered endpoint solutions. Of those questioned, 78% said they were looking to have more than one endpoint security solution in place by the end of 2015. Adding an additional layer in this way augments front-line threat protection, with the majority of respondents admitting that "a single endpoint security program can't catch all malware."



Conclusions

1. Attacks are now commonplace, irrespective of company size and vertical sector.

2. Ransomware is emerging as an enterprise threat which, when it occurs, can be severely impactful.

3. IT leaders are worried by the emerging threat from browser vulnerabilities

4. Respondents see the largest impact from attack as the post-incident clean-up and decreased effectiveness of the affected employees.

5. IT leaders agree that advanced threats have made traditional antivirus less effective, and are adopting a layered endpoint in response.

Appendix

- Blind online survey designed by independent research firm Lawless Research using Qualtrics survey software

- 685 endpoint security purchase decision-makers from Research Now online panel in US companies with 50 or more employees:
  - *50 to 99: 121*
  - *100 to 999: 343*
  - *1,000+: 221*