A Custom Technology Adoption Profile
Commissioned By Trend Micro

October 2015

Evolving Threats Call For Integrated Endpoint Security Solutions With Holistic Visibility

Introduction

High-profile attacks from malicious malware occur with frightening regularity. 53% of midsize and enterprise businesses in the US, the UK, France, and Germany reported a breach of sensitive data within the past year, and by one estimate, the number of malware examples rose by 75% in 2014 versus the previous year. This evolution of advanced threats overwhelms both IT organizational bandwidth and capabilities of traditional antivirus methods such as blacklisting, leaving firms exposed to tremendous risk. At the same time, some prominent discussions in information security circles suggest that prevention and even detection are lost causes. However, our data show that IT security buyers reject this notion, and instead actively seek advanced technologies that integrate prevention, detection, and control/remediation capabilities that provide deep visibility into the threat life cycle to halt or mitigate damage.

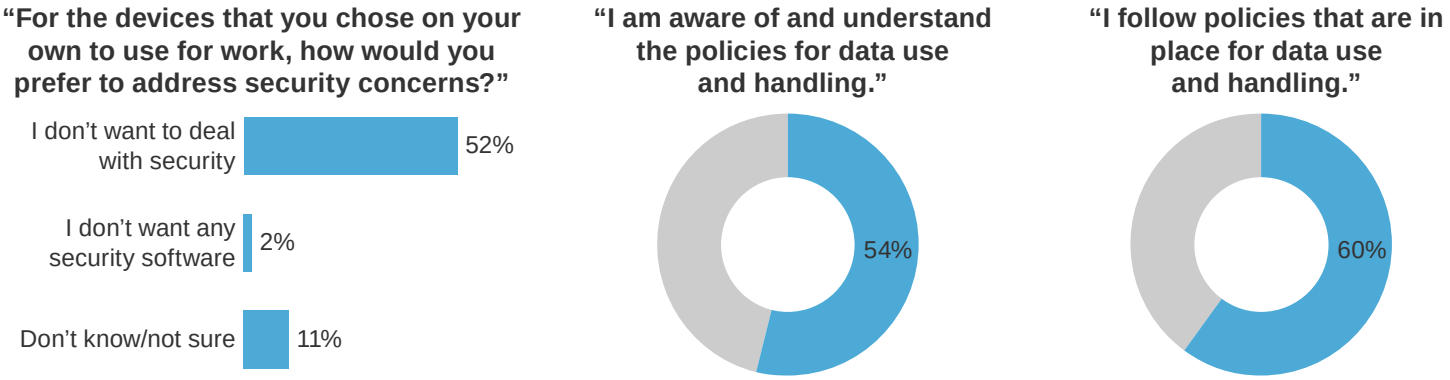
This Trend Micro-commissioned profile of IT security decision-makers at companies with between 500 and 5,000 employees in the US, the UK, France, and Germany evaluates the evolving nature and prevalence of malware and the elements of protection needs being sought by firms as a result. The study is based on Forrester's own market data and a custom study of the same audience.

Advanced Threats And Ambivalent Employees Put Firms At Risk

The pervasiveness of malicious actors and the malware they let loose — along with the detrimental effects that affect companies and individuals alike — is not lost on anyone who has paid attention to the news in recent years, let alone IT security staff. The rate at which such threats are growing, along with increased vulnerability wrought by modern work styles and employee attitudes, however, are less appreciated. Our study found that:

- **The number and nature of threats are advancing.** The number of examples of new malware continues to leapfrog counts from previous years at an alarming rate. In 2013, over 80 million new malware were detected, a number that grew by a whopping 75% in just one year to over 140 million in 2014.[1] Not only is malware proliferating in pure numbers, but its variants are also becoming more numerous and sophisticated, thereby overwhelming both the capacity and abilities of signature-based antivirus engines and resulting in missed threats and a poor endpoint experience for users.[2] Of particular concern is the increasingly targeted nature of attacks that are now more likely to be aimed at specific organizations. In the first eight months of 2015, one trusted intelligence firm tracked 144 targeted attacks that led to publicly disclosed breaches of data, while noting only seven broad attacks in the same time period.[3]
- **Most firms have experienced a sensitive data breach.** High-profile breaches of personal data at retailers, government agencies, health care companies, and other entities make the news with frightening regularity. These headline-grabbing events, however, represent a drop in the bucket among the massive number of attacks that hit American businesses. In fact, 53% of the IT security decision-makers we surveyed reported their firms as having experienced a breach of sensitive data within the past year, in addition to 4% who admitted they weren't sure whether or not their firm was attacked.
- **Information workers are ambivalent about endpoint security.** Despite the deluge of malicious attacks on businesses, information workers, defined as those who use an Internet-connected device for work for an hour or more per day, now use multiple personal devices to perform their duties. 61% of these workers use their own smartphones for work, while 56% do the same with personally-owned tablets.[4] Mobile form factors are particularly prone to a litany of risks across disparate use cases, but these individuals are ambivalent about the threats posed to the sensitive corporate information on their devices. While only 2% of these workers don't want any security software on the devices they choose for work, 52% indicated that they don't want to deal with security, leaving the onus of threat protection on companies. This lack of concern is especially troubling considering that 60% of information workers said they don't follow policies in place for data use and handling, and 54% aren't even aware of them (see Figure 1).

FIGURE 1
Employees Are Ambivalent About Endpoint Security, Even On Their Own Devices



Base: 2,188 information workers in the US, the UK, France, and Germany

Source: Business Technographics® Global Devices And Security Workforce Survey, 2014, Forrester Research, Inc.

Insufficient Legacy Antivirus Solutions And Scant Internal Resources Don't Address The Full Threat Life Cycle

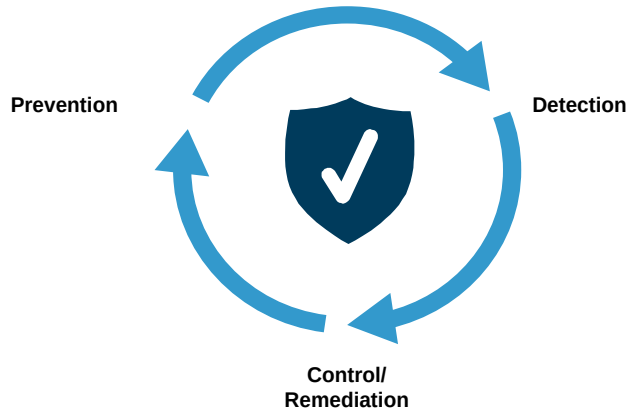
The threat life cycle refers to three stages of an organization's interaction with malware: prevention, detection, and control/remediation. A sound approach to fighting malicious code and actors must address each element of the life cycle (see Figure 2). However, the sheer number and nature of today's threats mean that one or more stages are often, if not typically, overlooked due to insufficient scalability or capabilities of existing solutions or inadequate IT resources. Insufficient technical protections also overwhelm security staff with stretched bandwidths and poor knowledge of new or evolved threats, further weakening an already compromised line of protection. However, decision-makers are waking up to their increasing levels of vulnerability and are challenging notions that portray comprehensive protection as nothing more than a dream. We found that:

› **Firms aren't prepared to prevent and detect today's threats.** IT security professionals are less than confident in their preparedness to take on threats with their existing capabilities. While slightly fewer than half (47%) agreed that their current visibility into endpoint behavior lacks the depth and breadth required to detect zero-day malware or advanced threats, a significant 28% remain unsure, leaving only 26% who believe they have adequate endpoint visibility. Furthermore, 63% believe their organization lacks the staffing expertise to respond to detected events (see Figure 3).

› **Antivirus adoption is being ditched in favor of advanced solutions.** While antimalware technologies, having been on the market since the late 1980s, remain the most ingrained security software type, the pure magnitude and severity of modern threats are testing the viability of their top status. IT security professionals are now keenly aware of the gaps in protection that leave their sensitive information vulnerable and are seeking a better solution. Among firms without a given endpoint security technology in place, antimalware is being considered for implementation at a lower rate than any other solution. Instead, security buyers now seek more advanced preventative technologies, led by endpoint behavioral analysis with remediation, endpoint investigation/forensics tools, application execution isolation, and application whitelisting (see Figure 4).

FIGURE 2

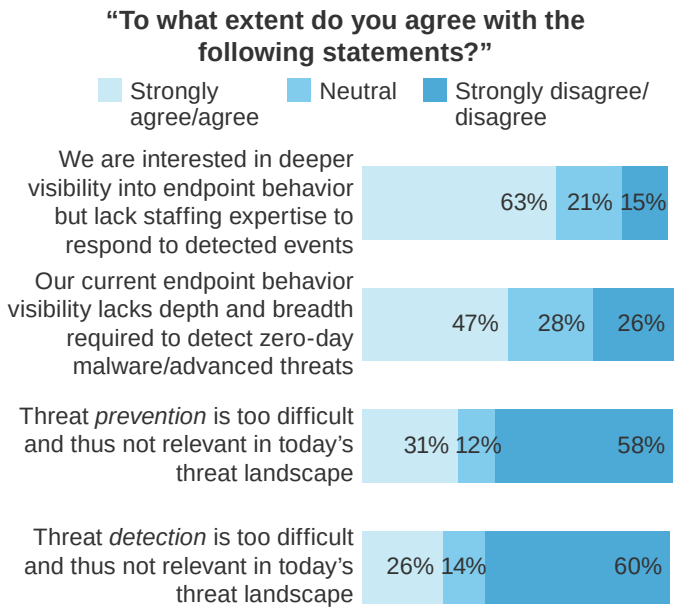
Fighting Today's Malware Takes A Three-Stage Approach



Source: Forrester Research, Inc.

FIGURE 3

Threat Prevention And Detection Are Viewed As Important, But Firms Are Challenged To Obtain Adequate Insight Into Endpoint Behavior



Base: 154 IT security decision-makers in the US, the UK, France, and Germany

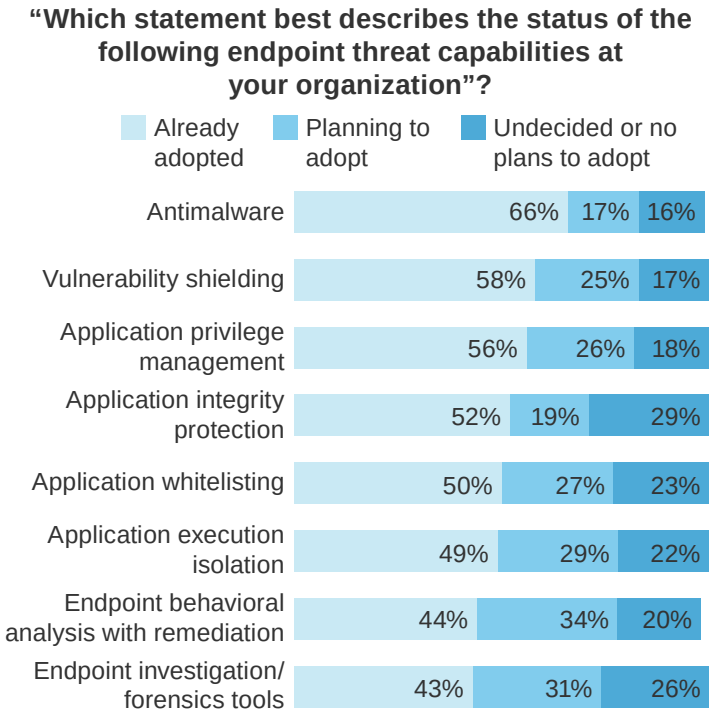
(percentages may not total 100 because of rounding)

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, June 2015

› **Prevention is dead. Long live prevention.** A recent line of conversation within information security circles is that prevention is dead, and thus resources must be focused more exclusively on detecting threats after they have infiltrated a system.[5] This attitude is a byproduct of the ineffectiveness of traditional antivirus solutions to protect against advanced threats. In fact, 31% of our survey respondents feel that prevention is so challenging that it's not relevant in today's threat landscape, compared with 26% for threat detection (see Figure 3).

FIGURE 4

Planned Adoption Of Advanced Endpoint Security Technologies Threatens AV's Dominant Position



Base: 154 IT security decision-makers in the US, the UK, France, and Germany

(percentages may not total 100 because of rounding)

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, June 2015

IT Security Seeks A Holistic, Integrated View Of The Threat Life Cycle

Security professionals may attest anecdotally to the importance of prevention, detection, and control/remediation capabilities, but does that sentiment carry over when it comes time to make an investment in technology? According to our survey, it's not just talk; IT security is putting its money where its mouth is, and is especially cognizant of how to wisely implement capabilities in a way that connects each element of the life cycle:

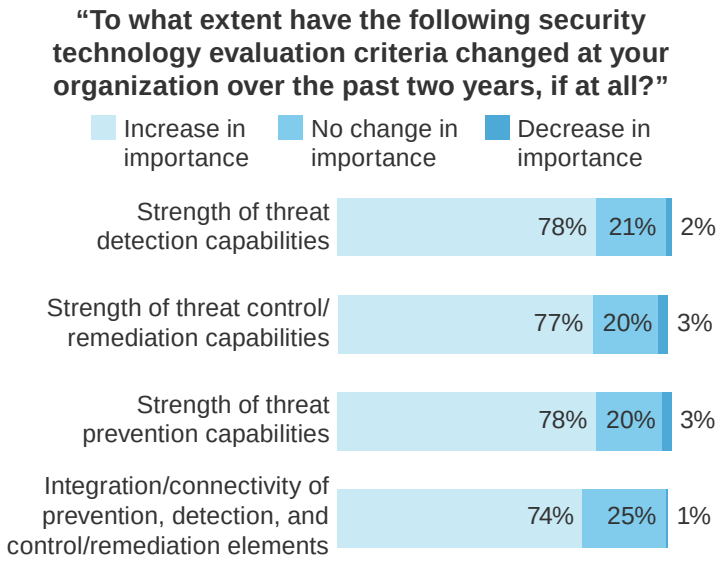
› **IT endpoint security budgets and requirements account for each part of the threat life cycle.** Today's malware and the journeys they follow from origin to infiltration are complex, necessitating a holistic view of the threat life cycle by security staff in order to understand specific threats and execute a counteroffensive. This is truer now more than ever, as a majority of employees make use of their own devices for work, utilize applications adopted by individual lines of business, and pay little attention to data policies. As a result of the need for holistic visibility, and the failure of legacy solutions to deliver on that need, 77% to 78% of security respondents we surveyed indicated an increase in importance of detection, prevention, and control/remediation capabilities in their firms' security technology evaluation criteria (see Figure 5). It follows logically that these firms now dedicate significant portions of their security budgets for each of the stages, with medians of 40%, 33%, and 26% allocated to threat prevention, dedication, and control/remediation, respectively (see Figure 6).

› **IT buyers recognize the value of interconnected threat prevention, detection, and control/remediation capabilities.** Not only are the three distinct stages of the threat life cycle recognized as critical, but so too is the importance of integrations between them in order to protect sensitive information. An overwhelming 87% of the IT security decision-makers we surveyed believe that such an interconnected structure of threat prevention, detection, and control/remediation technologies is important for adequate protection against advanced adversaries, and 79% said that that sentiment is shared across their organization, as evidenced by increased interest (see Figure 7). What's more, this view is now firmly implanted in technology evaluation criteria, with 74% reporting integration as having increased in

importance in such critique and selection processes over the past two years (see Figure 5). These organizations understand the value of a connected security platform when prevention, detection, and response functions operate in lock-step; detected events are remediated more quickly; and prevention policies can be automatically updated to ensure those threats are blocked in the future. Bridging these three capabilities reduces the requirement for skilled security incident response staffing while also reducing operational friction for the security administration team.

FIGURE 5

Threat Prevention, Detection, And Control/Remediation — And Their Integration — Are Big Considerations For Security Technology Buyers



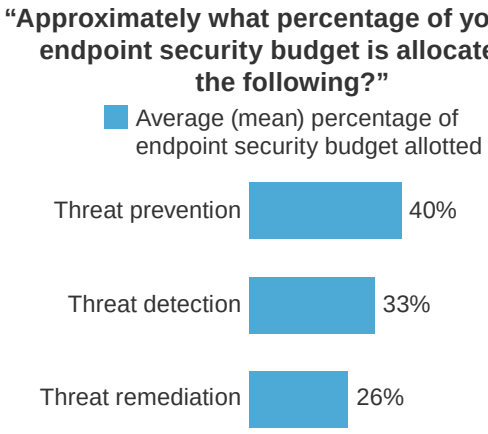
Base: 154 IT security decision-makers in the US, the UK, France, and Germany

(percentages may not total 100 because of rounding)

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, June 2015

FIGURE 6

Prevention, Detection, And Remediation Are Each Allocated Significant Budget



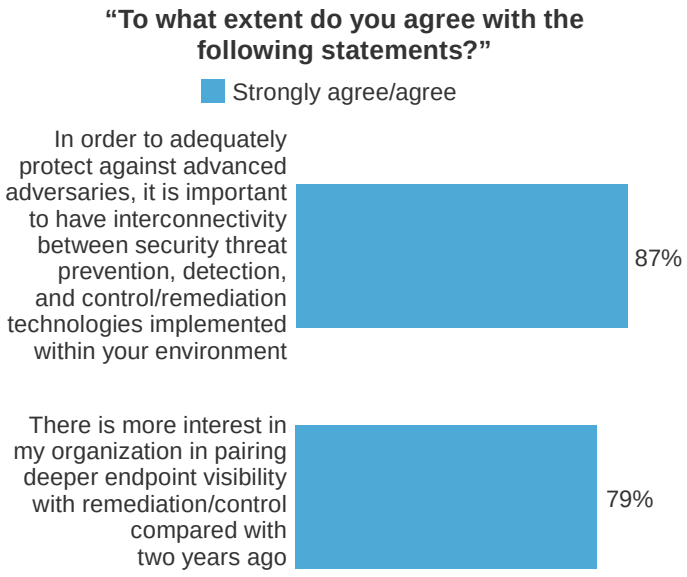
Base: 154 IT security decision-makers in the US, the UK, France, and Germany

(percentages may not total 100 because of rounding)

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, June 2015

FIGURE 7

Integration Of Capabilities Addressing Each Phase Of The Threat Life Cycle Is Viewed As Critical



Base: 154 IT security decision-makers in the US, the UK, France, and Germany

Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, June 2015

FORRESTER®

Conclusion

As a litany of advanced threats threatens the sensitive data held by organizations across industries, firms do themselves a great disservice by relying on outdated antivirus technologies that aren't designed to handle the volume or nature of evolved malware. As demonstrated evidence of sound data governance policies become table stakes in the eyes of customers, firms will need deep visibility into each part of the threat life cycle — prevention, detection, and control/remediation. Fortunately, a large majority of IT security decision-makers we interviewed are taking both the threats and the solution seriously. They actively seek a balanced approach with advanced capabilities designed with modern threats in mind. Ultimately, this will allow them to adequately defend the data that is most vital to their organizations.

Methodology

This Technology Adoption Profile was commissioned by Trend Micro. To create this profile, Forrester leveraged its Global Business Technographics® Security Survey, 2015 and its Business Technographics Global Devices And Security Workforce Survey, 2014. Forrester Consulting supplemented this data with custom survey questions asked of IT security technology decision-makers in the US, the UK, France, and Germany. The auxiliary custom survey was conducted in June 2015. For more information on Forrester's data panel and Tech Industry Consulting services, visit www.forrester.com.

Endnotes

[1] Source: The AV-Test Institute (https://www.av-test.org/en/statistics/malware/).

[2] Source: "Prepare For The Post-AV Era Part 1: Five Alternatives To Endpoint Antivirus," Forrester Research, Inc., June 9,, 2014.

[3] Source: CyberFactors, a wholly owned subsidiary of CyberRiskPartners and sister company of CloudInsure.

[4] Source: "The State Of Enterprise Mobile Security, Q2 2015: Strategies Continue To Focus On Mobile Apps," Forrester Research, Inc., May 13, 2015.

[5] Source: "Forrester's Targeted-Attach Hierarchy Of Needs: Assess Your Advanced Capabilities," Forrester Research, Inc., July 24, 2014.

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.