FORRESTER®

A Custom Technology Adoption Profile Commissioned By Trend Micro

Evolving Threats Call For Integrated Endpoint Security Solutions With Holistic Visibility

GET STARTED ▶

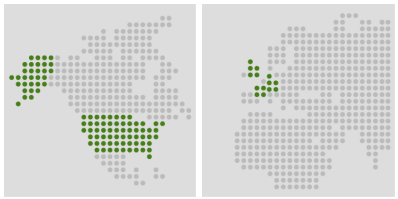
A Custom Technology Adoption Profile Commissioned By Trend Micro

Evolving Threats Call For Integrated Endpoint Security Solutions With Holistic Visibility

Tackling A New Breed Of Threats

High-profile, targeted attacks from malicious actors now occur with frightening and increasing regularity. This evolution of advanced threats overwhelms both IT organizational bandwidth and the capabilities of legacy antivirus tactics, particularly as the increasing number of endpoint devices used by employees expands attack surfaces. How are organizations responding?

In June 2015, Trend Micro commissioned Forrester Consulting to evaluate the evolving nature and prevalence of malware among medium-sized and large enterprises, as well as the elements of protection being sought by these firms as a result. This study is based on Forrester's own market data and a custom study of the same audience.



Custom Survey Demographics

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

Respondents' Company Sizes

60% 1,000 to 4,999 employees

40% 500 to 999 employees

Top Industries Represented

18% Finance/insurance

12% Manufacturing/materials

10% Business/consumer services

8% Telecommunications

8% Transport/logistics

A Custom Technology Adoption Profile Commissioned By Trend Micro

Evolving Threats Call For Integrated Endpoint Security Solutions With Holistic Visibility

1 2 3

The Number And Nature Of Threats Are Advancing

In 2013, a staggering 80 million new malware were detected. But that figure pales in comparison to the 140 million examples reported in 2014 – a 75% increase in just one year that didn't relent in 2015. Beyond the pure numbers, today's malicious actors are also more likely to target specific organizations. In the first eight months of 2015, one intelligence firm tracked 144 targeted attacks that led to publicly disclosed data breaches and only seven broad attacks.‡

These attacks aren't limited to high-profile examples from the headlines. In fact, 53% of the IT security decision-makers we surveyed were breached within the past year, in addition to 4% who admitted they didn't know whether or not they had been attacked.

The Threat Landscape Has Intensified

95% of attacks are targeted.‡

53% of companies have been targeted over the past year.*

‡Source: CyberFactors, a wholly owned subsidiary of CyberRiskPartners and sister company of CloudInsure

*Base: 154 IT security decision-mak3ers in the US, the UK, France, and Germany
Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, June 2015

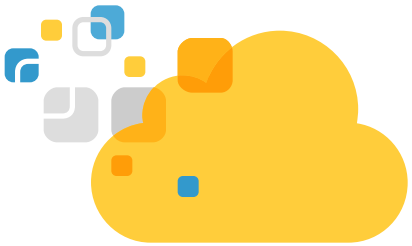
A Custom Technology Adoption Profile Commissioned By Trend Micro

Evolving Threats Call For Integrated Endpoint Security Solutions With Holistic Visibility

1 2 3

Vulnerability Is High As Information Workers Tap Sensitive Data

The escalating threat of targeted attacks is especially worrisome given the types of vulnerable data that can be accessed by many employees on a day-to-day basis. Information workers -– those who use an Internet-connected device for work an hour or more per day – often report drawing from various data pertaining to customers, business deals, intellectual property, and employees. Any compromise of such sensitive information can introduce a laundry list of consequences.



A Custom Technology Adoption Profile Commissioned By Trend Micro

Evolving Threats Call For Integrated Endpoint Security Solutions With Holistic Visibility

Employees Are Ambivalent About Endpoint Security As They Leverage Personal Devices

Information workers – the same group that often accesses privileged information as part of their jobs – now use multiple personal devices to perform their duties. 61% of these workers use their own smartphones for work, while 56% and 30% do the same with their own tablets and laptops, respectively.

Despite the deluge of malicious attacks on businesses, these workers have a generally carefree attitude towards security threats, even as personal devices increase their organizations' attack surfaces. Forrester data indicates that 40% of information workers don't follow data use and handling policies – and 46% aren't even aware of them. What's more, a majority (52%) of these workers say they don't want to deal with security, thereby placing the burden of threat protection squarely on companies.

I am aware of and understand the policies for data use and handling

I follow policies that are in place for data use and handling

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.

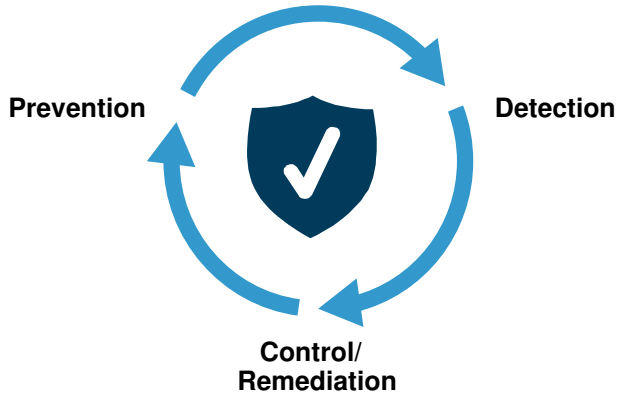
"For the devices that you chose on your own to use for work, how would you prefer to address security concerns?"

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.

1 2

Firm's Aren't Prepared To Prevent And Detect Today's Threats

There are three stages of an organization's defensive interaction with malware: prevention, detection, and control/remediation, which together constitute a threat life cycle. However, the sheer number and nature of today's threats – particularly those that find entry through vulnerable endpoint devices – means that one or more stages are often overlooked due to insufficient scalability or capabilities of existing resources. Only 26% of survey respondents believe they have adequate endpoint visibility, and 63% believe their organization lacks the staff expertise to respond to detected events.



A Custom Technology Adoption Profile Commissioned By Trend Micro

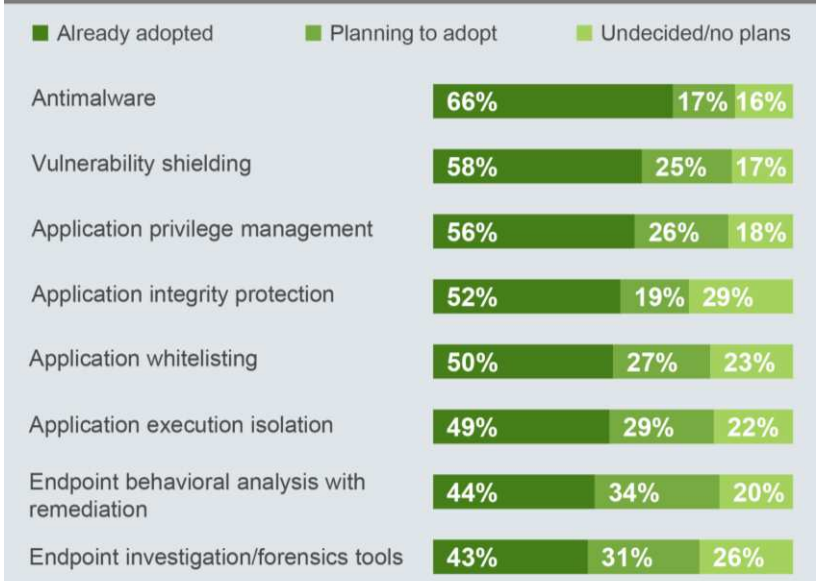
Evolving Threats Call For Integrated Endpoint Security Solutions With Holistic Visibility

1 2

Antivirus Technology Is Being Reinforced With Advanced Solutions

While antimalware technologies remain the most ingrained security software type, modern threats are testing the viability that status. Security professionals are keenly aware of the gaps that leave sensitive information vulnerable. As such, the greatest rates of planned implementation are associated with more advanced technologies, led by endpoint behavioral analysis with remediation, endpoint investigation/forensics tools, application execution isolation, and application whitelisting.

"Which statement best describes the status of the following endpoint threat capabilities at your organization?"



Base: 154 IT security decision-makers in the US, the UK, France, and Germany (percentages may not total 100 due to rounding)
Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, June 2015

A Custom Technology Adoption Profile Commissioned By Trend Micro

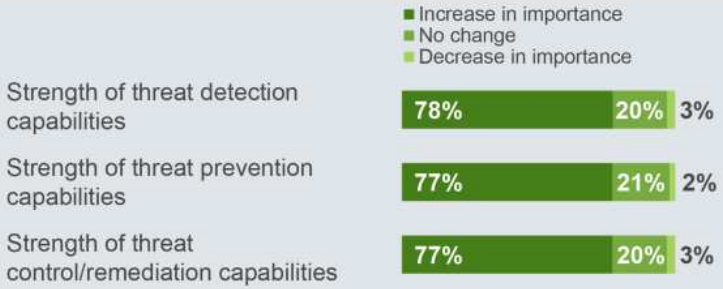
Evolving Threats Call For Integrated Endpoint Security Solutions With Holistic Visibility

1 2

IT Endpoint Security Requirements And Budgets Now Account For Each Part Of The Threat Life Cycle

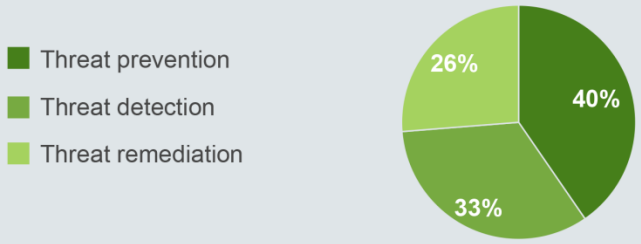
The complex journeys today's malware follow from origin to infiltration necessitate a holistic view of the threat lifecycle. As a result, IT departments aren't focusing on either preventing, detecting, or controlling threats – they're prioritizing them all. Strong majorities of survey respondents told us that each stage is garnishing increased importance at their organizations, as well as significant allocations in their endpoint security budgets.

"To what extent have the following security technology evaluation criteria changed at your organization over the past two years, if at all?"



Base: 154 IT security decision-makers in the US, the UK, France, and Germany (percentages may not total 100 due to rounding)
Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, June 2015

"Approximately what percentage of your total endpoint security budget is allocated to the following?"



Base: 154 IT security decision-makers in the US, the UK, France, and Germany (percentages may not total 100 due to rounding)
Source: A commissioned study conducted by Forrester Consulting on behalf of Trend Micro, June 2015

A Custom Technology Adoption Profile Commissioned By Trend Micro

Evolving Threats Call For Integrated Endpoint Security Solutions With Holistic Visibility

1 2

IT Buyers Seek Interconnected Endpoint Protection

Not only are all 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 sentiment is shared across their organization. This view is now firmly implanted in technology evaluation criteria, with 74% reporting integration as having increased in importance in such critiques.

"To what extent do you agree with the following statements?"
(combined answers of agree and strongly agree)

87% Interconnectivity between threat prevention, detection, and control is important to protect against advanced adversaries.

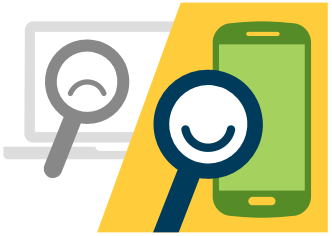
79% There is more interest in my organization in pairing endpoint visibility with remediation compared with two years ago.

74% Integration of prevention, detection, and remediation is more important in security technology evaluation compared to two years ago.

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

Conclusion

As demonstrated evidence of sound data governance policies become table stakes in the eyes of their customers, firms realize the inadequacy of antiquated antimalware tools to protect against advanced, targeted threats. As a result, a large majority of IT security decision-makers we surveyed now prioritize capabilities that provide deep visibility into each stage of the threat life cycle – prevention, detection, and control/remediation – as well as their interconnectivity.



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 forrester.com