A Custom Technology Adoption Profile Commissioned By McAfee | March 2017

Mastering The Endpoint

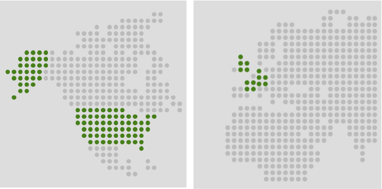
Organizations Find Value In Integrated Suites

GET STARTED ▶

Overview

In the face of constantly evolving threat vectors, IT security decision makers struggle to manage endpoint security effectively. More than two-thirds of enterprises have had their organization’s sensitive data compromised in the past year, and incidents require significant time and manual effort to remediate — and even then are often only remediated for certain devices. Security decision makers desire integrated solutions that increase their efficiency, visibility, and overall protection across their various endpoint technologies.

In January 2017, McAfee commissioned Forrester Consulting to evaluate common tools and strategies for managing endpoint security and the perceived efficacy of those strategies. Forrester conducted an online survey of 252 IT security decision makers from the US, the UK, France, and Germany, and our findings suggest that organizations are significantly challenged by overly manual security tools and desire connected security solutions that are fast, accurate, and integrated.



Geography

United States: 38%

France: 20%

Germany: 22%

United Kingdom: 20%

Company size

500 to 999 employees: 20%

1,000 to 4,999 employees: 40%

5,000 to 19,999 employees: 22%

20,000 or more employees: 18%

Role

C-level executive: 16%

Vice president: 15%

Director: 34%

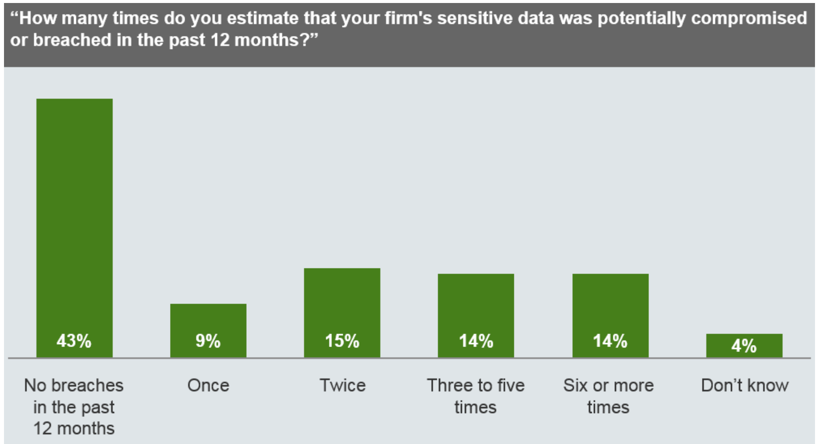
Manager: 35%

1 2 3

Enterprises Are Increasing Investments In Endpoint Security

As the use of new channels and devices increases, so does the number of vulnerabilities that companies must manage. Forrester's data shows that the majority of enterprises in the US and EMEA have had their organization's sensitive data compromised in the past 12 months. These incidents can be devastating, leading to reputational damage, lost customers, and even lost partners or employees.

As the most common targets of breaches, endpoints and servers are the top concern of IT security professionals. Forrester's data shows that endpoint security budgets account for approximately 10% of the overall IT security budget in 2016.[1]



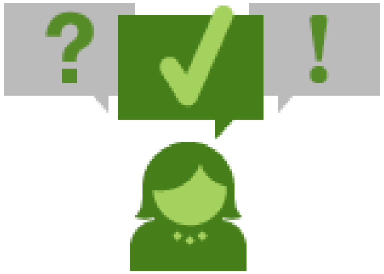
Base: 373 IT managers and above at enterprises in the US, the UK, DE, and FR
(Respondents included = 29%, filter applied)
(percentages may not total 100 because of rounding)
Source: Forrester's Global Business Technographics® Security Survey, 2016

1 2 3

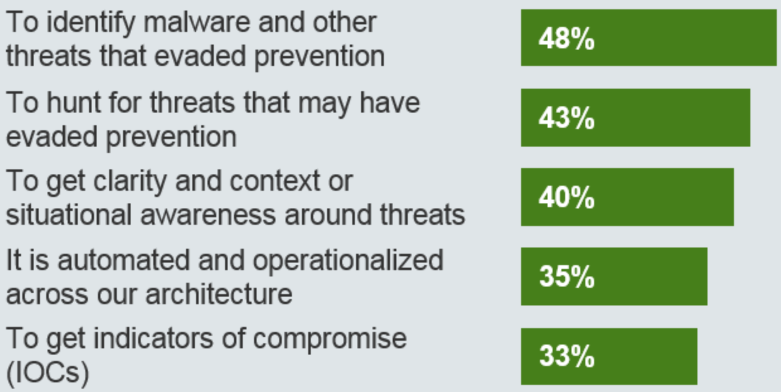
Threat Intelligence Is Maturing

To mitigate breaches and their potential effects, IT pros are investing in new and better endpoint security solutions. Our study found that of those who have been breached in the past year, 35% are increasing security and audit requirements, 26% are increasing spending on threat intelligence technologies, 26% on prevention technologies, and 22% on incident response programs.

Decision makers expect more from their security solutions than just external protection. Our study found that organizations are most commonly using threat intelligence to search for malware and threats that are already inside of their systems, rather than using market insight to keep new threats out.



"In what ways is your organization using threat intelligence? Select all that apply."



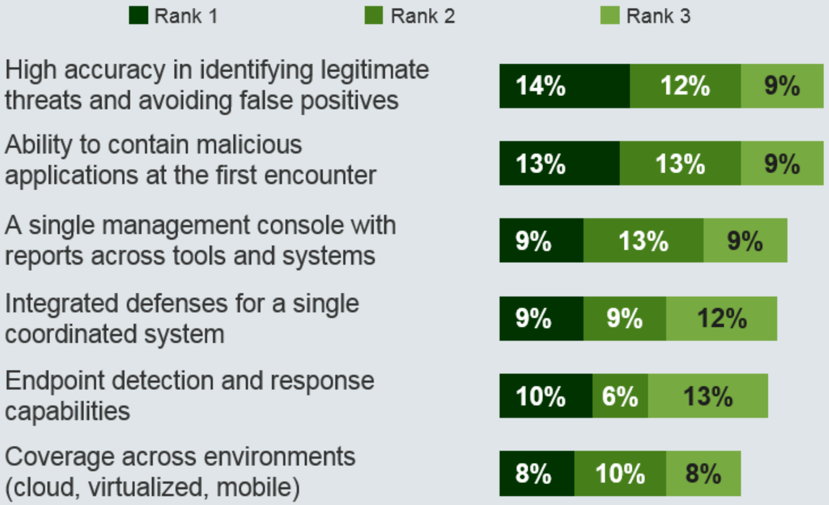
Base: 252 IT decision makers in the US, the UK, France, and Germany
Source: A commissioned study conducted by Forrester Consulting on behalf of McAfee, January 2017

1 2 3

Organizations Need Solutions That Are Fast, Accurate, And Integrated

IT security decision makers are overwhelmed by the evolving security landscape. To win the fight against an increasing number of attack vectors, they need efficient and intelligent tools that they can rely on to accurately filter through noise to identify and remediate legitimate threats. Our study found that IT security decision makers prioritize endpoint security solutions that deliver high accuracy in identifying legitimate threats and avoiding false positives, as well as have the ability to contain malicious applications at the first encounter.

"What are the most important features of an endpoint security suite?"



Base: 252 IT decision makers in the US, the UK, France, and Germany
Source: A commissioned study conducted by Forrester Consulting on behalf of McAfee, January 2017

1 2

Businesses Have Too Many Security Tools

A key challenge in managing endpoint security is that organizations have too many tools. Our study found that on average, organizations must monitor 10 different endpoint security agents, which requires use of at least five different interfaces to investigate and remediate a security incident.

In addition to adding significant time and manual effort, this large number of tools also drives up the price and complexity, both of which are listed by respondents as key barriers to managing risk effectively.

Eighty-one percent of respondents believe that there are barriers in place that inhibit their ability to effectively manage risk.

"Using your best estimate, approximately how many different endpoint security agents does your organization have in place?"

Median: 10

Base: 195 IT decision makers in the US, the UK, France, and Germany
Source: A commissioned study conducted by Forrester Consulting on behalf of McAfee, January 2017

"Using your best estimate, how many different interfaces or screens are required for a security professional at your organization to respond to a malware incident?"

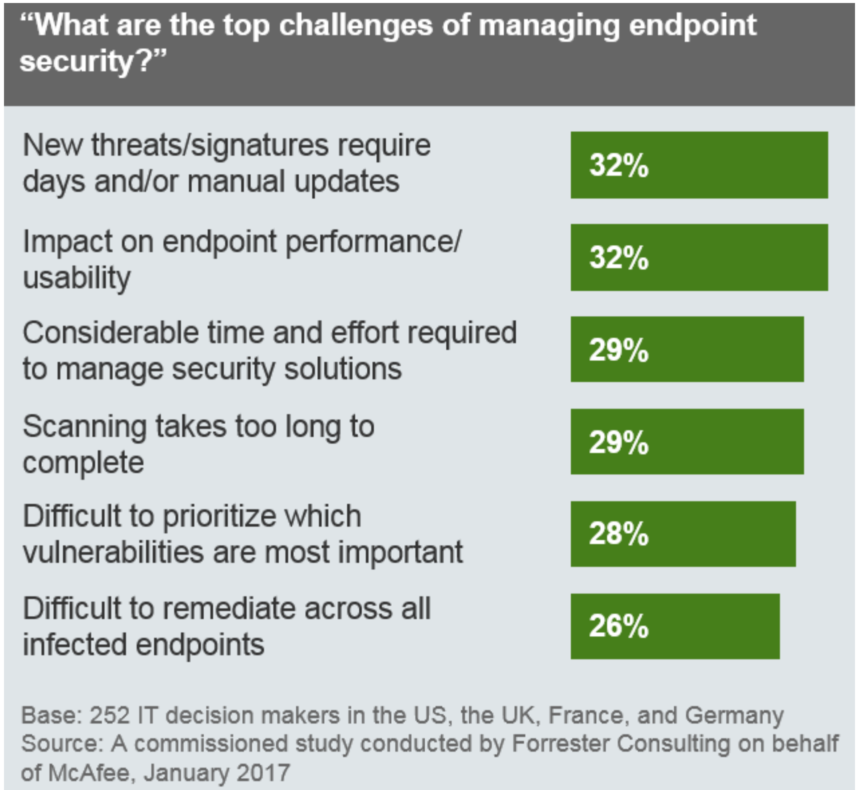
Median: 5

Base: 200 IT decision makers in the US, the UK, France, and Germany
Source: A commissioned study conducted by Forrester Consulting on behalf of McAfee, January 2017

1 2

Manual Processes Are The Norm

Given the complexity of enterprise security environments, organizations must do a lot of manual work and make decisions about vulnerabilities that they may not fully understand. Our study found that the top challenges in managing endpoint security include the time and effort required to respond to new threats/signatures, performance concerns, difficulty in prioritizing vulnerabilities, and difficulty ensuring that attacks are remediated across all infected endpoints.



"What are the top challenges of managing endpoint security?"

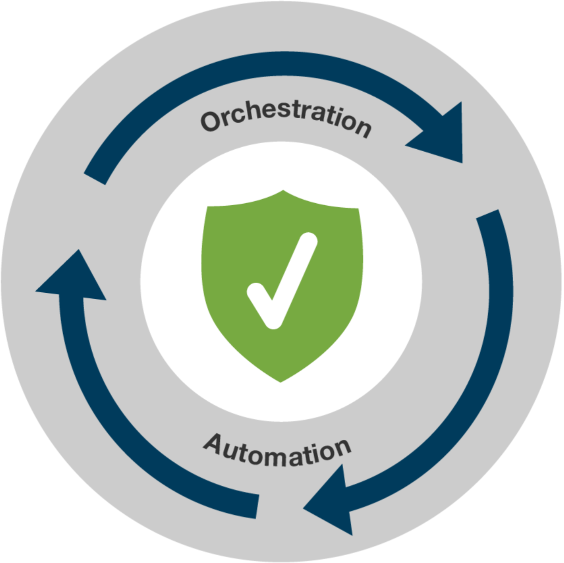
New threats/signatures require days and/or manual updates
32%
Impact on endpoint performance/ usability
32%
Considerable time and effort required to manage security solutions
29%
Scanning takes too long to complete
29%
Difficult to prioritize which vulnerabilities are most important
28%
Difficult to remediate across all infected endpoints
26%

Base: 252 IT decision makers in the US, the UK, France, and Germany
Source: A commissioned study conducted by Forrester Consulting on behalf of McAfee, January 2017

Enterprises Need Robust, Integrated Solutions

IT security professionals have three core needs when they look for endpoint security solutions: attack prevention, detection, and remediation. While historically, best-of-breed solutions for each of these reigned supreme, our study found that the majority of respondents now prefer an integrated suite solution that can manage all three of these key functions. IT decision makers evaluate potential vendors on their ability to increase efficiency and accuracy while reducing complexity.

Over 50% of respondents prefer a single vendor for each on-premises and as-a-service endpoint security solution.



Remediation
- Attack containment
- Configuration management
- Vulnerability remediation

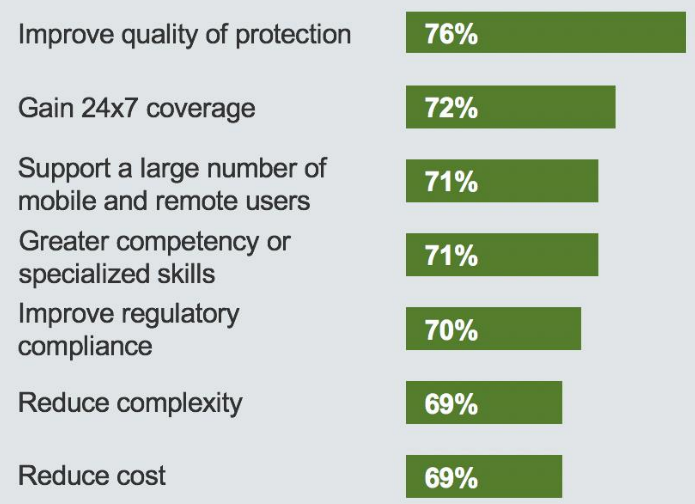
Detection
- Behavioral monitoring
- Context building/intelligence integration

Prevention
- Malware execution blocking
- System hardening
- Application control

Cloud Solutions Are On The Rise

As IT professionals consider solutions, they are increasingly looking at cloud options. Buyers of cloud security solutions cited a number of drivers for cloud adoption, including improved quality of protection (76%), 24x7 coverage (72%), support for a large number of mobile and remote users (71%), greater competency or specialized skills (71%), and improved regulatory compliance (70%).

"How important were the following in driving your firm's interest in adopting as-a-service security offerings?"



Base: 743 IT managers and above at enterprises in the US, UK, DE, and FR
Source: "Forrester's Global Business Technographics Security Survey, 2016"

Conclusion

To ensure fast, efficient, and comprehensive remediation of breaches, IT security decision makers have acknowledged the need to reduce the complexity of their endpoint security environments. Today's enterprises value integrated endpoint security solutions that can effectively handle the whole process of endpoint security, including attack prevention, detection, and remediation. Single-vendor suite solutions and cloud technologies are on the rise due to their perceived benefits, including simplicity, lower costs, and better integrated coverage across platforms.

METHODOLOGY

This Technology Adoption Profile was commissioned by McAfee.

To create this profile, Forrester leveraged its Global Business Technographics® Security Survey, 2016. Forrester Consulting supplemented this data with a custom survey of 252 IT decision makers at the manager level and above in the US, the UK, France, and Germany at organizations with 500 or more employees. This survey was completed in January 2017.

[1] Source: "The Forrester Wave™: Endpoint Security Suites, Q4 2016," Forrester Research, Inc., October 19, 2016.

Project Director:

Mark Brozek
Sr. Market Impact Consultant

Contributing Research:

Forrester's Security and Risk research group

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.