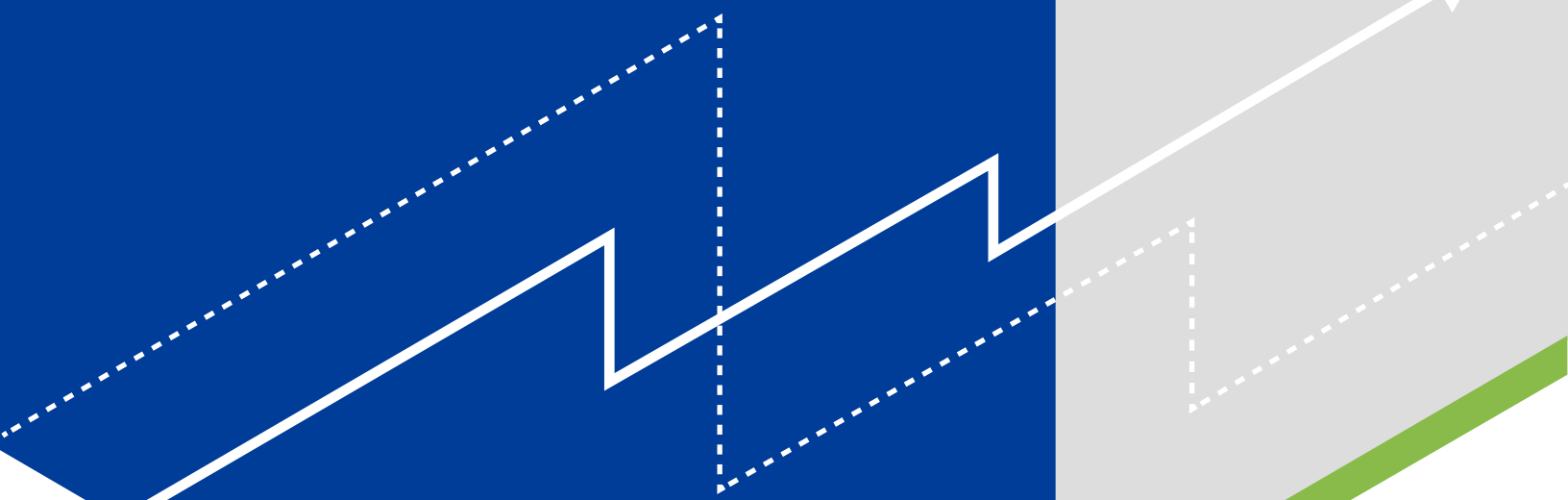
A Forrester Consulting
Thought Leadership Spotlight
Commissioned By Google

September 2017

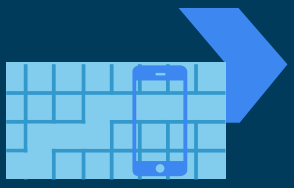
Rethink Enterprise Endpoint Security In The Cloud Computing Era



Project Director:
Karin Fenty,
Senior Market Impact
Consultant

Contributing Research:
Forrester's Security &
Risk research group

FORRESTER®



Personal devices and APIs are increasingly important to endpoint security.

Cloud service providers play an important role in helping enterprises secure endpoints.

Executive Summary

In the year 2016 alone, the world learned about security breaches that compromised nearly 2 billion records.[1] Employee endpoints are increasingly targeted: Nearly two-thirds (64%) of external attacks last year targeted a corporate-owned, employee-owned, or mobile device.[2] Data breaches cost companies time and money, weaken brand reputation, and jeopardize customer and employee trust.

As companies embrace cloud services and encourage employee mobility, digital interactions with company resources have become more distributed and virtualized, blurring the traditional concept of the endpoint. Optimizing traditional and nontraditional endpoints for access to cloud services is critical, particularly when it comes to security. To protect company and customer data, it is increasingly necessary for enterprises to revisit how they approach endpoint security.

In June 2017, Google commissioned Forrester Consulting to evaluate enterprise challenges and best practices for endpoint security in the cloud computing era. Forrester conducted a global online survey with 1,221 security decision makers at enterprises that use cloud services. Our study showed that companies need to take a broader view of endpoint security that includes all on- and off-network devices and software with access to company data.

KEY FINDINGS

- **Cloud services and employee mobility necessitate a broader perspective on endpoint security.** Nontraditional endpoints like employees' personal devices have become more relevant to endpoint security with the prevalence of software-as-a-service (SaaS), bring your own device (BYOD), and single sign on. Cloud also increases the importance of considering APIs as part of a holistic enterprise endpoint security strategy, because in the cloud, APIs act as access points to corporate data.
- **Current enterprise endpoint security strategies have not kept up with new imperatives.** Despite universal concerns about API security, only 44% of security decision makers consider APIs as part of their endpoint security strategy. Similarly, although most companies allow employees to access resources through personal devices, just 43% consider personal smartphones part of their endpoint strategy.
- **Enterprises are enlisting cloud service providers to offer unique help.** The number of enterprises leveraging public cloud platforms has more than doubled in the last three years.[3] As enterprises trust cloud service providers to be the custodians of their data, cloud providers can help by controlling how data is exchanged through APIs, which in turn helps protect company resources from malicious actors. Seven in 10 companies already rely on cloud providers for endpoint security.

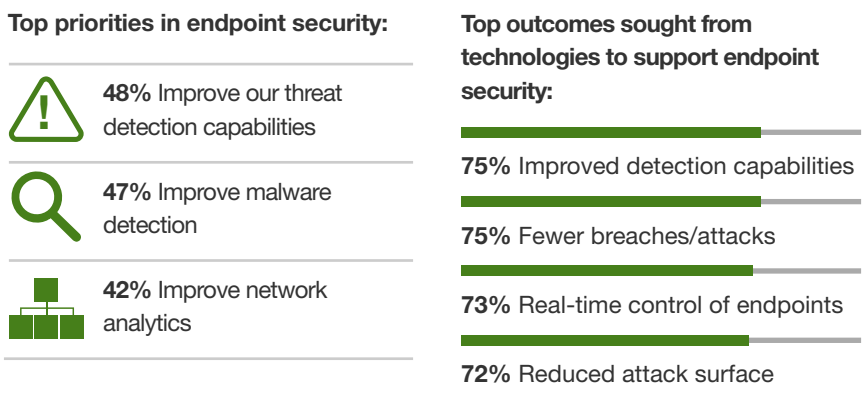
Modern Companies Need To Redefine Endpoint Security

More than half of global enterprises (53%) experienced at least one compromise or breach during a 12-month period between 2015 and 2016 — a 5% increase over the previous year.[4] Endpoint security is critical to protecting against these breaches because external attackers most commonly target corporate servers, company-owned devices, and employee-owned devices.[5]

Our global study of 1,221 IT security decision makers showed that enterprises consider improved detection and analytics capabilities essential to endpoint security. Threat detection and network analytics drive top sought outcomes like fewer breaches, real-time control of endpoints, and reduced attack surfaces (see Figure 1). But detecting and controlling all endpoints has become trickier as the volume and variety of endpoints accessing company resources continue to rise.

73% of security decision makers seek technologies that enable real-time control of endpoints.

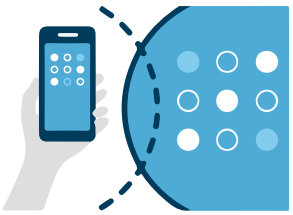
Figure 1



Base: 1,221 IT security decision makers at global enterprises that use cloud services
Source: A commissioned study conducted by Forrester Consulting on behalf of Google, July 2017

NONTRADITIONAL ENDPOINTS AND APIS ARE MISSED OPPORTUNITIES AND RISK DRIVERS

By enabling access to data and applications from any device or browser, cloud service delivery expands an enterprise's attack surface. End users access company data from an increasingly vast number of devices on and off the network, most often from the browser as a central access point. To close the gap between the user and cloud platform, enterprises need to protect not only corporate servers and company-owned devices, but employee-owned devices with access to company resources and APIs that act as the access points between external connections and company data.



Our survey of enterprises that use cloud services revealed that most security professionals have not embraced this new perspective on endpoint security, leaving few companies confident in their ability to deliver desired outcomes. Specifically, we found that:

FORRESTER®

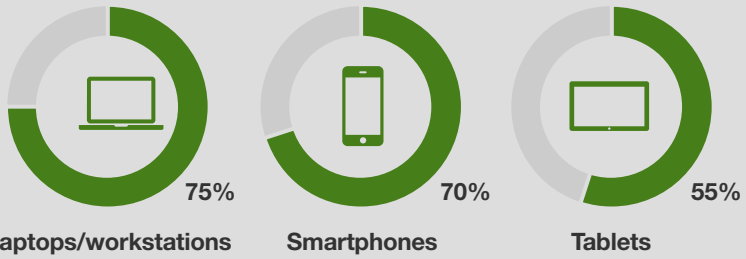
› **The browser has become a central access point for business apps and email.** As companies embrace the cloud, browser security is essential because more and more business activities are executed within web browsers. For example, 76% of the companies we surveyed have browser-based email options and 70% enable employees to access office applications from a browser (see Figure 2). With the browser being a primary interface for business functionality, it becomes not only a target for attackers, but an important aspect of endpoint security strategy.

› **Employees increasingly access company resources via personal devices.** Through formal BYOD programs, single sign on options, and other programs that aim to promote employee mobility, the vast majority of companies (84%) allow employees to access company data from their personal laptops, smartphones, and tablets (see Figure 2). These personal devices expand the enterprise's attack surface for malicious activities. Forrester data shows that even as personal devices become more prevalent for business use, employees expect IT to help secure those mobile devices through software updates and encryption[6].

72% to 77% of information workers say IT is responsible for updating security software, operating system updates, and encrypting documents on mobile devices.

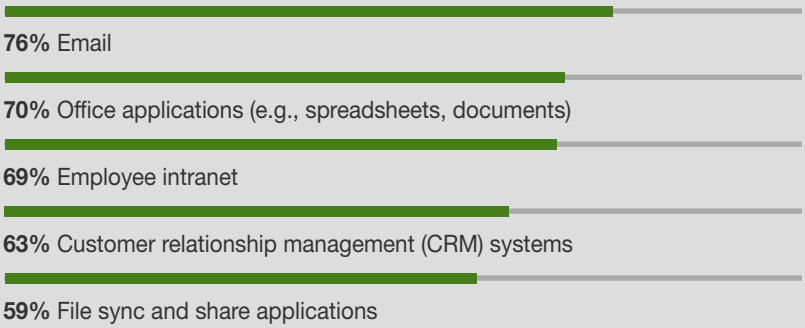
Figure 2

"Does your organization allow employees to use any of the following personal devices to access company resources, either through a formal BYOD program, single sign-on, or other program?"



16% N/A; access to company resources not allowed on any personal device

"Which of the following do your organization's employees access via a web browser?" (Showing top five responses)



Base: 1,221 IT security decision makers at global enterprises that use cloud services
Source: A commissioned study conducted by Forrester Consulting on behalf of Google, July 2017

Personal devices, browser-centric business apps, and APIs expand enterprise attack surfaces, creating security concerns.

FORRESTER®

› **Virtually everyone has concerns about APIs.** APIs are increasingly critical to the business because they allow companies to connect with external and internal resources that help improve customer and employee experiences. APIs are also a critical aspect of holistic endpoint security strategies because, ultimately, APIs are access points to company data. A whopping 97% of respondents cited security concerns about APIs, including concerns about cloud platforms, network protocols, and data in transit.

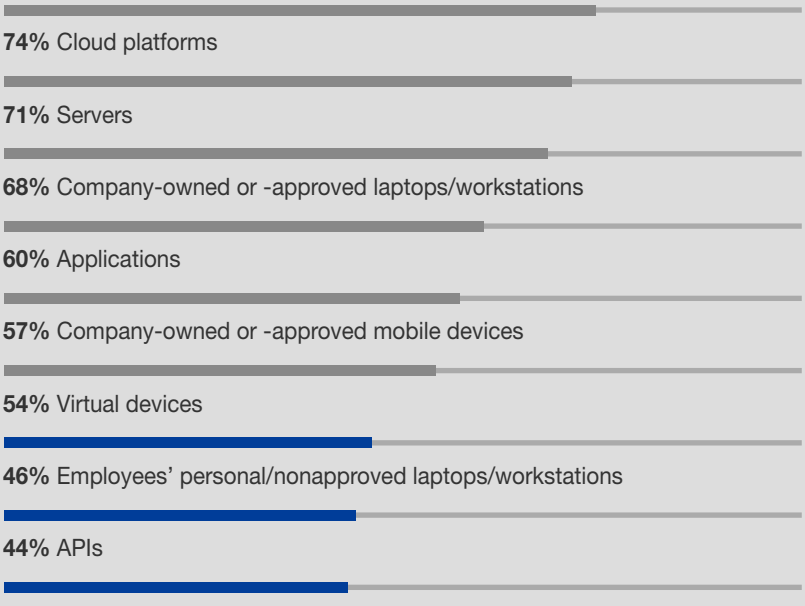
› **Despite these trends, most security teams fail to incorporate personal devices and APIs into their endpoint strategies.** Enterprises have not evolved their security strategies to reflect new imperatives in the cloud computing era. While most companies make efforts to secure endpoints such as cloud platforms, servers, and company-owned laptops, only 43% to 46% consider personal laptops, personal smartphones, and APIs as part of their endpoint security strategy. As a result, only 35% of security professionals feel their organization is very effective at managing access to enterprise assets, and only 32% said the same about monitoring endpoints for malicious activities (see Figure 3).

97% of respondents cited concerns about API security. Top API concerns include:

- **55%** Cloud platform concerns
- **53%** Network protocol attacks exposing data in transit
- **52%** Third-party risk

Figure 3

Technologies considered part of firms' endpoint security strategies:



Percent considered very effective at achieving outcomes:

35% Managing access to enterprise assets

32% Monitoring endpoints for malicious activity

Most companies fail to consider personal devices and APIs in their strategies, leaving few confident that they can secure all endpoints.

Base: 1,221 IT security decision makers at global enterprises that use cloud services
Source: A commissioned study conducted by Forrester Consulting on behalf of Google, July 2017

FORRESTER®

Cloud Service Providers Are Increasingly Important To Endpoint Security

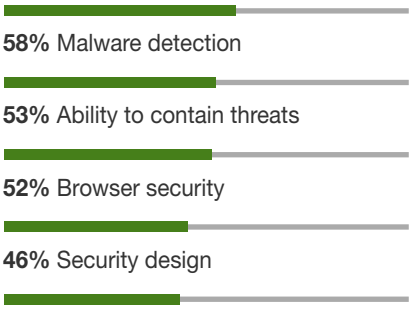
As the purview of endpoint security gets broader, enterprises need ways to monitor and control the greater volume and variety of endpoints accessing company resources. As companies embrace a more cloud-centric strategy for infrastructure and application delivery, they can tap cloud service providers for resources and expertise. Our study showed that:

- **Seven in 10 companies turn to cloud providers for endpoint security tools and solutions.** As organizations move more data and functionality to the cloud, they rely on tools provided by these cloud providers for securing their data. More and more, cloud providers are tasked with overseeing the authentication, patch management, and monitoring of these cloud environments on their customers' behalf. In fact, Forrester forecasts that native infrastructure-as-a-service/ platform-as-a-service (IaaS/PaaS) security spending will grow 41% over the next five years.[7]
- **API security is a driving factor in selecting cloud providers.** Cloud service providers can improve security by forcing user interaction with data through a secure API, through which they can control the access and modification of data — i.e., the asset that needs to be protected. As much as the browser is the primary interface for traditional endpoints, the API is the access point to the cloud. In fact, API security was the second most important criterion respondents use to select a cloud provider, behind infrastructure protections and monitoring.
- **Security buyers prioritize malware detection, threat containment, and browser security in endpoint security tools.** How vendors approach security design and their reputation are also key criteria for selecting endpoint security tools (see Figure 4). Cloud service providers are uniquely positioned to deliver on these needs because of their centralized view of endpoint environments and the ability to quickly and efficiently distribute threat data or remediations back down to the endpoint. With greater visibility and the ability to respond quickly and return the endpoint to a "clean" state, enterprises can both prevent attacks and minimize business disruptions when they occur. For these reasons, 71% of respondents currently use an endpoint solution from a cloud provider compared to 49% who use specialist vendor solutions.

71% of respondents use solutions from cloud providers for endpoint security.

Figure 4

Most important considerations for user endpoint security tools:
(Showing top five responses)



Base: 1,221 IT security decision makers at global enterprises that use cloud services
Source: A commissioned study conducted by Forrester Consulting on behalf of Google, July 2017

43% consider security of API access one of the most important criteria in selecting a cloud provider.

FORRESTER®

Key Recommendations

Endpoint protection requires a resilient and resistant platform that can be updated quickly, compartmentalize user tasks, and apply protections to holistically protect the system or device from even inadvertent misuse. As attackers leverage a myriad of techniques to compromise these devices, it has become critical to apply mitigating controls at each layer of the endpoint security stack.

As organizations embrace cloud-centric infrastructure and applications, cloud service providers are increasingly relevant players alongside other third-party specialists and other point solutions. Security professionals at enterprises using cloud services should consider the following recommendations:

Vulnerability management is essential for the entire endpoint security stack. The endpoint security stack includes everything from the device, up through the firmware, to the operating system, and the software installed on the device. Working with a trusted cloud service provider who can help you manage and deploy updates across the entire endpoint security stack will reduce the complexity of managing a diverse endpoint environment.

Consider the connection between browsers and APIs in your endpoint strategy. Browsers and APIs are the two closest interfaces between users and cloud resources. Working with a single vendor who can provide support for both sides of this communication channel will ensure enhancements are available compatibly and in parallel.

Resilience is a key factor in protecting user data. Each layer of the endpoint security stack presents a potential avenue for attack. Endpoint security requires a top-down approach for containing threats starting with concepts such as same-origin policy for protecting user browsing data, process isolation, verified boot, and trusted base configurations to which an endpoint can be recovered. Ensure your endpoint security strategy has considerations for each of these protections to ensure the resilience of your endpoint in protecting user data.

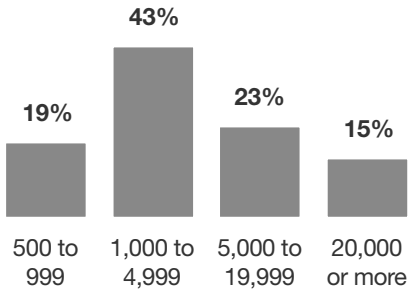
Leverage cloud provider security expertise. Cloud providers manage bare metal to provide the cloud abstraction that many organizations rely on. Securely managing these devices requires top talent and world-class expertise that cloud providers expose to you through endpoint tools and integrations. When considering protections for your cloud environment, your cloud providers may be able to provide better tooling and expertise in the environment they are managing than specialist third parties.

Appendix A: Methodology

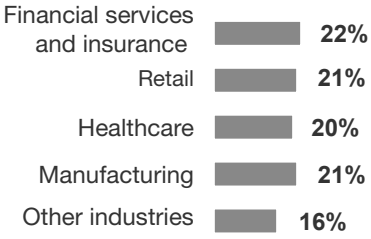
In this study, Forrester conducted an online survey of, 1,221 respondents at enterprise organizations in North America (US and Canada), EMEA (UK, Germany, France, Italy, and Netherlands), APAC (Japan, India, and Australia), and Latin America (Brazil and Mexico) to evaluate endpoint security trends and technologies, as well as security monitoring trends and technologies. Survey participants included security decision makers in IT and security/risk roles. Questions provided to the participants explored endpoint and monitoring priorities, approaches, pain points, and technology needs. Respondents were offered a small incentive as a thank you for time spent on the survey. The study began in June 2017 and was completed in July 2017.

Appendix B: Demographics/Data

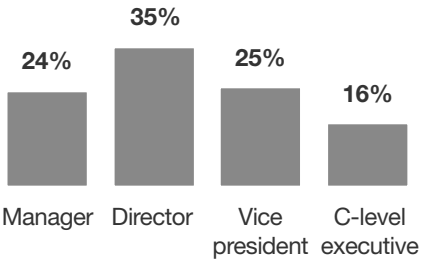
Company size



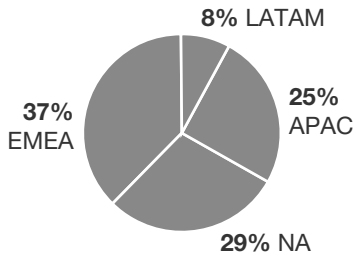
Industry



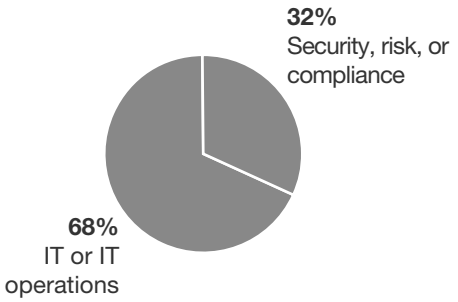
Respondent level



Region



Role



100% of surveyed companies are currently using SaaS, IaaS, PaaS, or private cloud services.

Base: 1,221 IT security decision makers at global enterprises that use cloud services
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Google, July 2017

FORRESTER®

Appendix C: Supplemental Material

RELATED FORRESTER RESEARCH

"The Top Security Technology Trends To Watch, 2017," Forrester Research, Inc., April 26, 2017.

"Top Cybersecurity Threats In 2017," Forrester Research, Inc., January 26, 2017.

"The 2016 State Of Endpoint Security Adoption," Forrester Research, Inc., April 25, 2016.

Appendix D: Endnotes

[1] Source: "Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2016," Forrester Research, Inc., February 15, 2017. The 2 billion records noted also incorporate an updated estimate of 1 billion records for the Yahoo breach, discovered in 2016. See: "Protect Your Intellectual Property And Customer Data From Theft And Abuse," Forrester Research, Inc., July 12, 2017.

[2] Base: 225 security decision makers at global enterprises with 1,000 or more employees. Source: Forrester Data Global Business Technographics Security Survey, 2017.

[3] In North America and EMEA, the proportion of enterprises with 1,000 or more employees using public cloud services rose from 15% to 33% from 2014 to 2016. Source: "Benchmark Your Enterprise Cloud Adoption," Forrester Research, Inc., January 3, 2017.

[4] Source: "Planning For Failure: How To Survive A Breach," Forrester Research, Inc., September 9, 2016.

[5] Source: "The State Of Enterprise Mobile Security: 2016 To 2017," Forrester Research, Inc., January 12, 2017.

[6] Base: 1,983 information workers at global financial services, manufacturing, healthcare, and retail enterprises. Source: Forrester Data Global Business Technographics Telecommunications And Mobility Workforce Survey, 2016.

[7] Source: "The Cloud Security Market Grows From $1.5 Billion In 2017 To $3.5 Billion In 2021," Forrester Research, Inc., July 6, 2017.