A Forrester Consulting
Thought Leadership Paper
Commissioned By Absolute

March 2021

Take A Proactive Approach To Endpoint Security

Endpoint Resilience Has Become A Critical Capability As Workforce Dynamics Change

FORRESTER®

Table Of Contents

Project Director:
Vanessa Fabrizio,
Market Impact Consultant

Contributing Research:
Forrester's Security & Risk
Management research group

FORRESTER®

Executive Summary

The digital age was changing the security landscape long before the COVID-19 pandemic; it simply accelerated the arrival at an unavoidable destination.

The security landscape has become increasingly complex with the realities of digital transformation and the need for immediate work-from-home (WFH) solutions ushered in by the COVID-19 pandemic. Subsequently, threats to endpoint devices have become more prevalent.

In response, many businesses are redefining in-office guidelines and allowing their employees to work from home. This means corporations can no longer solely rely on network and perimeter-based security controls. Instead, they need to increase focus on securing the actual endpoint devices. Decision-makers must consider investments that improve their firm's endpoint security by providing visibility and control that can ensure the protection of devices, data, and applications in this new era.

As a result, there is need to maintain visibility and control over remote endpoints. The ability to maintain a secure connection regardless of location or network environment defines the concept of endpoint resiliency, which is an emerging theme in today's complex IT environment. Firms are focused on improving proactive security approaches and automation of security controls that drive a higher quality of protection and increase their levels of endpoint resiliency.

Absolute commissioned Forrester Consulting to evaluate endpoint security practices and the challenges associated with endpoint resiliency. Forrester surveyed 157 IT and security decision-makers responsible for endpoint protection to explore this topic. We found:

KEY FINDINGS

› **Endpoint security has evolved with increased WFH and hybrid work policies.** Firms are refocusing their security priorities to match the realities of remote working. In the next year, they are specifically focused on automating the protection of sensitive or at-risk data, geolocation, and security control health.

› **Security leaders are facing new endpoint security challenges.** As the world migrates to a new work-from-anywhere environment, firms' priorities are shifting. It's no longer an option to deprioritize risk associated with endpoint devices. Surveyed security leaders said their top challenges are maintaining compliance, enforcing security standards, and understanding the health of security controls.

› **Security leaders struggle to measure the ROI of their firms' existing security investments.** Only 38% of respondents said they can measure the ROI of their firm's security investments. To accurately determine ROI, decision-makers need overarching visibility into the health and function of the security controls installed on their firm's endpoints. Otherwise, it makes it difficult to make decisions about future investments.

› **Endpoint resiliency is the solution.** Sixty-six percent of respondents said they believe that securing modern business environments requires a proactive approach to endpoint resiliency. Decision-makers said endpoint resilience would provide benefits such as improved data and device visibility and stronger protection of sensitive data.

Endpoint Security Evolves With Increased Remote Work

Endpoint devices are a workforce productivity standard that has increased since the beginning of the pandemic. Sixty-six percent of respondents indicated that their firm's use of endpoint devices has increased since the pandemic began. The enhanced reliance on endpoint devices has changed the way security leaders operate. In surveying 157 IT and security leaders, we found that:

- **Firms reassessed their policies and capabilities as a result of the COVID-19 pandemic.** Decision-makers reevaluated their firm's security policies (82%), secured remote-access capabilities (76%), and extended visibility and measurement capabilities (71%).
- **Firms reprioritized automation efforts.** In the next year, automation efforts will focus on sensitive or at-risk data (60%), geolocation (52%), security control health (48%), web-based application usage (36%), patch management (35%), and hardware inventory (32%). These are all critical areas when dealing with remote workers. This is a dramatic change from previous automation strategies when firms had a greater focus on in-office workers and network security.

76% of respondents indicated their firm's use of endpoint devices increased since the beginning of the COVID-19 pandemic.

Figure 1

"Which endpoint data points are you planning to monitor automatically within the next 12 months?"

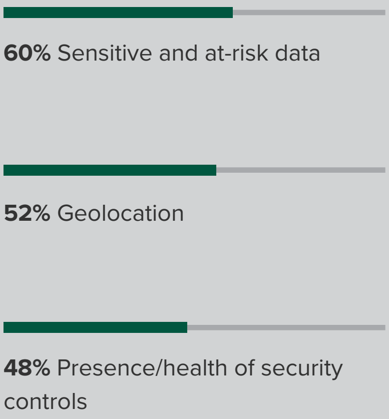
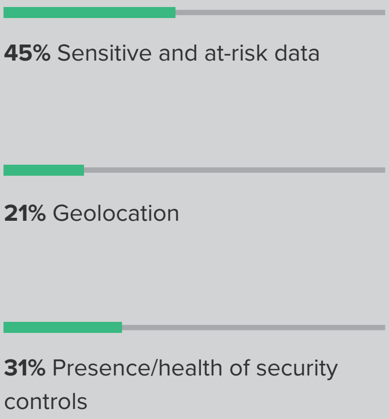


Figure 2

"Which endpoint data points are you able to automatically monitor, (2020)?"



Base: 157 IT security decision-makers responsible for endpoint protection
Source: A commissioned study conducted by Forrester Consulting on behalf of Absolute, December 2020

In the next year, firms are focusing their automation efforts on sensitive or at-risk data, geolocation, and security control health.

Security Leaders Face New Endpoint Security Challenges

Securing and managing remote endpoints has historically been challenging for organizations. Prior to the pandemic, firms acknowledged endpoint security risk, but they focused more on network security strategies. Now, with the rapid increase in remote workers, priorities have evolved to focus on securing remote endpoint devices. Decision-makers understand the urgency, but their firms face new challenges as they strive to improve the security of their endpoint environments. We found:

- **The need for visibility has increased with remote work.** Security respondents said that prior to the COVID-19 pandemic, their firms' main endpoint security challenge was threat identification. Today, the most significant challenge is securing their firms' remote workforce. Respondents also said maintaining compliance, enforcing security standards, and understanding the health of security controls are top concerns (see Figure 3).
- **Security leaders need measurable investments.** As the security landscape evolves, so must security investments. However, respondents said their firms struggle to measure ROI. Only 38% of surveyed security leaders said their firm can measure the ROI of its security investments, and 31% disagreed entirely (see Figure 4).

  The inability to measure ROI is directly linked to firms' endpoint visibility. To determine the efficiency of their investments in security controls, decision-makers must be able to measure the efficacy of the controls, which requires overarching visibility into their firm's status and health.

Only 38% of surveyed security leaders said they could measure the ROI of their firm's security investments.

Figure 3

"What were/are your biggest endpoint security challenges?"

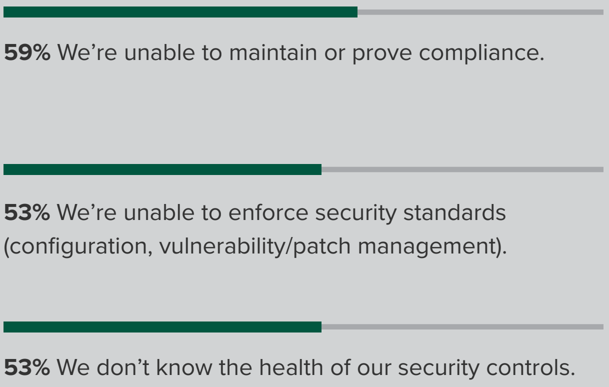
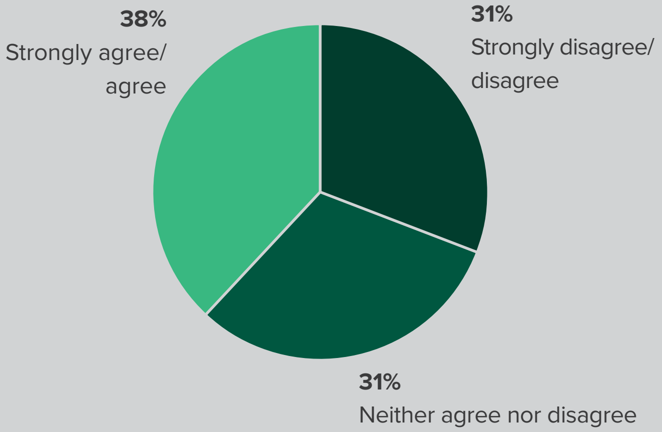


Figure 4

"How much do you agree with the following statement?"

I can measure the ROI of my security investments.



Base: 157 IT security decision-makers responsible for endpoint protection
Source: A commissioned study conducted by Forrester Consulting on behalf of Absolute, December 2020

Modern Business Environments Require Resilient Endpoints

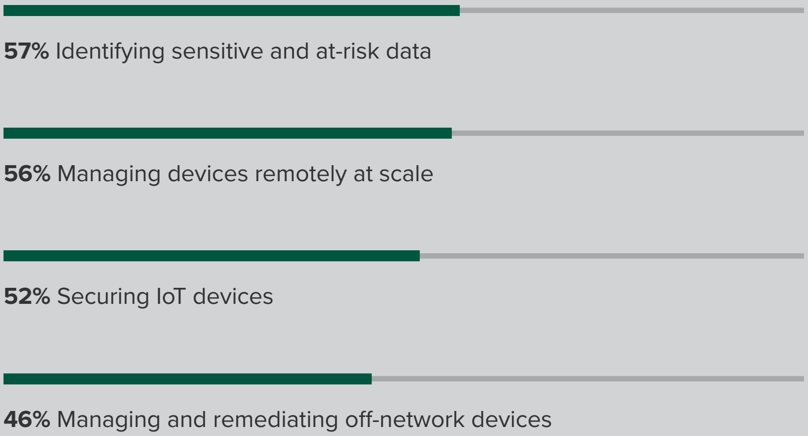
It’s not debatable: Organizations must evolve to meet the demands of changing business environments. When evaluating how best to secure their workforces today, 66% of respondents identified taking a proactive approach to endpoint resilience as a requirement. Leaders cited the following capabilities as most critical:

- **Visibility and control of all endpoint devices.** Respondents said having the ability to identify sensitive and at-risk data and to manage devices remotely at scale would make their firm’s endpoint management more effective (see Figure 5). Decision-makers are looking to ramp up capabilities that support a remote workforce.
- **Security and control of sensitive data.** It is not enough to merely identify data; companies must be able to monitor its state and take action as required. Improving endpoint data management is the number one benefit respondents expect from investing in endpoint resilience.

55% of respondents said that they believe endpoint resilience would help secure sensitive and corporate customer data.

Figure 5

“Which capabilities would make your endpoint management more effective?”

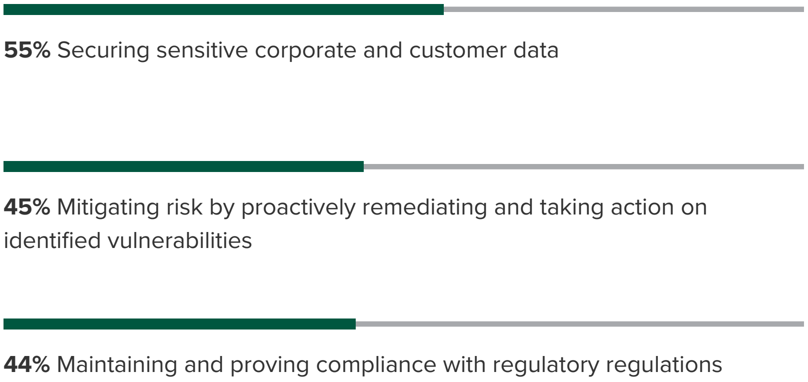


Base: 157 IT security decision-makers responsible for endpoint protection
Source: A commissioned study conducted by Forrester Consulting on behalf of Absolute, December 2020

66% of respondents said they believe securing modern business environments requires a proactive approach to endpoint resilience.

Figure 6

“Which business benefits do you think endpoint resilience would provide to your organization?”



Base: 157 IT security decision-makers responsible for endpoint protection
Source: A commissioned study conducted by Forrester Consulting on behalf of Absolute, December 2020

Key Recommendations

Forrester's in-depth survey of IT and security leaders about endpoint security yielded three important recommendations:

Endpoint resilience starts with reliable endpoint visibility and control. Maintaining a trusted connection with your endpoints is required to detect unsafe behaviors or conditions that could put sensitive data at risk. This includes having visibility and control of the endpoint hardware, operating system, applications, and data gathered on the device; and having the ability to self-heal the device, mission-critical security controls, and productivity applications. Using network security solutions alone is inadequate.

Ensure endpoint misconfigurations are automatically repaired when possible. Do not assume that the health of your IT controls or security tools installed on your employees' endpoints will remain stable over time. Endpoints that are taken out of the office for extended periods of time and those that lack a reliable connection can easily drift from previously established secure configuration baselines and open new vulnerabilities for attackers to exploit. For example: Security agents often fail and stop communicating with their central management servers. Automating the frontline endpoint security configuration tasks and repairs is a critical component to endpoint resilience.

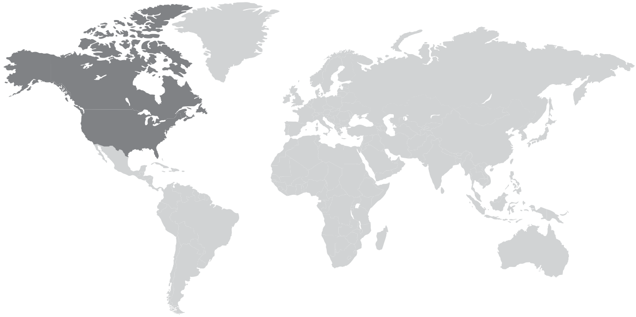
Focus on ROI in all new security purchases. Once you have a strong connection to your endpoints and a better understanding of the health of your hardware and software, you can more accurately determine the ROI of your security purchases. Organizations typically have a litany of endpoint security and management agents to contend with, and each new product introduced can serve as both a potential risk and an operational burden. Focus on and maintain continuous endpoint visibility so you can ensure that controls are always working as intended. By doing this, you will ensure the ROI of your security investments — both from risk reduction and operational perspectives.

Appendix A: Methodology

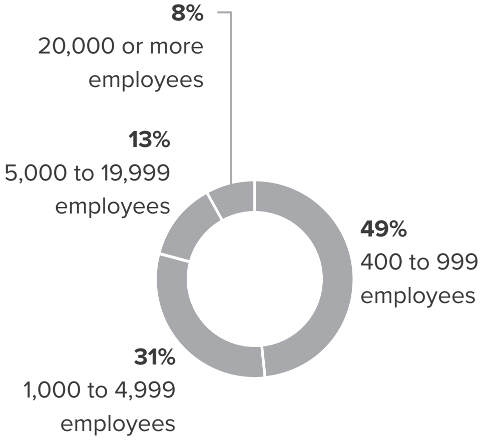
In this study, Forrester interviewed 157 IT and security respondents in the United States and Canada to evaluate their firms' endpoint resilience practices and challenges. Survey participants included decision-makers in endpoint protection. Respondents were offered a small monetary compensation as a thank you for time spent on the survey. The study began in November 2020 and was completed in December 2020.

Appendix B: Demographics

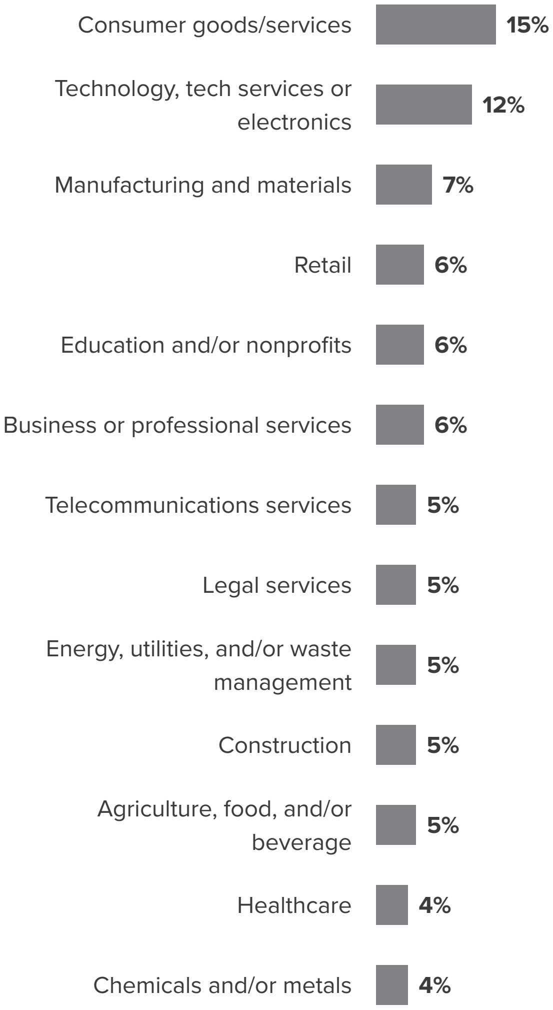
COMPANY LOCATION



COMPANY SIZE



INDUSTRY



Base: 157 IT security decision-makers responsible for endpoint protection
Source: A commissioned study conducted by Forrester Consulting on behalf of Absolute, December 2020