# Identity and Access Management


Summary Results | February 2019

# Survey Summary

- Between October 2018 and February 2019, Gatepoint Research invited selected executives to participate in a survey themed *Identity and Access Management*.
- Candidates from the 2018 Americas Target Accounts were invited via email and 110 executives have participated to date.
- Management levels represented are predominantly IT and security senior decision makers: 10% hold the title CxO, 10% are VPs, 37% are Directors, and 43% are Managers.
- Survey participants represent firms from a wide variety of industries including business and financial services, healthcare, media, manufacturing (primary, general, and high tech), public administration, retail and wholesale trade, telecom services, transportation, and utilities.
- Responders work for firms with a wide range of revenue levels:
  - 76% work in Fortune 1000 companies with revenues over $1.5 billion;
  - 8% work in Mid-Market or Large firms whose revenues are between $250 million and $1.5 billion;
  - 16% work in Small companies with less than $250 million in revenues.
- 100% of responders participated voluntarily; none were engaged using telemarketing.

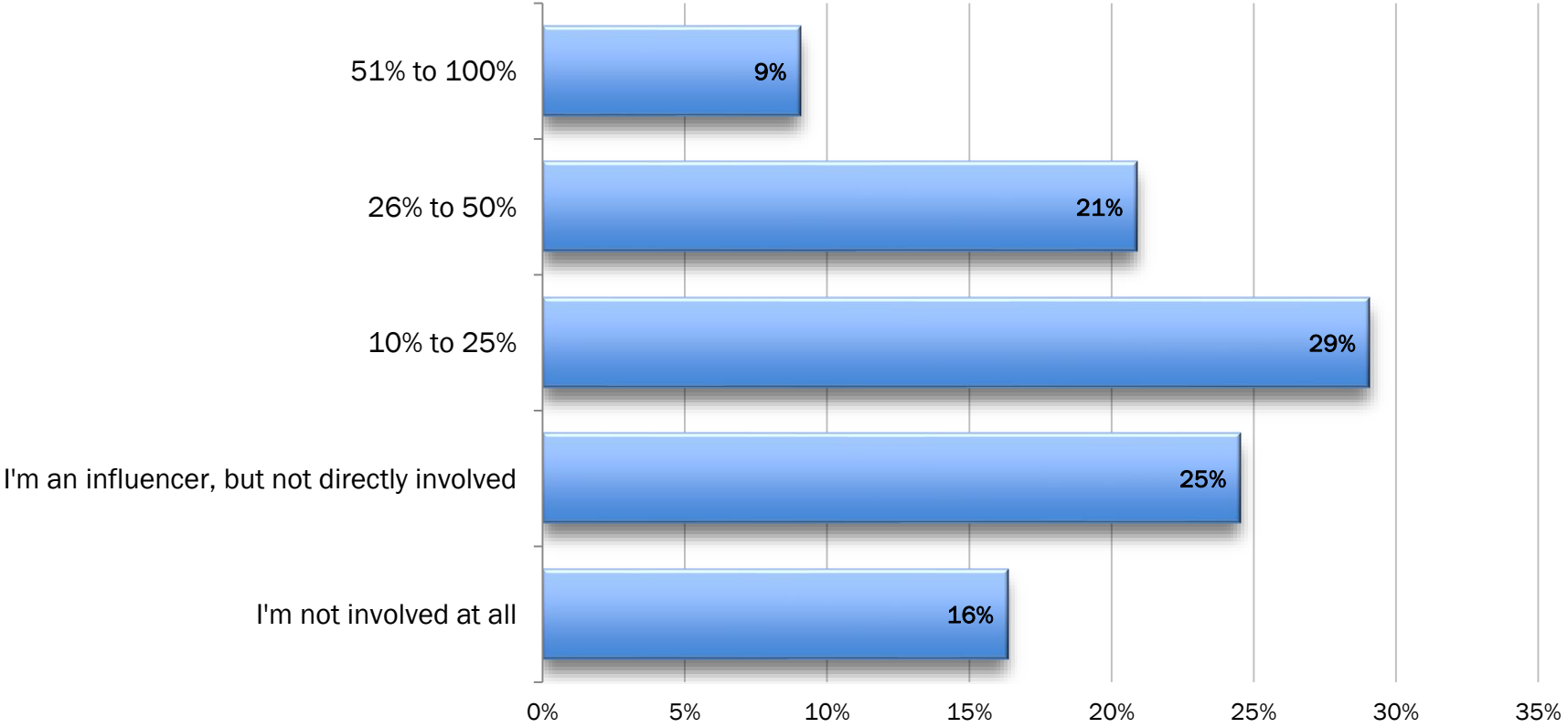
# Executive Overview

Who are you, and are you really who you say you are? Detecting authenticity has become more complicated than ever. The need to capture, identify, and ultimately authenticate users protects customers' and employees' identities from potential harm. What are organizations doing to ensure the highest level of security?

This survey asks respondents to report:

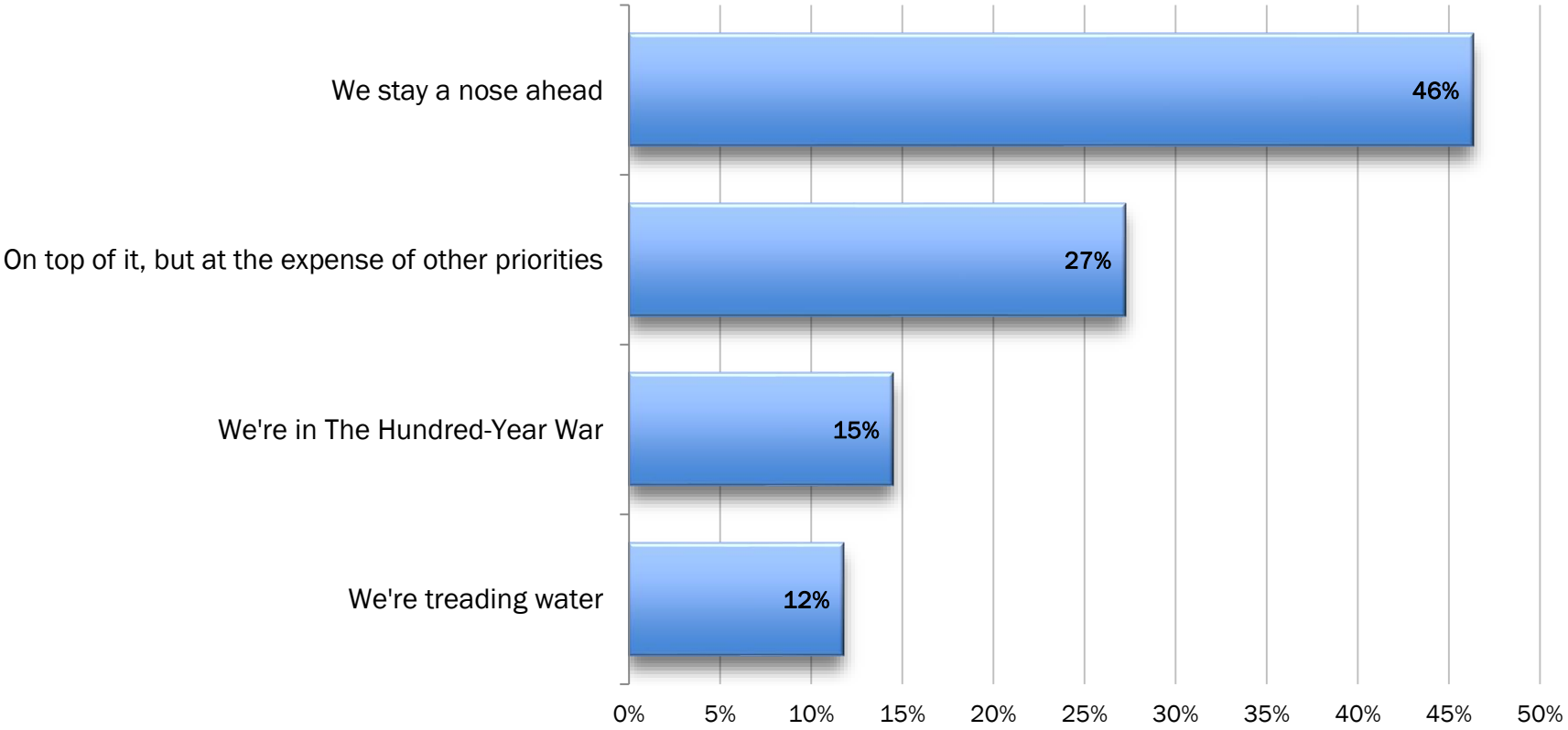
- How are they currently performing against threats and attacks?
- What software are they using? Can it identify and authenticate users? Which types of users?
- How confident are they that their current system can continue protecting them against future hacking technology??
- What concerns them most about security threats to their organization?
- What features are most important when considering new identity and authentication software?

# What percent of your job is dedicated to digital identity security?



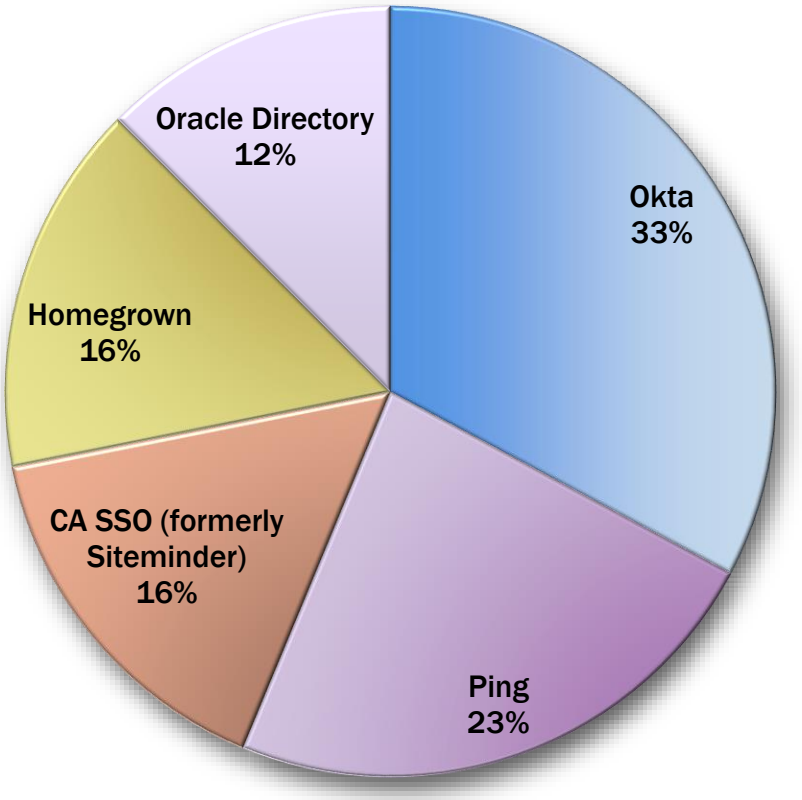

**All but 16% of respondents are either influencers in their organization's digital identity security, or are directly involved in the work.**

# What best describes your organization's efforts against security attacks?



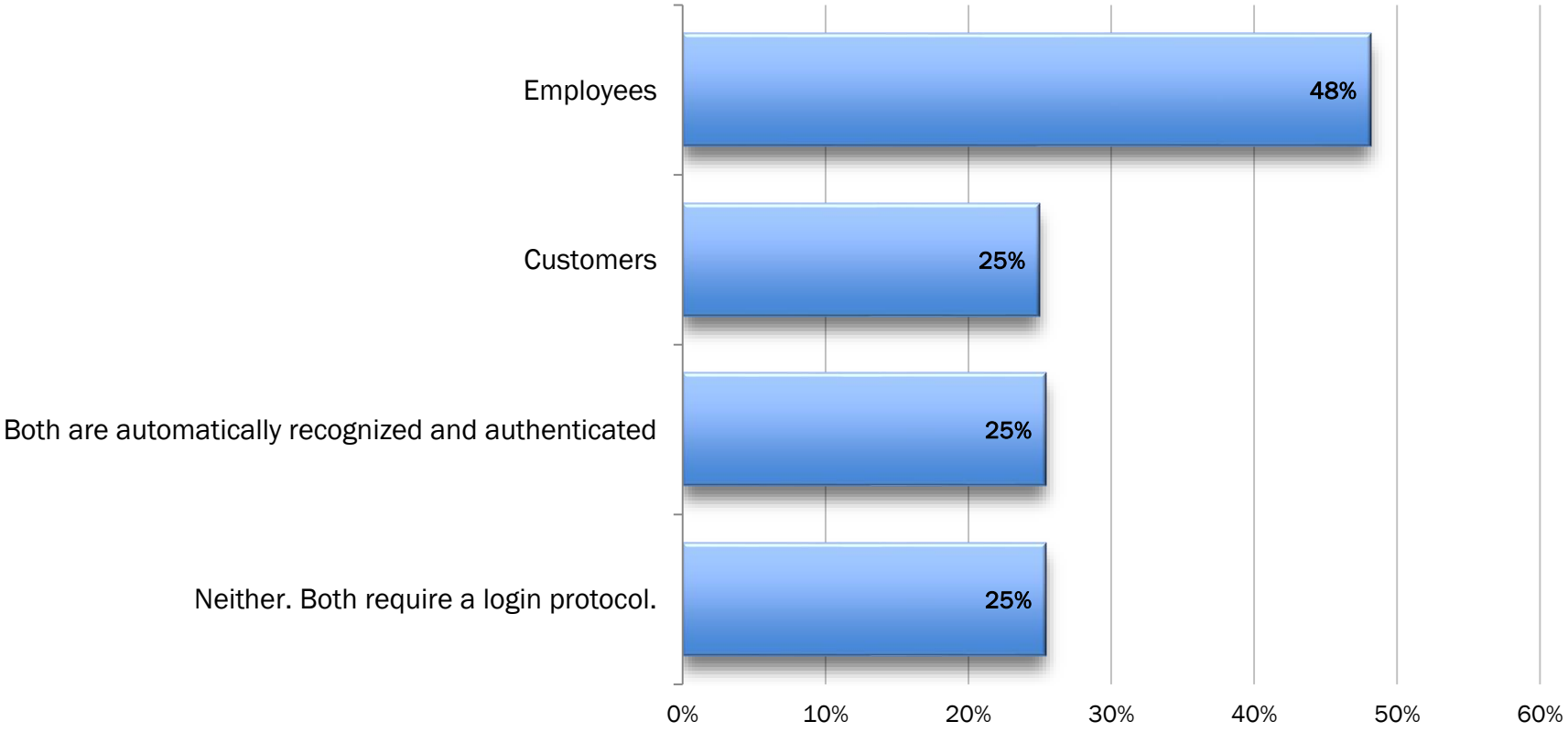

**Most respondents (73%) feel their security protocols are competently thwarting security attacks, yet 27% of those say it's at the expense of other business priorities. 15% wearily say it's a constant battle, while the rest (12%) are just treading water.**

# What identity and access management systems does your organization use?




A third of respondents report they use Okta identity and access management system, a 10-point edge over the next most popular, Ping. 16% use CA SSO or have a homegrown system, and 13% use Oracle Directory.

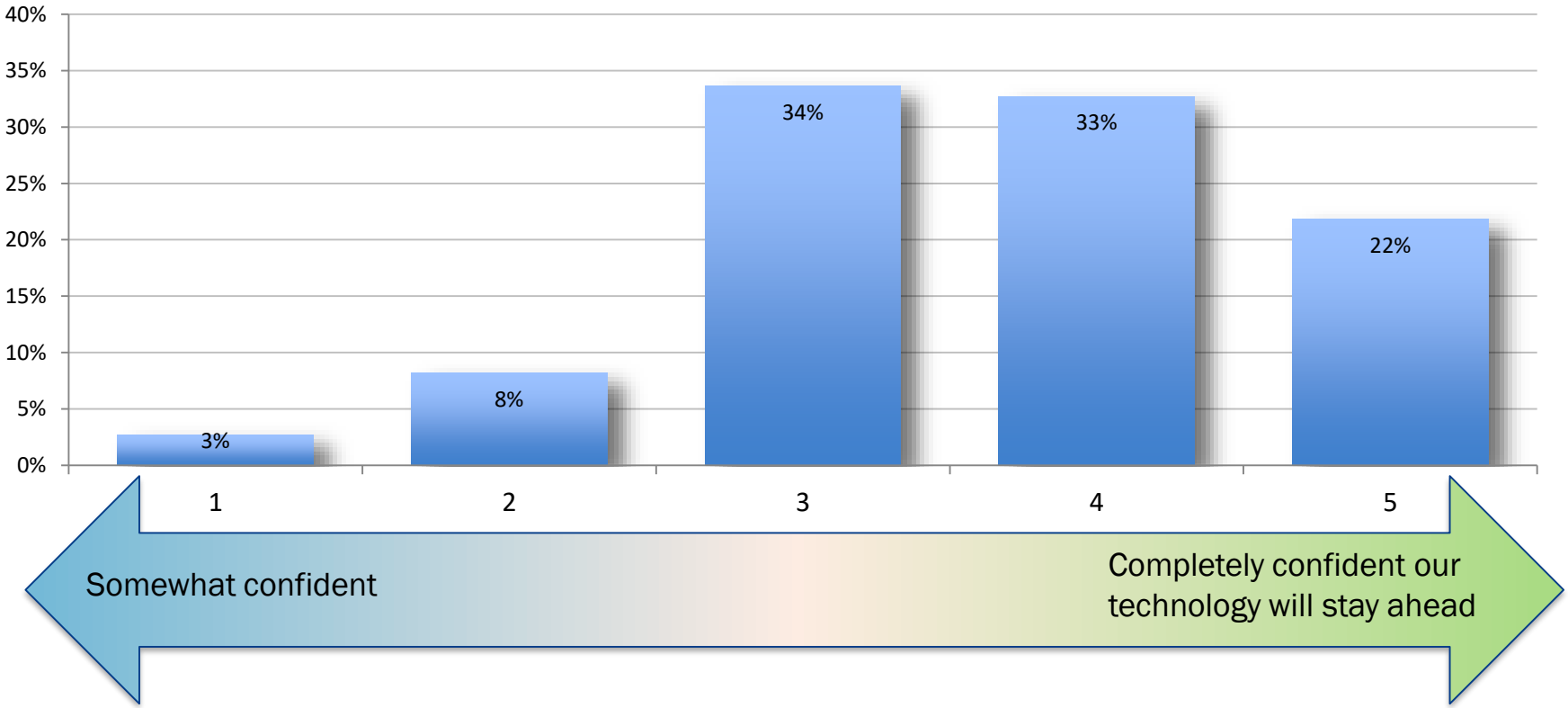
# Which users can your identity management system automatically recognize and authenticate?




**While nearly half of respondents' systems can automatically recognize and authenticate employees, and 25% can recognize and authenticate customers, a fourth of those surveyed require login protocol for both employees and customers.**

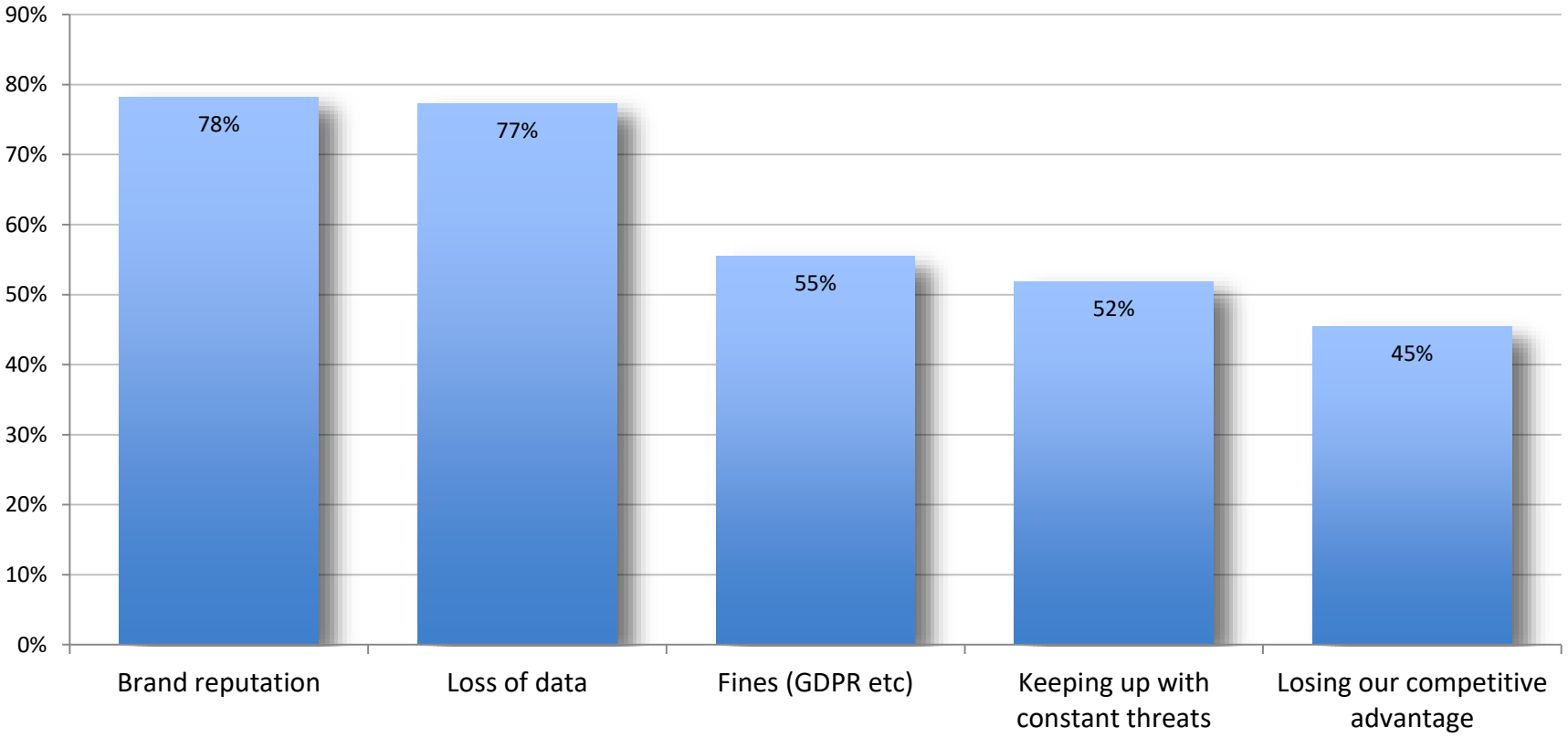
# Are you confident that your identity protection systems will continue to deter sophisticated hacking efforts?

**(Rate 1 to 5, 1 = somewhat confident, 5 = completely confident our technology will stay ahead)**



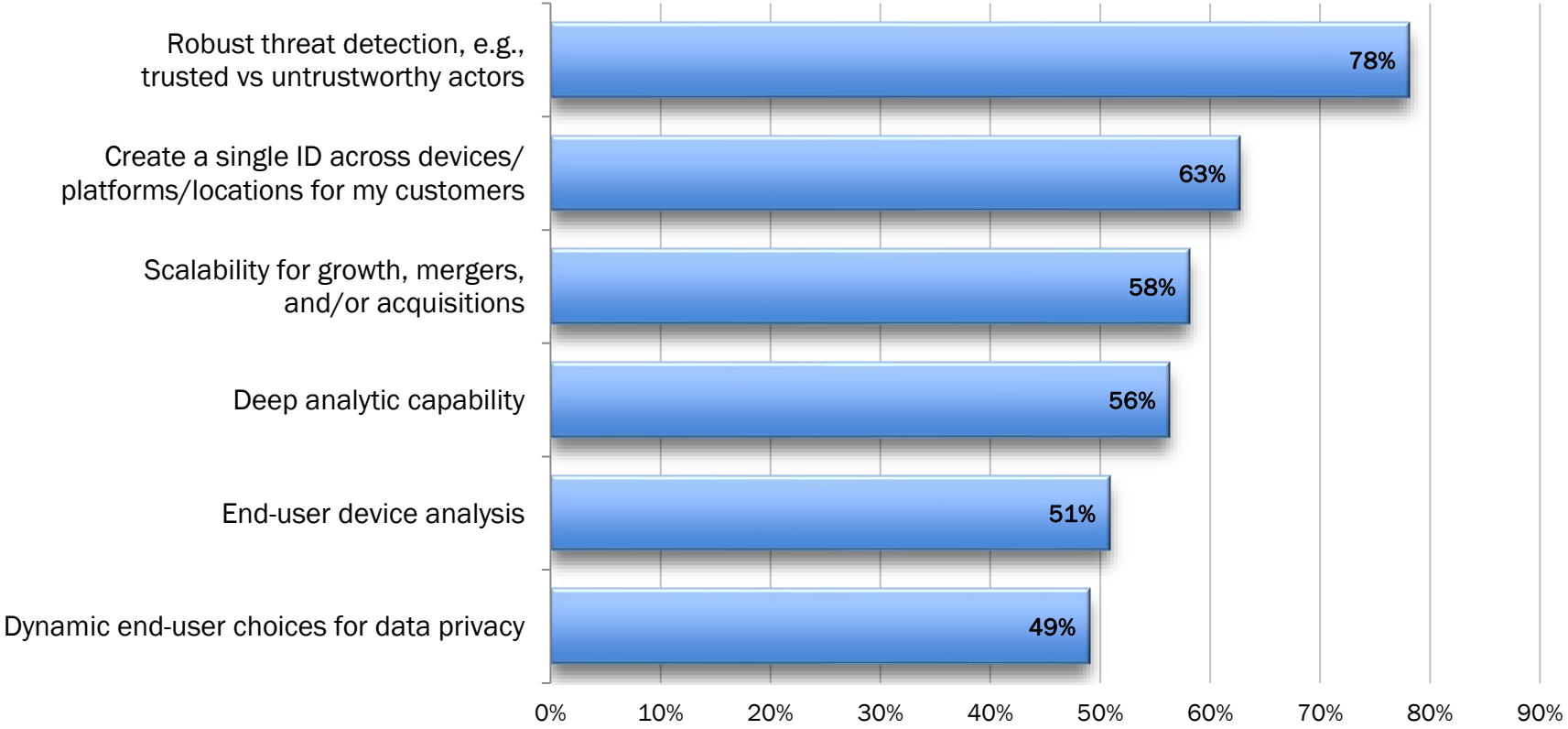

**Just 22% of respondents have the highest confidence in their technology's ability to stay ahead of sophisticate hacking efforts, but fully two thirds have high confidence. 11% report lower confidence.**

# What concerns you most about a digital identity security breach?



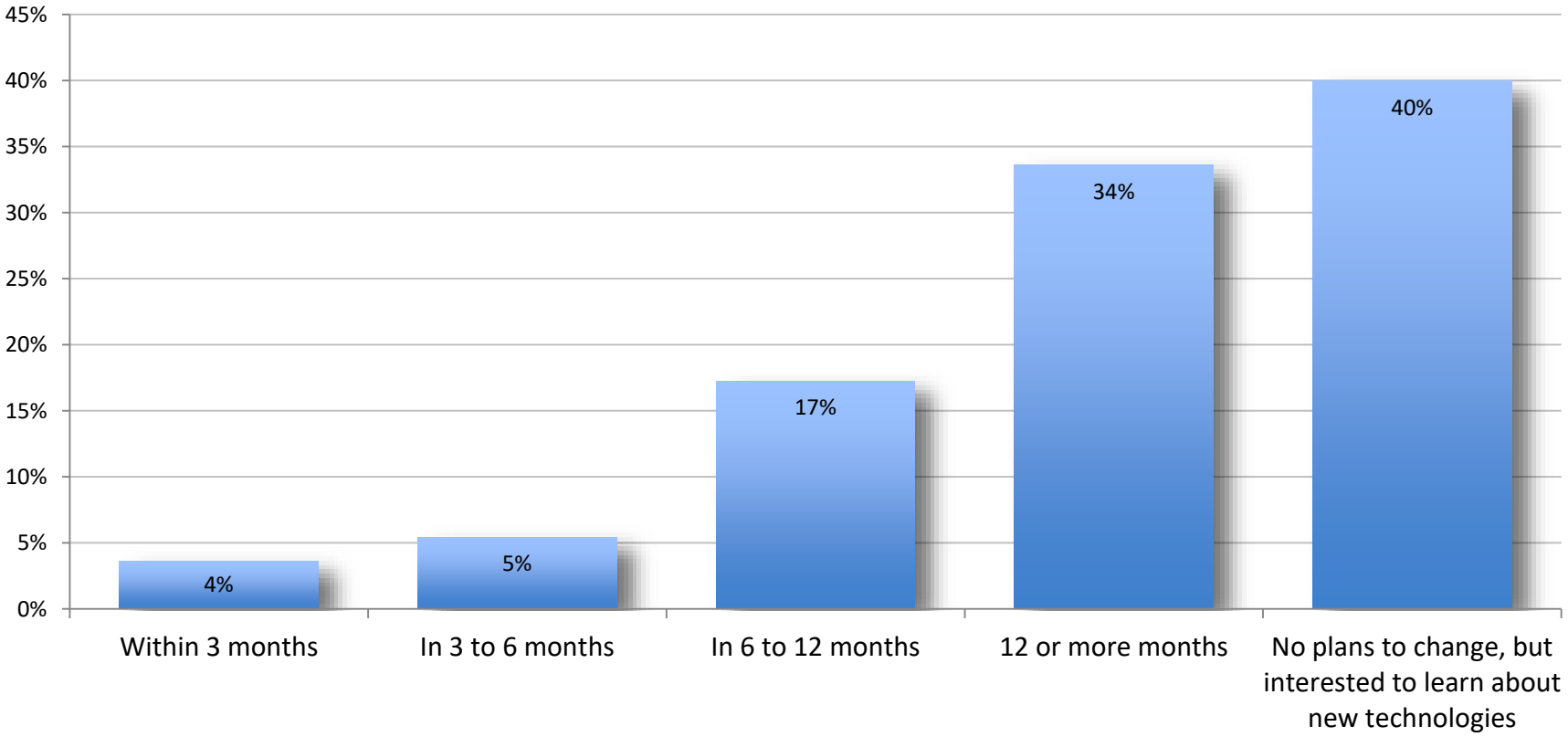

**Tarnishing their brand's reputation and loss of data keep three fourths of respondents awake at night. More than half also worry about non-compliance fines, and keeping up with constant hacking threats.**

# When considering a new identity and access management system, what features are must haves?



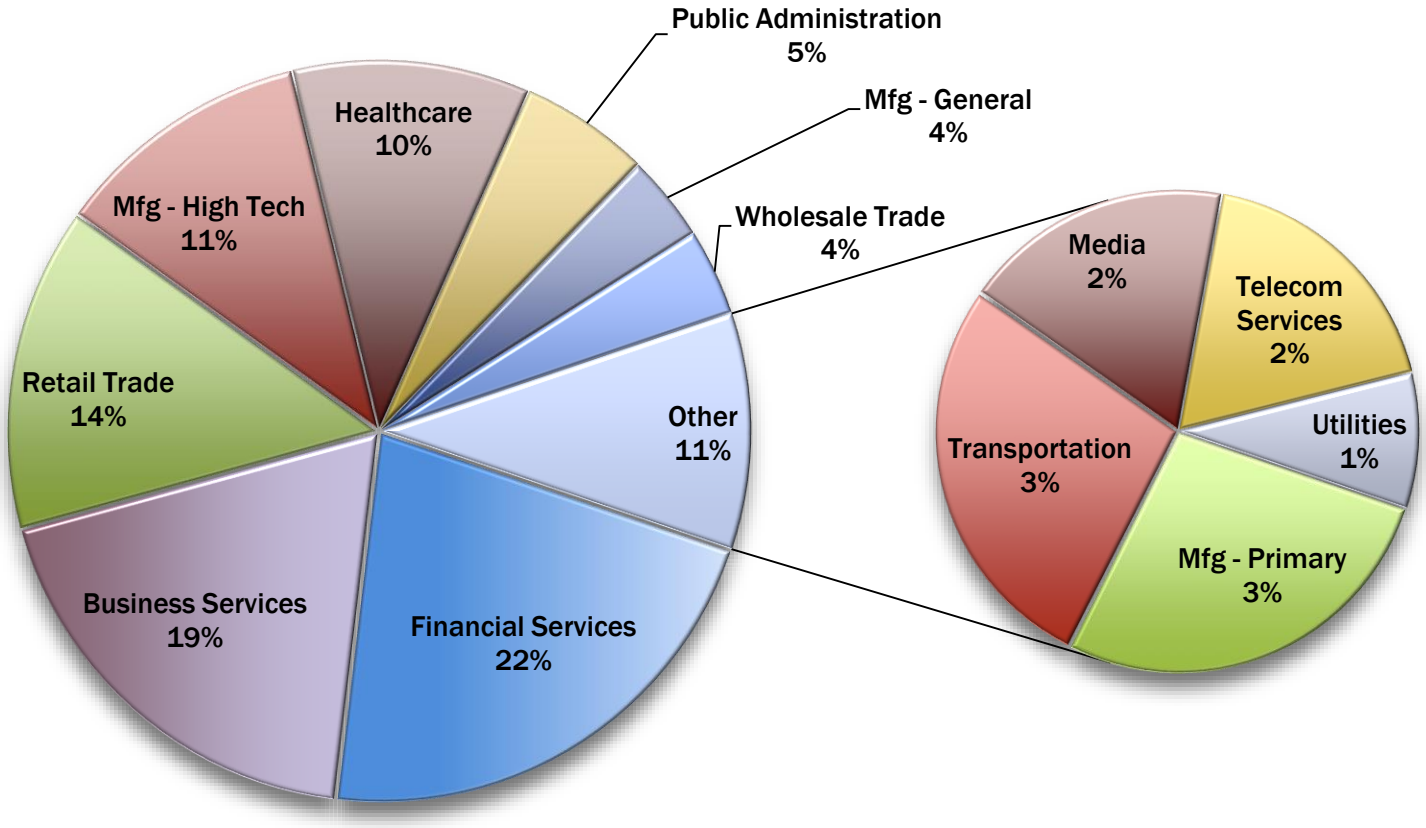

**The majority (78%) of those surveyed insist an upgrade or new system must include robust threat detection. Other must haves, in priority order: single sign on ID, scalability, analytics, end user device analysis, and data privacy choices.**

# When are you planning to refresh, upgrade or replace your current identity and access management system?



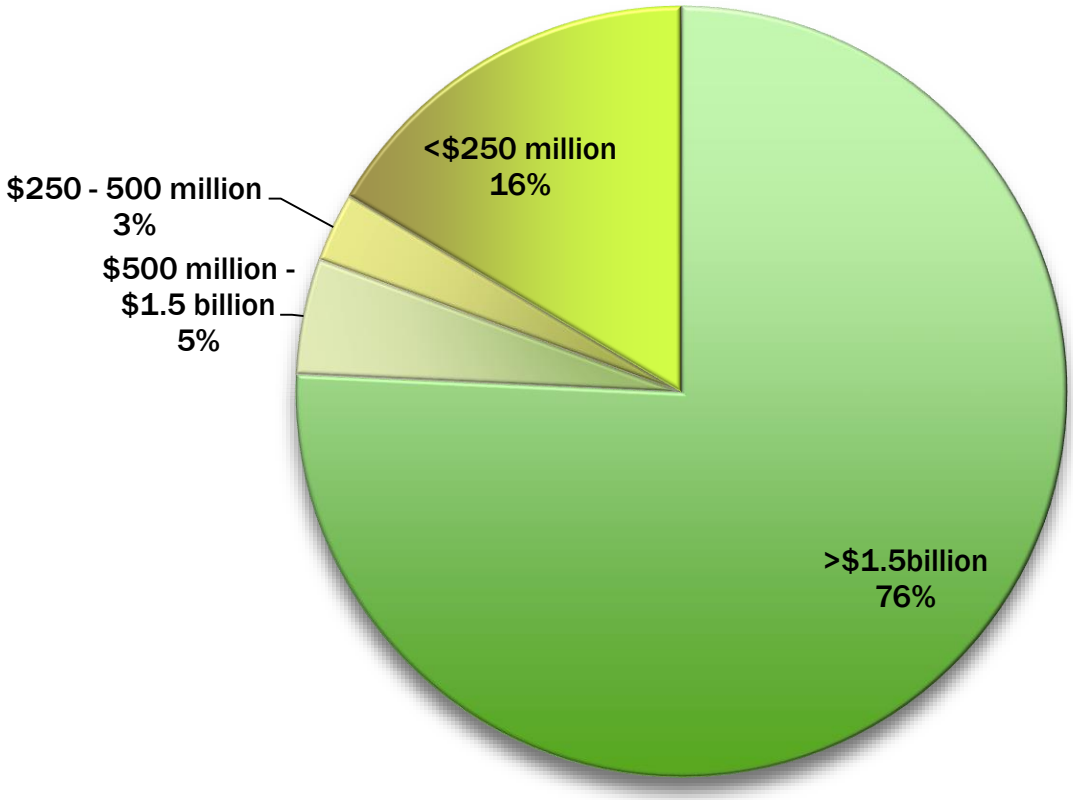

**26% of respondents plan to improve their current identity and access management system within the next 12 months. 34% say such action is likely to take place in the more distant future. Those with no plan in place say they'd like to know more about new technologies.**

# Profile of Responders:
# Industry Sectors



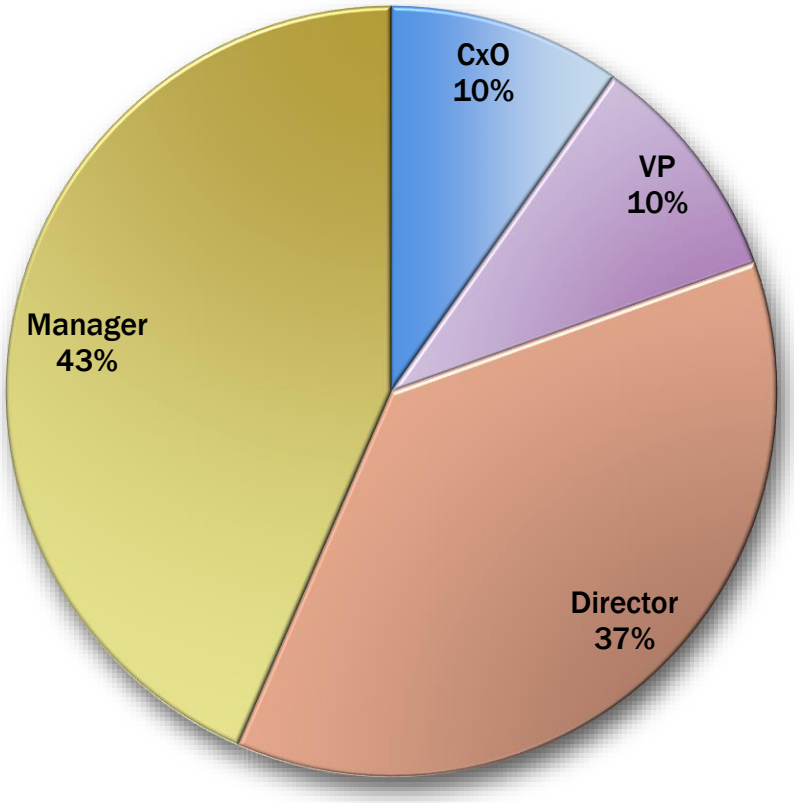

**Responders represent a wide variety of industries.**

# Profile of Responders:
# Revenue




**76% of those surveyed work in Fortune 1000 companies with revenues over $1.5 billion.**

# Profile of Responders:
# Job Level




**57% of those surveyed hold director or executive level positions in their organizations.**


ForgeRock offers a unified platform for both employees and consumers, identity and access management for the Internet of Things, customer, cloud, mobile, and enterprise environments.

[Learn more at forgerock.com]