ESG Research Insights Paper

The Role of the Trusted Data Center as the Secure Foundation for Midmarket Success

How Best Practices in Data Center Technologies and Management Lead to Reduced Risk, Increased Uptime, and Business Success

By Adam DeMattia, Director of Research; Scott Sinclair, Senior Analyst; and Jennifer Gahm, Senior Project Manager

November 2019

This Research Insights Paper was commissioned by Dell Technologies and Intel Corporation and is distributed under license from ESG.

Contents

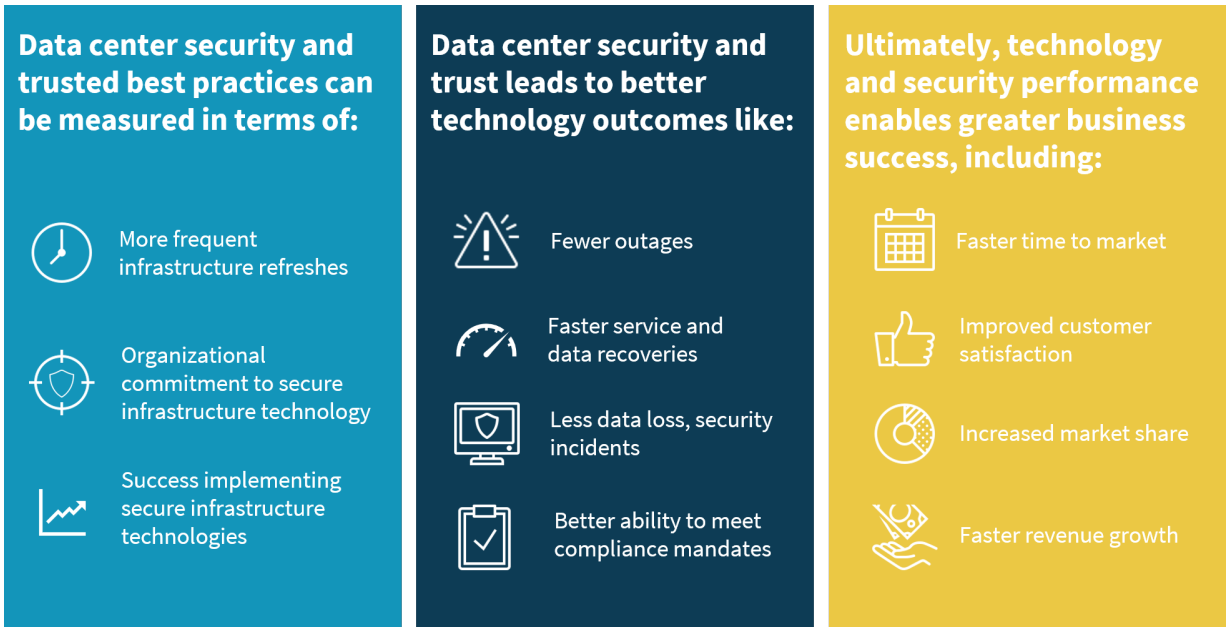
Executive Summary 3
Midmarket Landscape and Role of a Trusted Data Center 4
The Current State of Trusted Data Center Maturity in the Midmarket 5
The Importance of Operating a Trusted Data Center 6
Preventing Security Events and Maintaining Compliance 6
Minimizing Outages and Cost of Downtime 8
Reducing the Total Cost of Downtime with a Trusted Data Center 10
Technology Outcomes Fuel Business Advantages for Leaders 10
Improving Business Agility with a Trusted Data Center 10
Delighting Customers with a Trusted Data Center 11
A Trusted Data Center Is the Cornerstone of Midmarket Growth 12
The Bigger Truth 12
Learning from Leaders 12
How Dell Technologies Can Help 15
Appendix I – Research Methodology and Respondent Demographics 16
Appendix II – Criteria for Evaluating Organizations' Trusted Data Center Maturity 19

Executive Summary

Midmarket firms face many of the same data center security risks as their enterprise counterparts with far fewer resources at their disposal to mitigate them. Downtime, data theft, and regulatory non-compliance all pose existential threats to these organizations and as they drive for continuous innovation and advantage in an increasingly competitive landscape, they must ensure valuable data and IT assets are secure, protected, and available at all times.

How can midmarket organizations succeed in the face of these challenging market dynamics? This Research Insights report shows that the success organizations have enjoyed varies greatly, and further that organizations enjoying the greatest success demonstrate a clear organizational commitment to prioritizing security and operate fundamentally more secure data center environments. Figure 1 illustrates the relationship between secure data center technologies, improved security outcomes, and, ultimately, business success.

Figure 1. Relationship Between Trusted Data Center Best Practices and Technology and Business Results



Source: Enterprise Strategy Group

This relationship between data center security and business success was measured and validated by ESG's primary research capturing the perspectives of 1,650 strategic IT decision makers.

Key technologies inspected in the research include modern storage and server infrastructure, data security features like encryption, embedded firmware security capabilities, and data protection practices like backup frequency and replication. The remainder of this report details the segmentation criteria ESG used to group organizations into three categories (*Leaders, Followers,* and *Laggards)* and it also discusses the specific differences in technology and business performance between categories. For example, *Leaders*:

- Experienced 71% fewer security incidents and non-compliance events over the past 12 months than *Laggards.*
- Experience 42% fewer application outages and shrink their typical outage duration by 81% relative to *Laggards.*
- Reduce their annual cost of downtime by 89% compared to *Laggards.*
- Are 2.1x more likely than *Laggards* to be very successful at launching products to market ahead of competitors.
- Are 80% more likely than *Laggards* to exceed customer satisfaction goals.
- Expect to grow their revenue at 2x the rate of *Laggards* over the next few years.

Midmarket Landscape and Role of a Trusted Data Center

When it comes to IT, midmarket firms are in a uniquely challenging position. They have limited resources to invest in people and technology. This means IT leaders must make tough choices about which technology initiatives to focus on and which skill sets to invest in, and the choices they make often receive intense scrutiny from business leaders. The result is that the IT organization often can't advance all of the projects it would like to at the pace desired, and the staff running these projects is overburdened.

ESG research shows that these IT challenges are particularly acute when it comes to effective and efficient cybersecurity. In a recent survey, ESG asked 210 line-of-business executives to identify the biggest issues they have with their IT organizations' capabilities. Those employed at midmarket firms were more likely than their enterprise counterparts to report they have concerns about the IT organization's ability to provide adequate security and compliance controls. Moreover, at 38%, this was the most frequently cited issue among respondents employed at midmarket organizations. In the same survey, ESG asked respondents in the IT organization which areas of IT they felt had problematic skill shortages. Those employed at midmarket organizations most often reported cybersecurity (46% incidence).[1]

External pressures compound these challenges. Midmarket firms often find themselves battling with larger enterprises for customers. But they can't match these larger competitors dollar-for-dollar when it comes to sales, marketing, or technology, so they must be faster, more efficient, and more customer-centric to hold their own. Also, for many midmarket firms, the midmarket moniker is intended to be temporary. Most of these firms have high-growth aspirations, which again puts an emphasis on efficiency and effectiveness.

So, in the midmarket, data center security is often seen as an IT weak spot. Cybersecurity risk also has the potential to hurt these organizations relative to competitors: Outages can disrupt customer service, data loss saps productivity, and compliance violations often have direct financial consequences. **Midmarket organizations need to prioritize improving the security and dependability of their IT environments. By minimizing the negative business impact of security events, midmarket firms improve their ability to compete and succeed in their markets.**

But how can organizations make the right decisions? What guidelines should they follow? And is there any proof that validates that best practice adherence actually leads organizations to higher levels of technology and business success? ESG set out to answer these questions in a recent research survey of 1,650 IT decision makers at organizations with less than 1,000 employees.[2]

In order to evaluate how best practice adherence is linked to technology and business outcomes in the arenas of security and reliability, ESG developed a Trusted Data Center Maturity framework that put forward three core best practice areas made up of six specific behaviors against which organizations could be assessed:[3]

- **Frequent infrastructure refreshes**—ESG tested organizations to see if they are prioritizing the operation of newer on-premises infrastructure. Newer infrastructure generally includes a host of security and data protection capabilities that older solutions may lack. In short, organizations investing more in infrastructure refreshes are in a better position to drive improved outcomes for their organization. To be considered in adherence with this best practice area, organizations must:
    - Report the average age of their on-premises servers is less than three years.
    - Report the average age of their on-premises storage systems is less than three years.

[1] Source: ESG Master Survey Results, *2019 Technology Spending Intentions Survey*, March 2019.
[2] See Appendix I – Research Methodology and Respondent Demographics for more information.
[3] See Appendix II – Criteria for Evaluating Organizations' Trusted Data Center Maturity for more information.

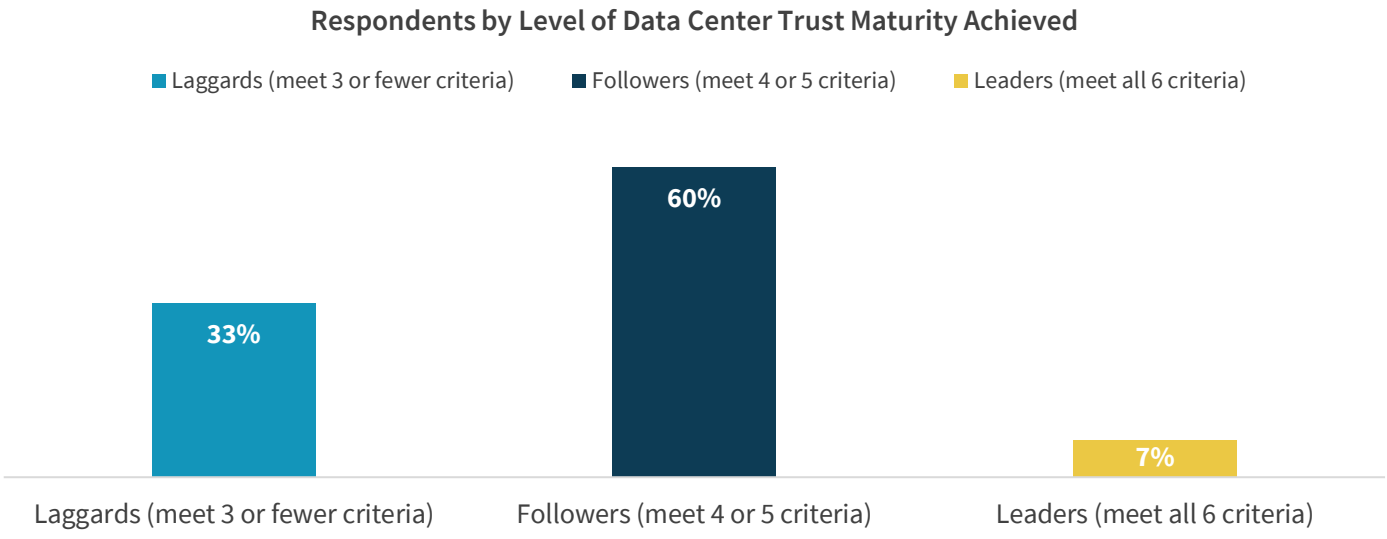
- Organizational commitment to relevant infrastructure technologies—Beyond a commitment to the latest and greatest infrastructure, ESG believes the organization must be committed to specific technology investments related to reliability and security in order to deliver the highest trust environment possible. To be considered in adherence with this best practice area, organizations must:
    - Believe it is important to encrypt sensitive data.
    - Believe it is important to invest in infrastructure solutions with market-leading security capabilities built into their firmware.
- Success acting on organizational commitment to targeted infrastructure investments—For an organization to believe an investment is important is one thing. It is another to actually allocate budget to make those investments real. ESG believes that organizations must not only recognize the importance of targeted investments to enable reliability and security, but also actively invest in these solutions to make secure outcomes real. To be considered in adherence with this best practice area, organizations must:
    - Encrypt sensitive data to protect it from theft or corruption.
    - Replicate sensitive data to secondary storage systems to maximize uptime and recoverability.

Organizations in alignment with all six best practices were placed in the Trusted Data Center "Leader" category. Organizations in alignment with four or five best practices were placed in the Trusted Data Center "Follower" category. And organizations in alignment with three or fewer best practices were placed in the "Laggard" category.

The Current State of Trusted Data Center Maturity in the Midmarket

ESG's analysis found that very few midmarket organizations are in alignment with all of the Trusted Data Center best practices put forward by its framework. In ESG's survey, just 7% of organizations achieved the Leader designation. Three-fifths (60%) of the organizations fell into the Follower category. And one-third (33%) were evaluated as Laggards (see Figure 2). The fact that nearly 5x as many organizations were scored as Laggards as were scored as Leaders shows that midmarket organizations have ample room to improve their level of data center security, reliability, and availability.

Figure 2. Benchmarking Data Center Trust



Source: Enterprise Strategy Group

The Importance of Operating a Trusted Data Center

Why does Trusted Data Center Maturity matter? In short, ESG's research showed that Trusted Data Center Leaders enable vastly superior security, availability, and business outcomes than their less mature counterparts.

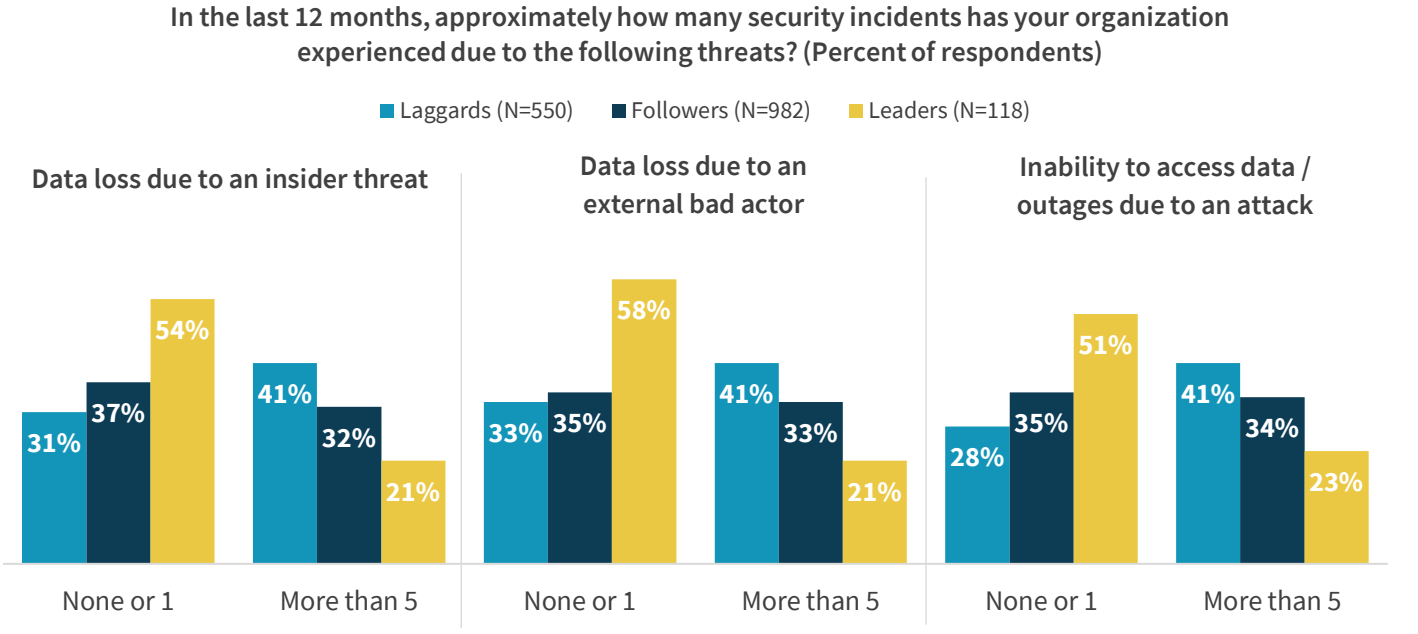
With respect to security and availability outcomes, ESG found that Leaders operate more reliable, resilient, and hard-to-compromise environments. As a group, they experience quantifiably fewer security incidents resulting in data loss or compromise, fewer instances of non-compliance with either internal governance or regulatory mandates, and fewer outages, which they recover from faster. In turn, high technology performance helps Leaders beat competitors to market, improve customer satisfaction, and grow both market share and revenue.

Preventing Security Events and Maintaining Compliance

Outages can stem from a variety of causes. A natural disaster can knock a location offline, human error can cause a service outage, or a system, whether a server, storage, or networking component, can simply fail. However, ESG's research delved deeper into one specific class of disruption: those tied to security threats.

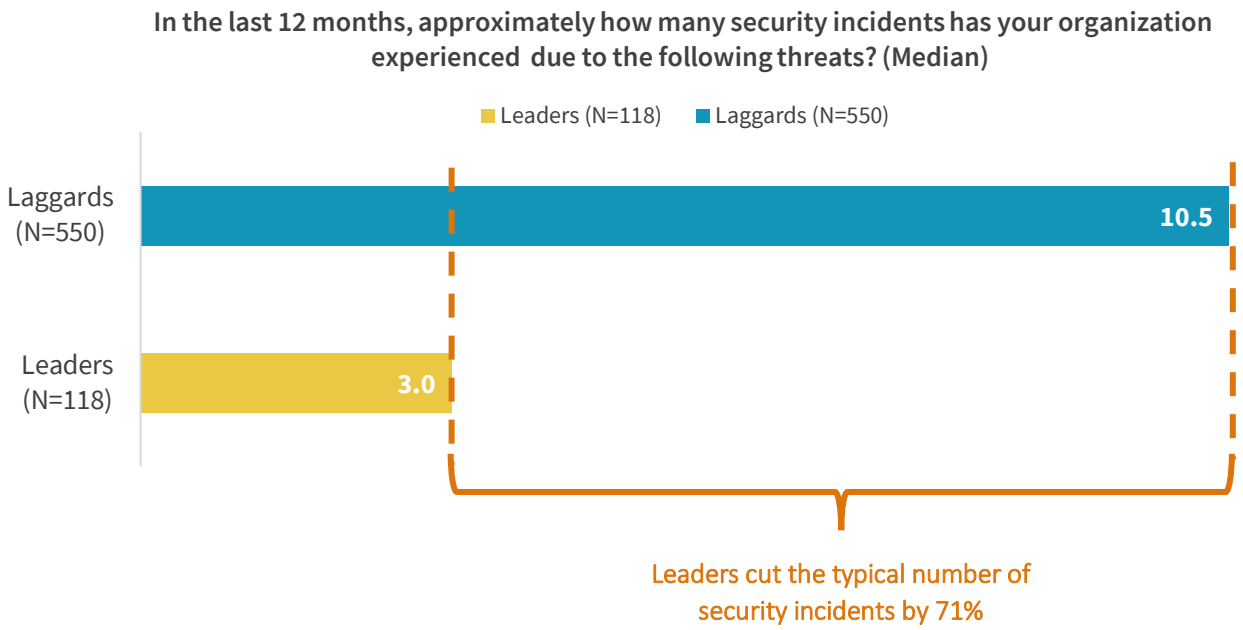
ESG asked respondents how many times in the past 12 months their organizations experienced security incidents tied to insider threats, data theft by cyber adversaries, and an inability to access data due to an ongoing cyber-attack. In each case, the majority of Leaders in ESG's research reported they had experienced either no events or one event. Lower maturity organizations were much less likely to report the same level of success preventing incidents tied to security threats (see Figure 3). **ESG aggregated the median number of security incidents experienced by each cohort of organization and found that Leaders experienced 71% fewer incidents over the past 12 months than Laggards (see Figure 4).**

Figure 3. Leaders Reduce the Number of Security Incidents Experienced



Source: Enterprise Strategy Group

Figure 4. Median Number of Security Incidents Experienced in Previous 12 Months

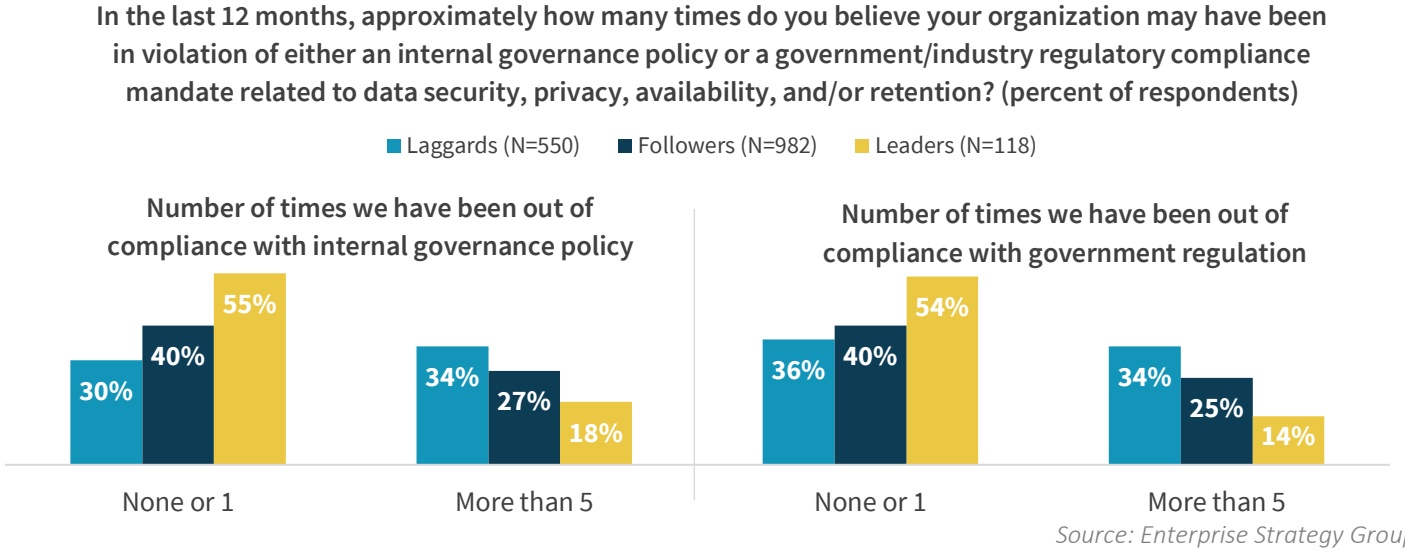


Source: Enterprise Strategy Group

Another driver of IT and business risk addressed in ESG's research is the ability, or lack thereof, of the organizations to maintain compliance. Compliance requirements, both internal and regulatory, can be stringent. For resource-constrained midmarket organizations, an efficient method of ensuring compliance is critical. At the same time, methodologies employed must be effective, as many midmarket organizations are in a poor position to absorb the financial penalties associated with regulatory non-compliance.

ESG asked respondents how many times in the past 12 months they believed their organization may have been in violation with either an internal governance policy or a government regulation. In both cases, the majority of Leaders in ESG's research reported they had either never been out of compliance or had been out of compliance only one time. Lower maturity organizations were much less likely to report the same level of success maintaining compliance (see Figure 5).

Figure 5. Leaders Reduce the Number of Times They Are Out of Compliance



Source: Enterprise Strategy Group

ESG aggregated the median number of times organizations were reported to be out of compliance for each cohort of organization and found that Leaders reduced the number of times they were out of compliance by 71% relative to Laggards. The data is clear: Organizations in adherence with Trusted Data Center best practices are much more effective at reducing the impact of cybersecurity incidents and maintaining compliance.

Minimizing Outages and Cost of Downtime

ESG's research explored a number of key performance indicators and outcomes tied to application availability and recoverability. In all cases, IT organizations operating newer infrastructure and with greater investment in high security and high reliability technology solutions enable superior results for their organization.

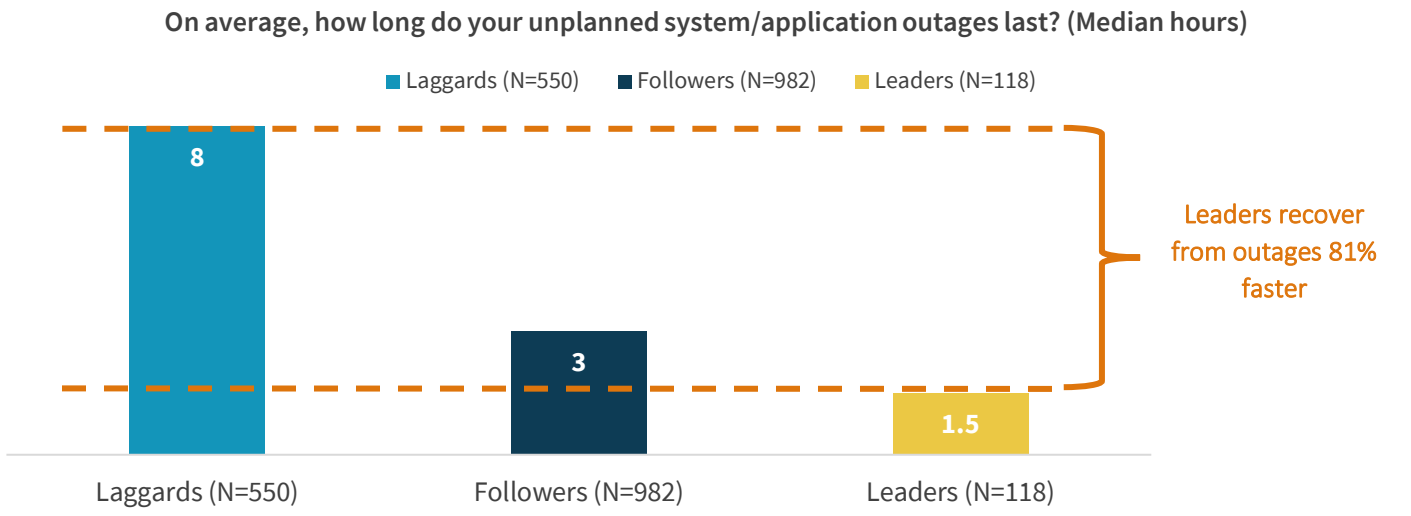
First, with respect to disaster recovery, ESG observed that Leaders in Data Center Trust are much more confident than Laggards in their ability to recover from a major outage like a natural disaster or some other location-wide outage in a timely manner. Leaders were 2.5x more likely than Laggards to be very confident that they could resume all business operations within a day of such an outage (48% versus 19%). Conversely, Laggards were 4.3x more likely than Leaders to be only somewhat confident, not very confident, or not at all confident in their ability to resume operations within a day (47% versus 11%) (see Figure 6).

Figure 6. Trusted Data Center Leaders Have Confidence in Their Recoverability Capabilities

Source: Enterprise Strategy Group

The data shows that Leaders have good reason to be more confident in their ability to recover from outages. ESG asked all respondents to quantify the typical duration of a system or application outage. While the median duration of an outage among Leaders was 1.5 hours, Laggards reported 8 hours. Compared with their low maturity counterparts, Leaders in Data Center Trust recover from outages 81% faster (see Figure 7).

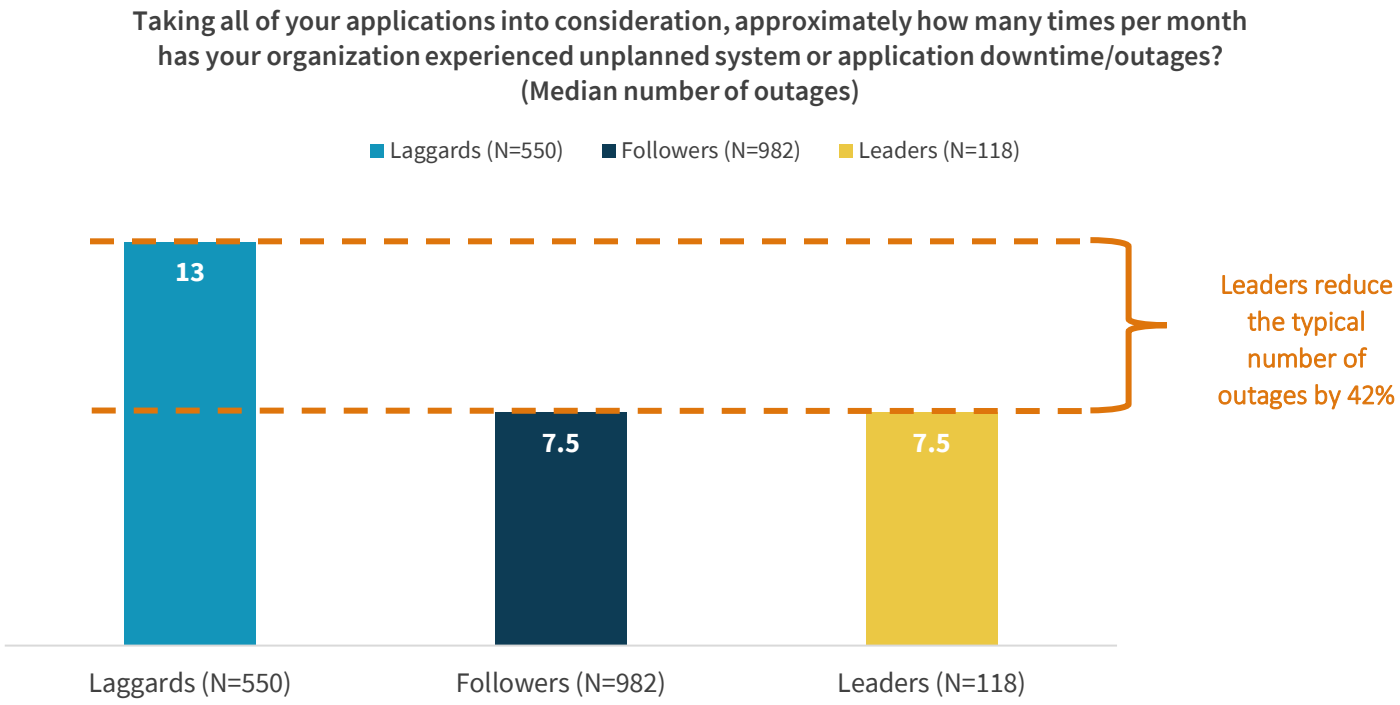
Figure 7. Trusted Data Center Leaders Recover Much Faster from Outages



Source: Enterprise Strategy Group

However, there is more to uptime and availability than just recovering from outages quickly. Just as important, if not more so, is the ability to prevent outages before they happen. Once again, the data shows that Leaders are more effective than lower maturity organizations. ESG asked respondents to consider the full scope of all applications and systems and to estimate how many times per month the organization experienced any unplanned downtime. Once again, using the median to normalize responses, Leaders reported experiencing 7.5 outages per month while Laggards reported 13 outages per month: Leaders in Data Center Trust reduce the number of outages by 42% (see Figure 8).

Figure 8. Trusted Data Center Leaders Experience Fewer Outages



Source: Enterprise Strategy Group

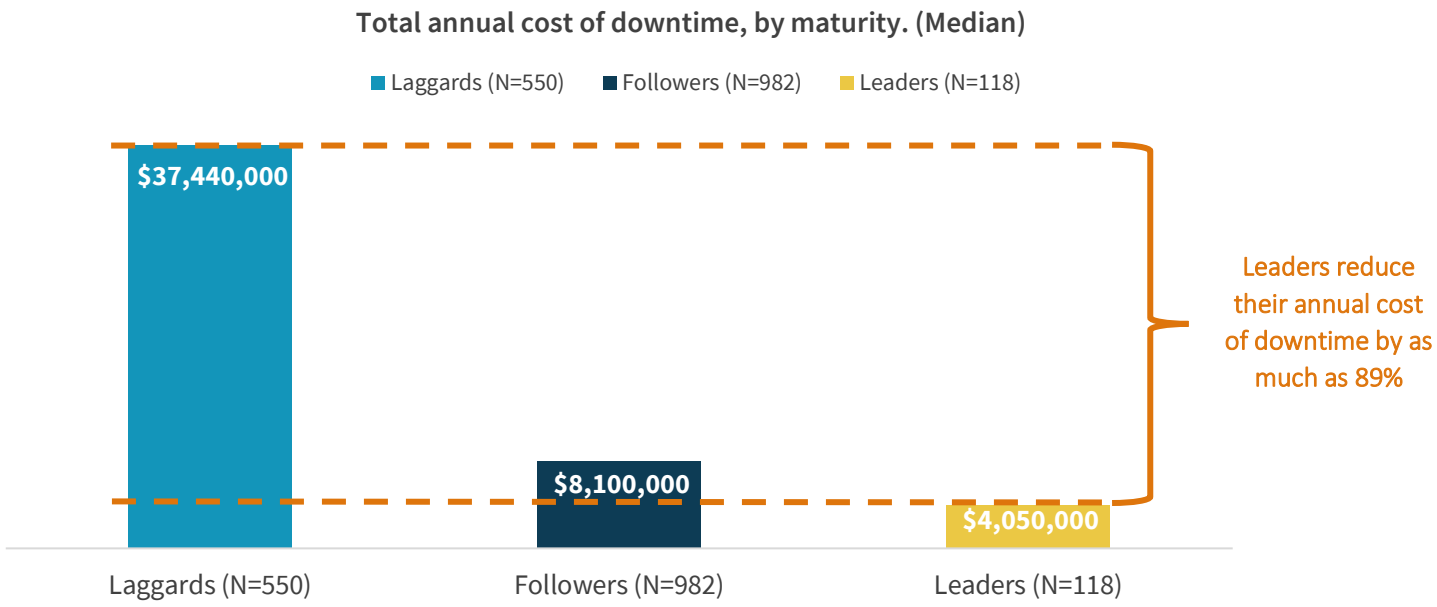
Reducing the Total Cost of Downtime with a Trusted Data Center

In addition to questioning respondents about the frequency and duration of application outages, ESG asked them to estimate their hourly cost of downtime for critical applications. By combining these three data points, ESG modeled an estimated average total cost of downtime for each group of organizations:

- First, ESG multiplied the median number of outages per month by 12 to determine the median number of outages per year among each tier of maturity.
- Next, ESG multiplied the number of outages per year by median duration (in hours) of outages to arrive at the median number of hours of downtime for each tier of maturity.
- Finally, ESG multiplied the total hours of downtime by the median cost of downtime reported by organizations in the survey ($30,000/hour).

In total, **Leaders save as much as $33.4M/year in downtime costs relative to Laggards, and $4.1M/year relative to Followers (a reduction of 89%) (see Figure 9).**

Figure 9. Leaders Drastically Cut Their Annual Cost of Downtime



Source: Enterprise Strategy Group

Technology Outcomes Fuel Business Advantages for Leaders

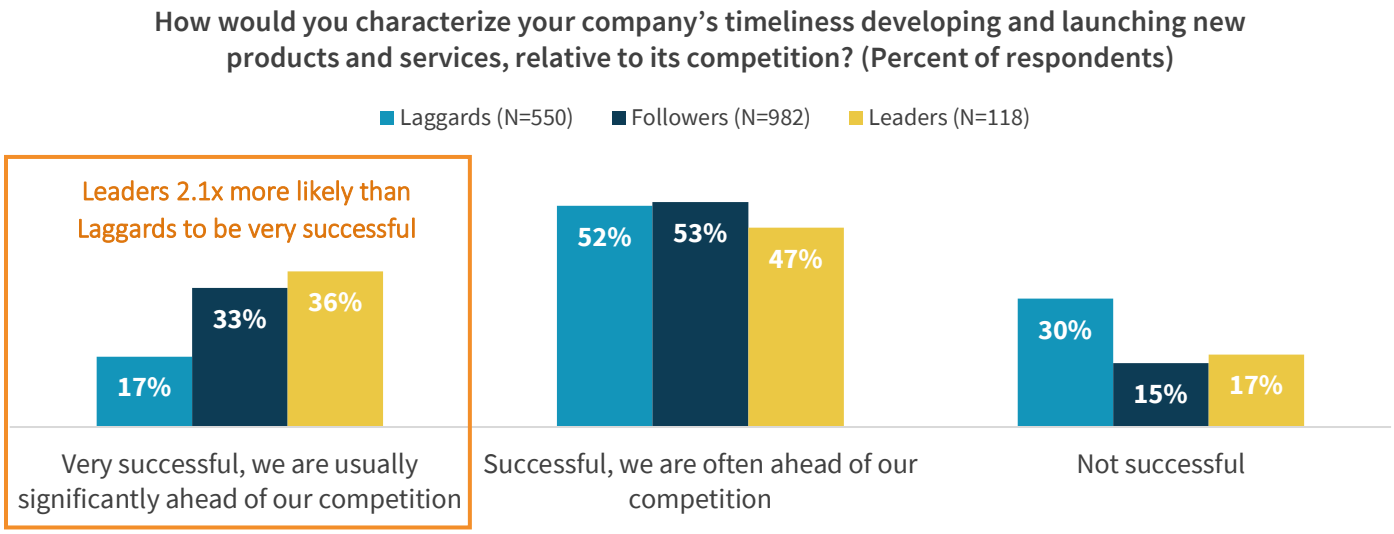
It is inarguable that organizations leading in Trusted Data Center Maturity are experiencing superior technology outcomes related to IT availability, recoverability, security, and compliance. ESG also found that Leaders better enjoy a host of business benefits compared with their lower maturity peers.

Improving Business Agility with a Trusted Data Center

ESG asked respondents how their organizations generally perform in go-to-market execution. **More than four-fifths of surveyed Leaders reported their organization is typically ahead of competitors when it comes to launching new products and services. Leaders were also more than twice as likely as Laggards to report they are usually *significantly* ahead of competitors (see Figure 10).** ESG believes the ability of these organizations to provide their employees with highly available

applications and highly recoverable data helps to maximize productivity and contributes to the success these organizations have achieved in beating competitors to market.

Figure 10. Leaders Outperform Competitors in Time to Market

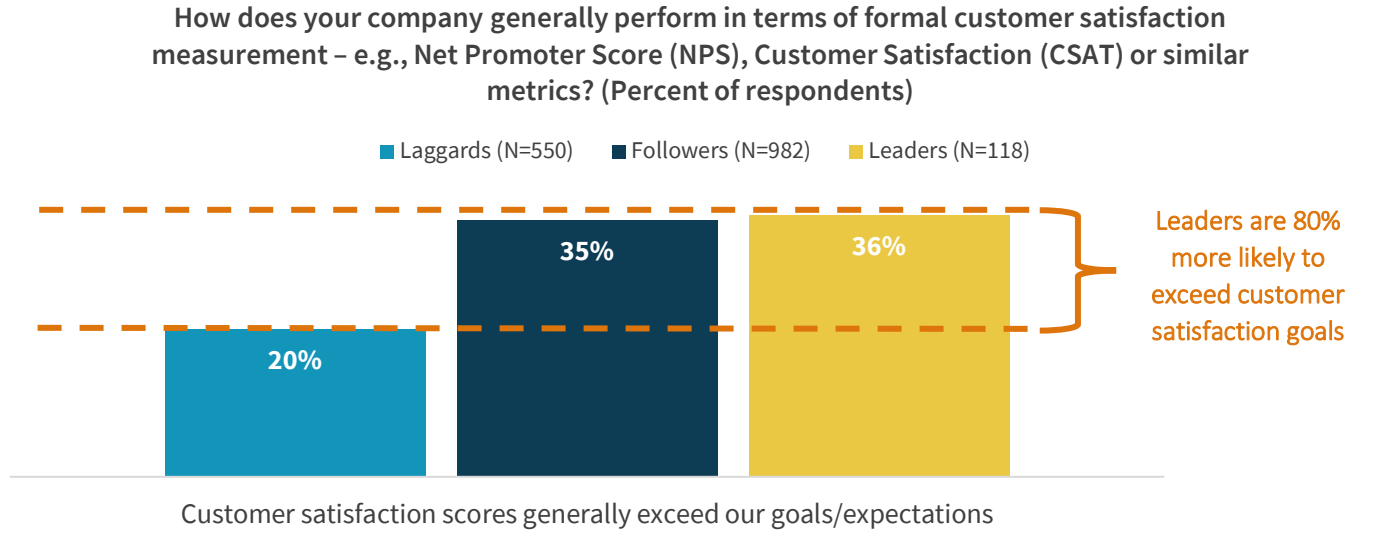


Source: Enterprise Strategy Group

Delighting Customers with a Trusted Data Center

ESG asked respondents how their organizations generally perform in terms of formal customer satisfaction measurement. **Leaders were 80% more likely to achieve customer satisfaction scores that exceed goals (see Figure 11).** Modern organizations depend on digital experiences to service customers. These trends are not unique to large multinational corporations as customer expectations across the board have moved toward "always on," and the consumption channels are increasingly digital. Leaders, with their highly available application portfolios, are best positioned to deliver on these expectations, which helps drive their superior satisfaction performance. Moreover, these organizations are better able to secure their customers' data. At this end of the market, a major breach of customer data could be an existential threat. Leaders experience fewer security incidents that could affect sensitive customer data and thus negatively impact customer goodwill.

Figure 11. Leaders Outperform Competitors in Customer Satisfaction



Source: Enterprise Strategy Group

A Trusted Data Center Is the Cornerstone of Midmarket Growth

As discussed, midmarket organizations face an intensely competitive business landscape. This data shows how Leaders at this end of the market are able to edge out competitors in terms of business agility and meeting and exceeding customer expectations. However, nothing can change the fact that these organizations must frequently compete against enterprise-class competitors with larger sales, marketing, and technology budgets. So, what does ESG's data say about these organizations' ability to grow and succeed over time?

ESG asked respondents whether their organization had increased, maintained, or lost market share relative to its competition in the past 12 months, and **99% of surveyed Leaders reported either maintaining or gaining market share.** Moreover, **Leaders were 46% more likely to report having gained market share compared with Laggards** (19% versus 13%).

In addition to past market share performance, ESG questioned respondents about their forward-looking revenue growth expectations. ESG asked respondents what annualized rate they anticipate their organization to grow (or contract) its top-line revenue over the next few years. **Leaders expressed considerably more optimism than Laggards: On average, Leaders expect revenue to grow at an annualized 22% for the next few years, twice the rate of Laggards (11%) (see Figure 12).**

Figure 12. Leaders Expect to Grow Faster than Peers

Source: Enterprise Strategy Group

The Bigger Truth

IT organizations in the midmarket face a perception from their line-of-business counterparts that the level of security and risk mitigation they can provide is problematic. Moreover, those in IT leadership positions at midmarket organizations frequently acknowledge a problematic skill shortage in the cybersecurity arena. However, ESG's research shows that specific actions organizations can take are strongly correlated to improved technical and business outcomes.

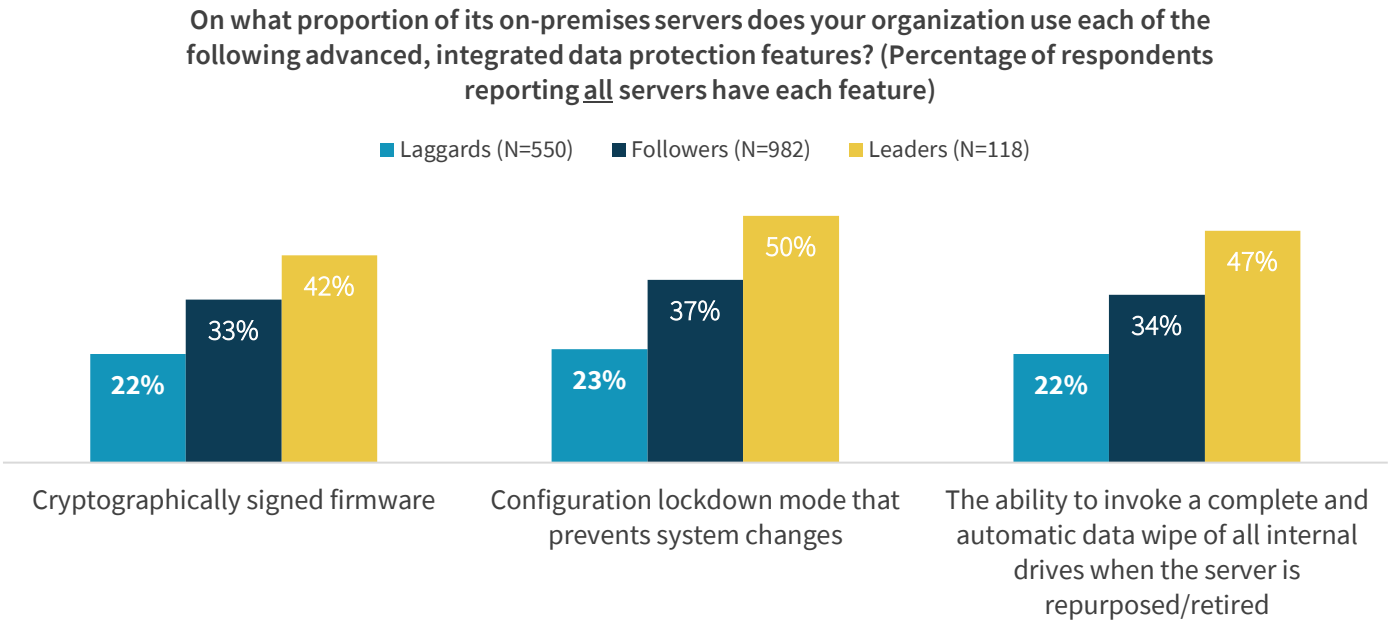
Learning from Leaders

Organizations should work toward improving their adherence to best practices in ESG's Trusted Data Center framework. Additionally, ESG identified a number of related behaviors and investments Leaders make more often than lower maturity counterparts. Organizations looking to improve their availability, dependability, security, and, ultimately, business competitiveness would do well to focus on the following:

1. **Frequently refresh server and storage infrastructure.** Within Leaders, the average storage system is 2.5 years old, which is two years younger than the average storage system at Laggards. Similarly, the average server within a Leader's data center is 1.5 years old, again two years younger than what ESG observed among Laggards. By operating more modern infrastructure, Leaders use solutions with more sophisticated security and data protection capabilities.

2. **Prioritize server solutions with sophisticated "built-in" security capabilities.** While newer servers will inherently tend to be more secure than older servers, there are specific security capabilities ESG included in its research: the ability to check that all system updates are cryptographically authenticated, automatic lockdown of configuration settings, and the ability to execute complete system erasures. Leaders were much more apt to report all their servers had each capability (see Figure 13). Organizations would do well to emphasize these capabilities in their solution evaluations.

Figure 13. Leaders Leverage Servers with Advanced Native Security Features

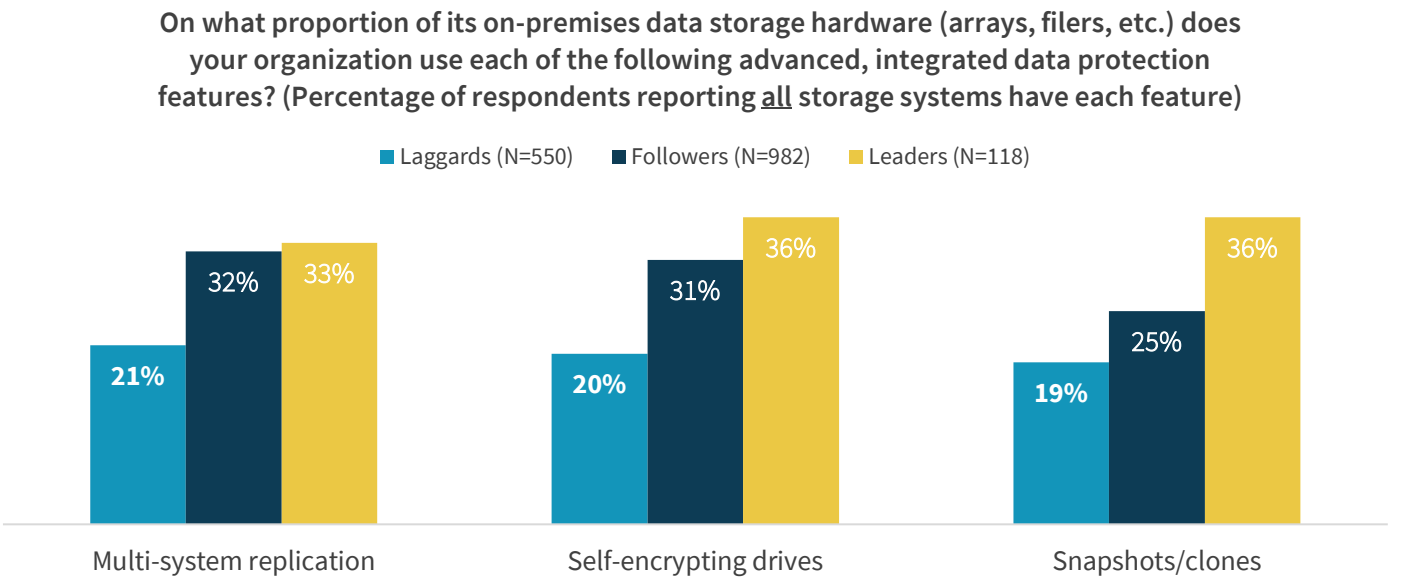


Source: Enterprise Strategy Group

3. **Automate everywhere.** Of course security features matter, but the fact remains that organizations' number one vulnerability is people. Mitigating that vulnerability takes automation. By removing human error from server management tasks, organizations can dramatically improve their risk profile. Leaders were much more likely than Laggards to report that server management tasks like server patching (41% versus 21%) and threat detection (42% versus 21%) were entirely automated at their organization.

4. **Pay close attention to the data protection features of storage systems.** Relative to the prior generation of arrays, newer storage systems generally ship with a multitude of integrated data protection features. However, ESG's research showed Leaders ensure specific features are present on all of their deployed storage arrays: the ability to replicate data to multiple systems, the use of self-encrypting drives, and native snapshots/cloning capabilities. Leaders were much more apt than lower-maturity organizations to report all their servers had each capability (see Figure 14). Organizations would do well to emphasize these capabilities in their solution evaluations.

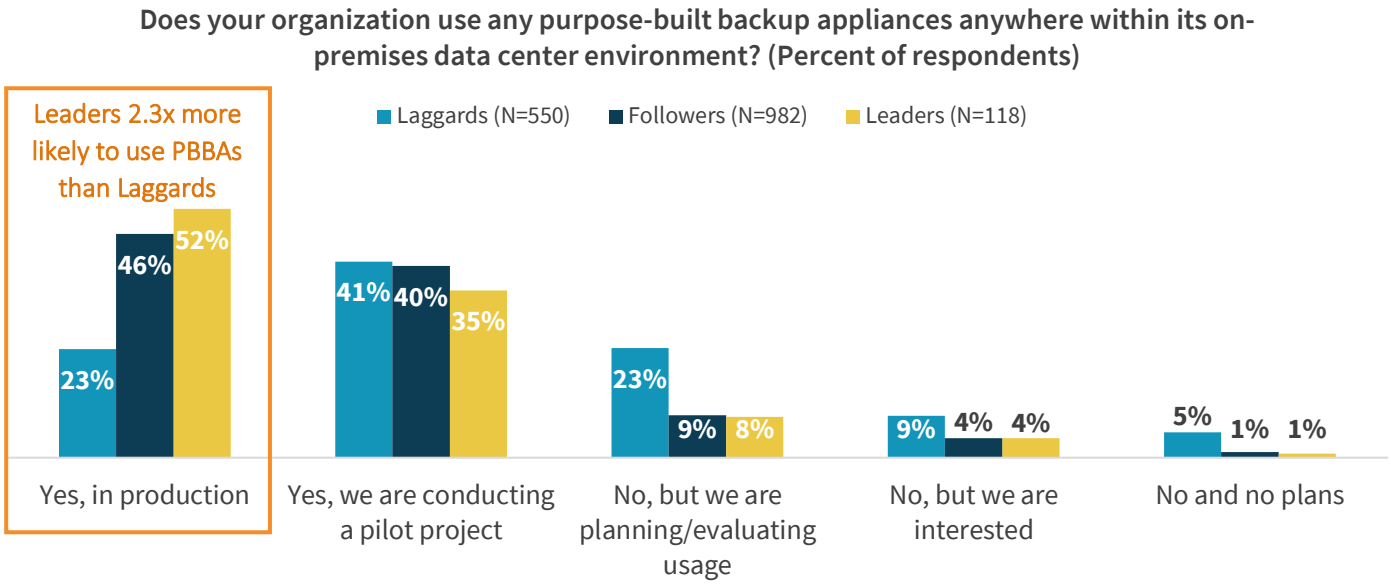
Figure 14. Leaders Leverage Storage with Advanced Native Data Protection Features



Source: Enterprise Strategy Group

5. **Leverage purpose-built backup appliances (PBBAs) to optimize results**. While redundant storage systems and replicated data help ensure recoverability, many organizations benefit from additional investments in purpose-built backup appliances. Such a standalone storage device can run its own backup-related workloads without impacting other servers. Because it is a separate device dedicated only to those workloads, it does not impact end-users by sapping resources away from devices handling active data or applications. Similarly, the performance of backup and restore operations is optimized due to the dedicated resources. While not all midmarket organizations find they need this degree of infrastructure tiering, Leaders were much more apt to have invested in this second layer of storage (see Figure 15).

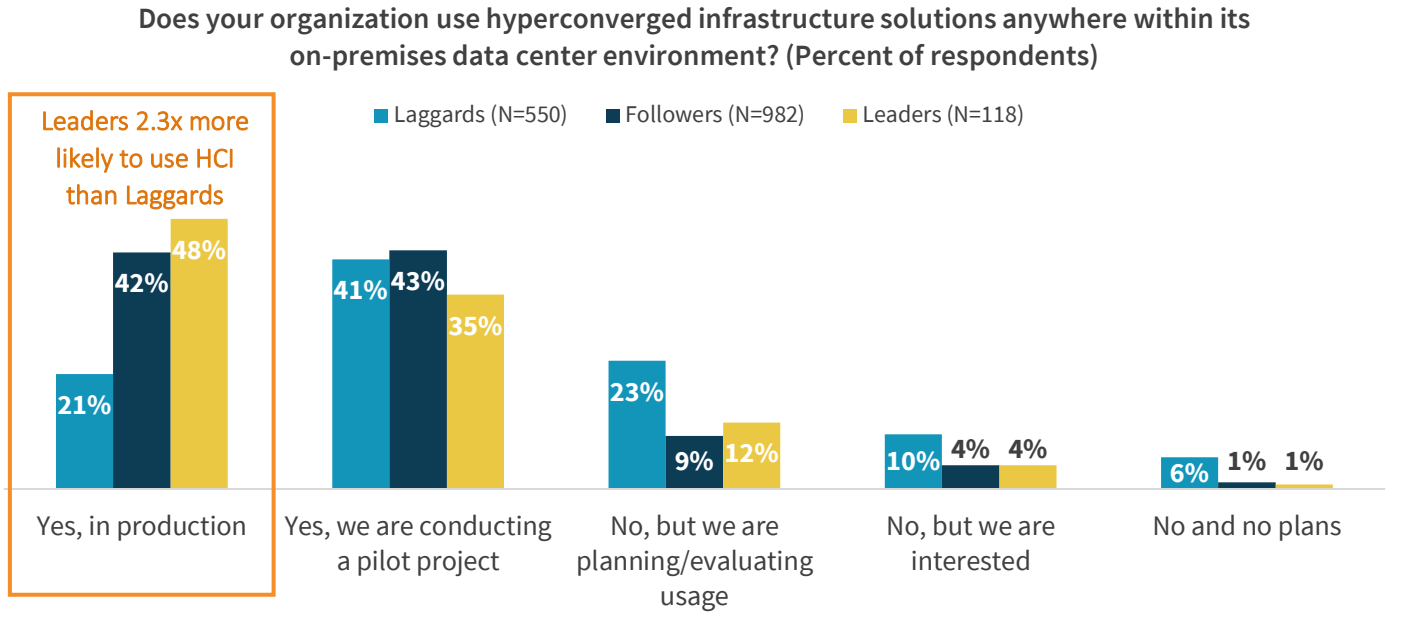
Figure 15. Leaders Have Often Deployed PBBAs



Source: Enterprise Strategy Group

6. **Explore hyperconverged infrastructure solutions to free up invaluable staff resources.** ESG research shows that midmarket organizations question their IT staff's cybersecurity capabilities. One solution to this problem is to allocate more staff to cybersecurity tasks. However, most midmarket organizations do not have superfluous IT staff sitting idle. Rather, those resources would need to come from other workflows. Hyperconverged infrastructure (HCI) can help. HCI eliminates the need for IT staff to spend days or weeks right-sizing separate compute, storage, and networking components. Similarly, deployment and integration are much more efficient with all the resources included in one box. This time saved can be applied to more pressing tasks—like security. Fitting with this hypothesis, ESG observed that Leaders make up the group that is most aggressively adopting HCI (see Figure 16).

Figure 16. Leaders Have Aggressively Adopted HCI



Source: Enterprise Strategy Group

How Dell Technologies Can Help

This ESG Research Insights Paper was commissioned by Dell Technologies and Intel Corporation. Dell Technologies powered by Intel technology, unites seven technology leaders—Dell, Dell EMC, Pivotal, RSA, Secureworks, Virtustream, and VMware—in one company with the power to drive security and IT transformation and generate real results for its customers.

Learn more about how Dell Technologies can help advance your Trusted Data Center Maturity.

Appendix I – Research Methodology and Respondent Demographics

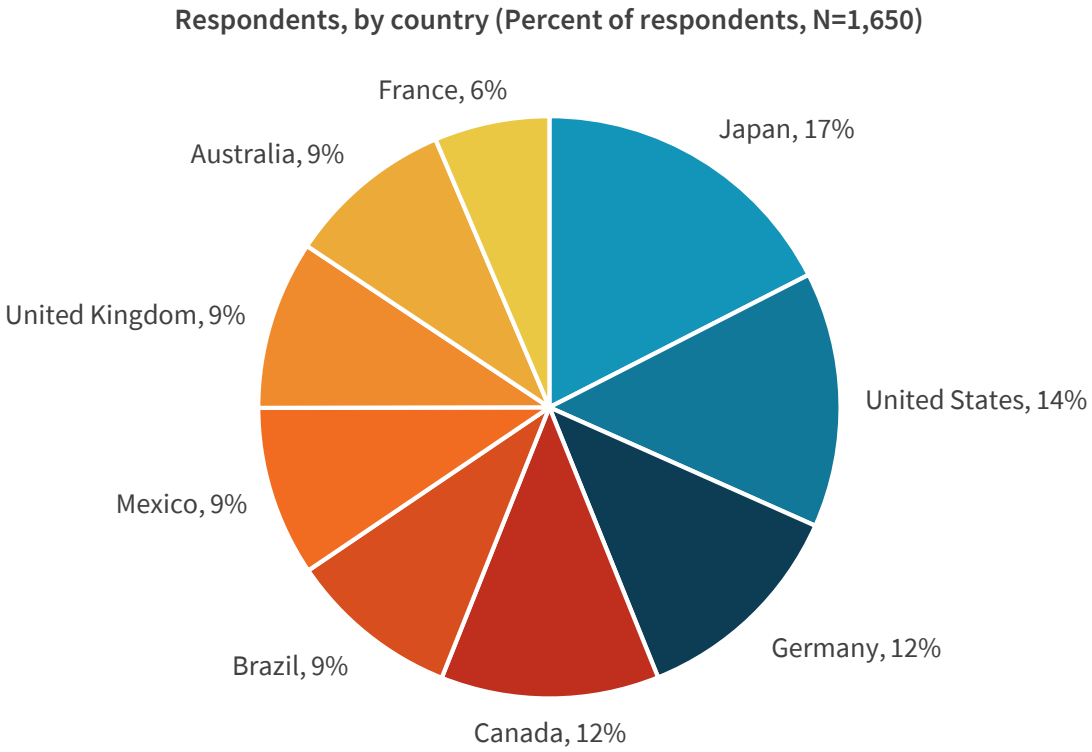
To gather data for this report, ESG conducted a comprehensive online survey of IT decision makers from private- and public-sector organizations across the globe. The survey was fielded between June 13, 2019 and July 8 , 2019. To qualify for this survey, respondents were required to be involved in the decision-making process for data center technology purchases at their organization. Moreover, they must have reported a high degree of familiarity with their organization's risk reduction strategies and priorities. Finally, the research was exclusive to the midmarket: All respondents must have been employed at organizations with between 100 and 999 total employees.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 1,650 respondents remained.

All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents. Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

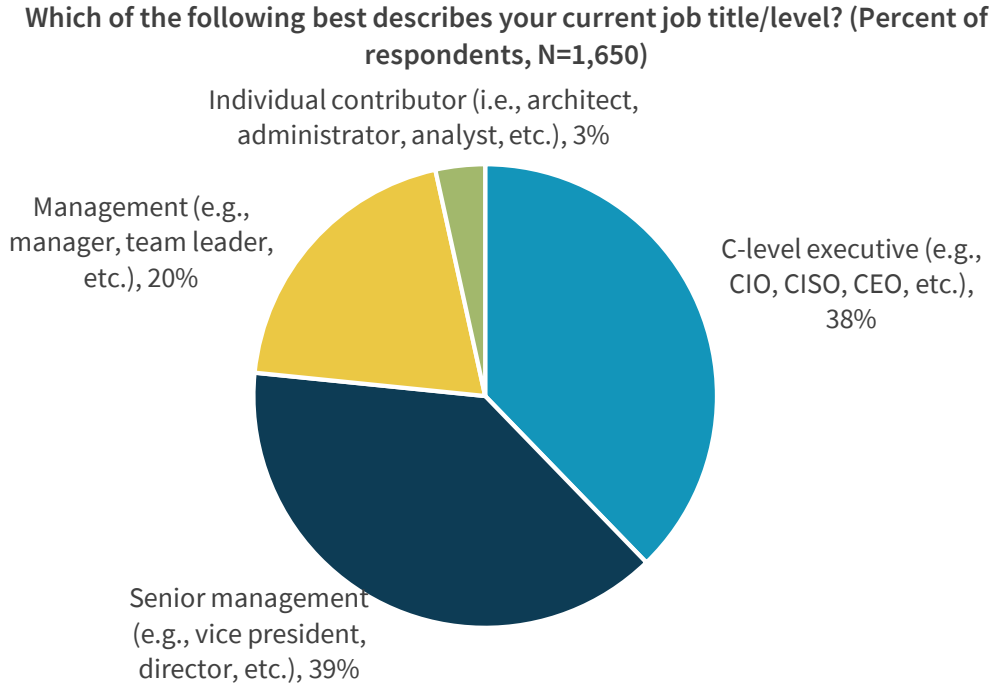
The figures below detail the firmographics of the respondent base, including respondents' country of residence, respondents' responsibility level, organizations' total number of employees, and organization industry.

Figure 17. Survey Respondents, by Country



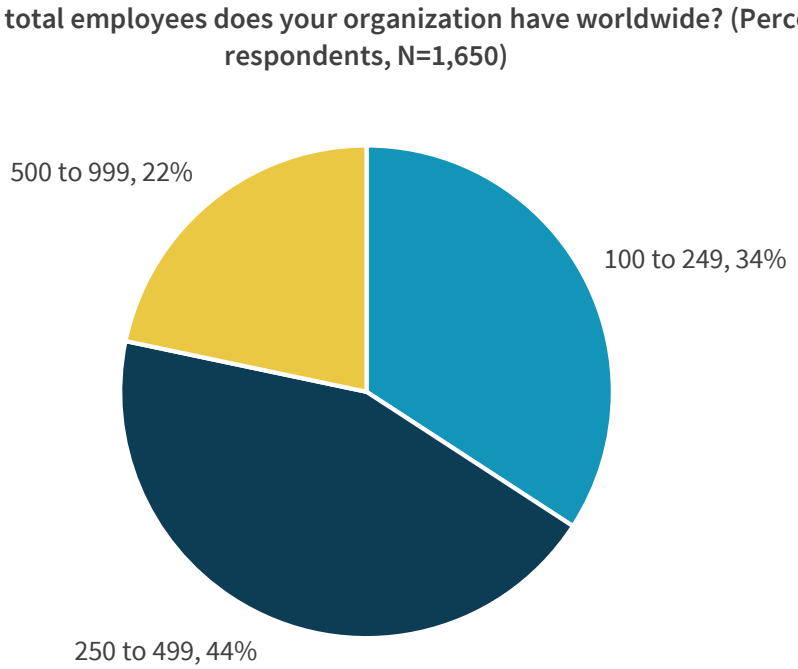
Source: Enterprise Strategy Group

Figure 18. Survey Respondents, by Job Level/Title



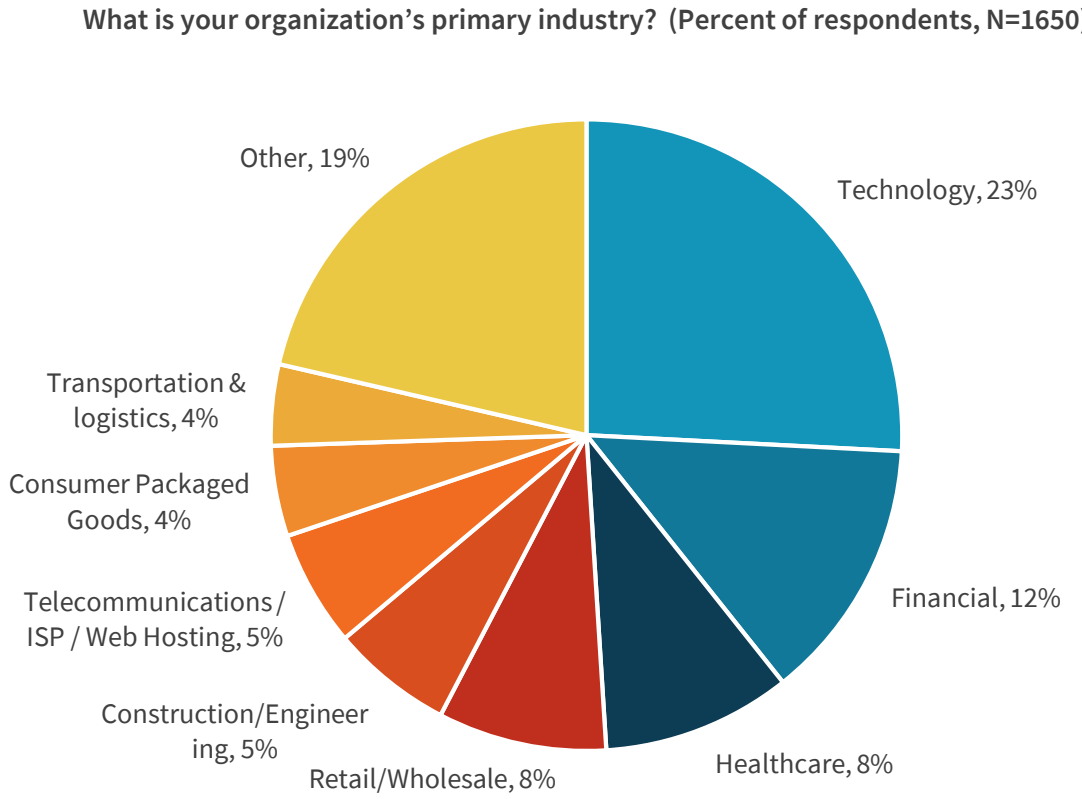
Source: Enterprise Strategy Group

Figure 19. Survey Respondents, by Organization's Number of Employees



Source: Enterprise Strategy Group

Figure 20. Survey Respondents, by Organization's Industry



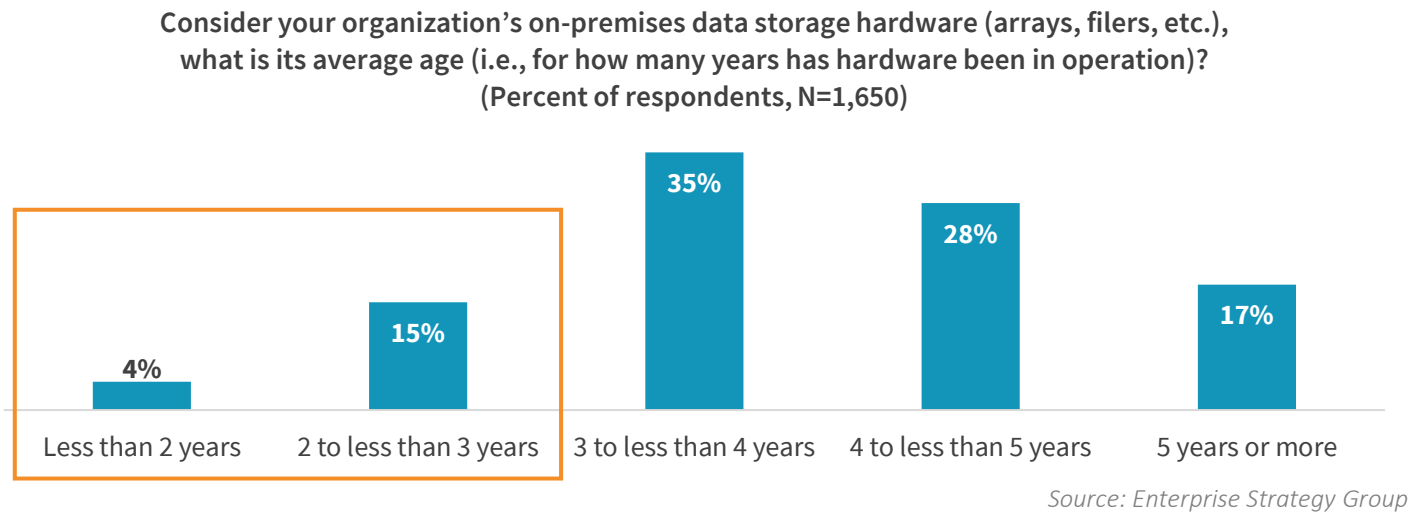
Source: Enterprise Strategy Group

Appendix II – Criteria for Evaluating Organizations' Trusted Data Center Maturity

In order to evaluate how best practice adherence is linked to technology and business outcomes, ESG developed a Trusted Data Center Maturity framework that put forward six concrete migration best practices against which organizations could be assessed. To assess these best practices, ESG asked six corresponding questions in its survey. Organizations in alignment with all of the best practices were placed in the Trusted Data Center "Leader" category. Organizations in alignment with four or five best practices were placed in the Trusted Data Center "Follower" category. And organizations in alignment with three best practices or fewer were placed in the Trusted Data Center "Laggard" category.

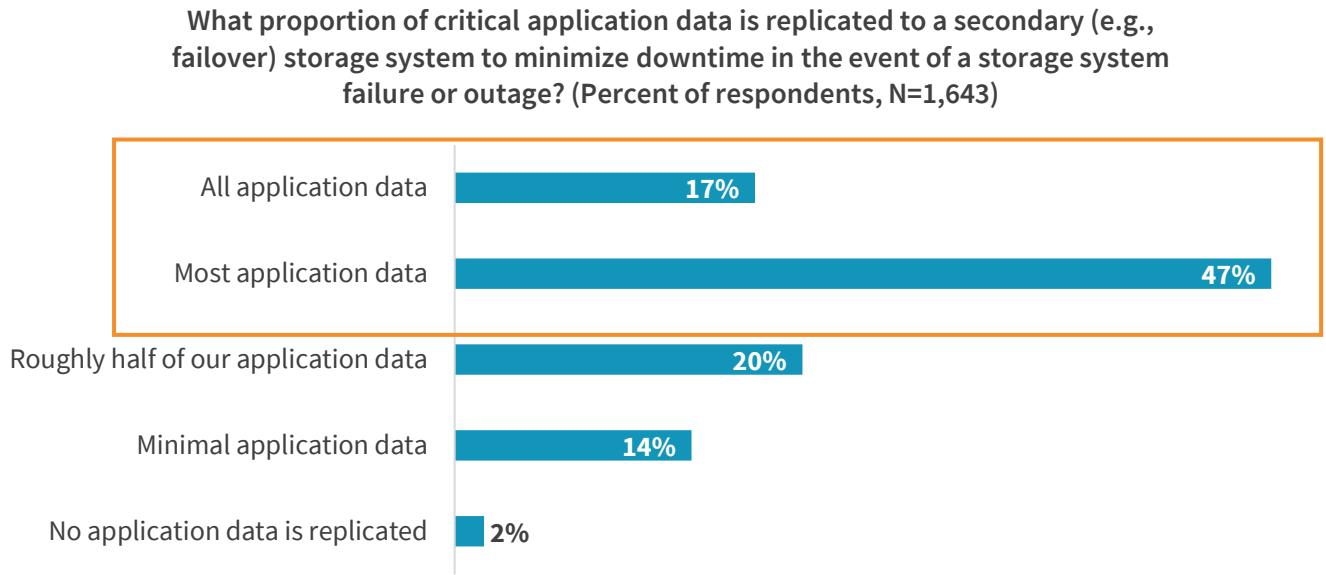
The questions ESG asked to assess Trusted Data Center Maturity are shown in the following figures. The responses aligned with migration best practices are highlighted.

Figure 21. Survey Respondents, by Age of Storage Hardware



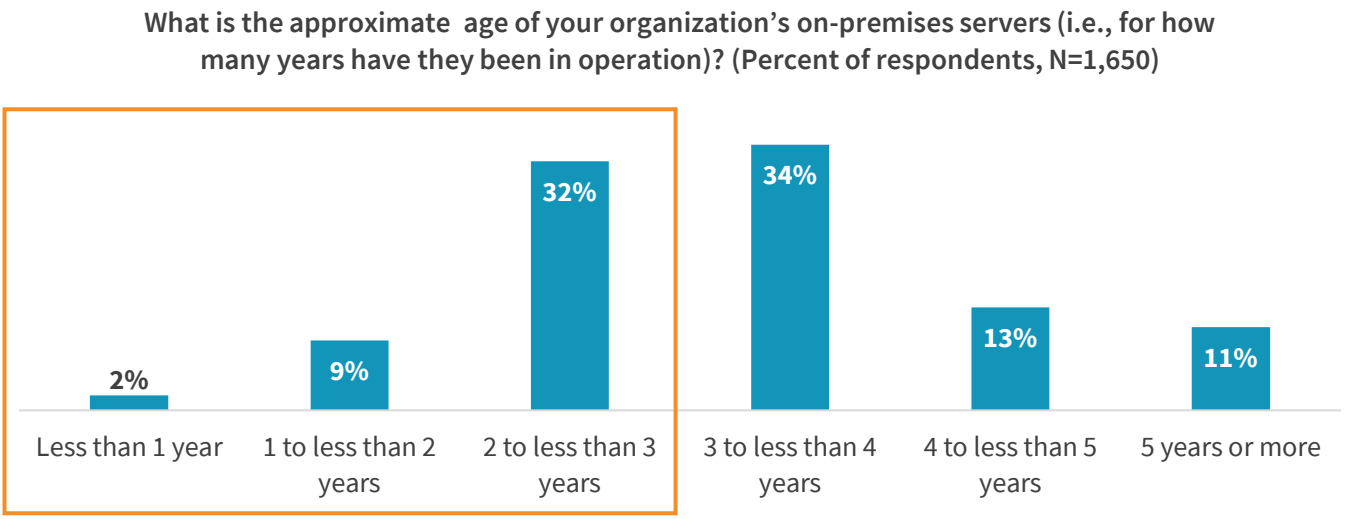
Source: Enterprise Strategy Group

Figure 22. Survey Respondents, by Proportion of Critical Data Replicated



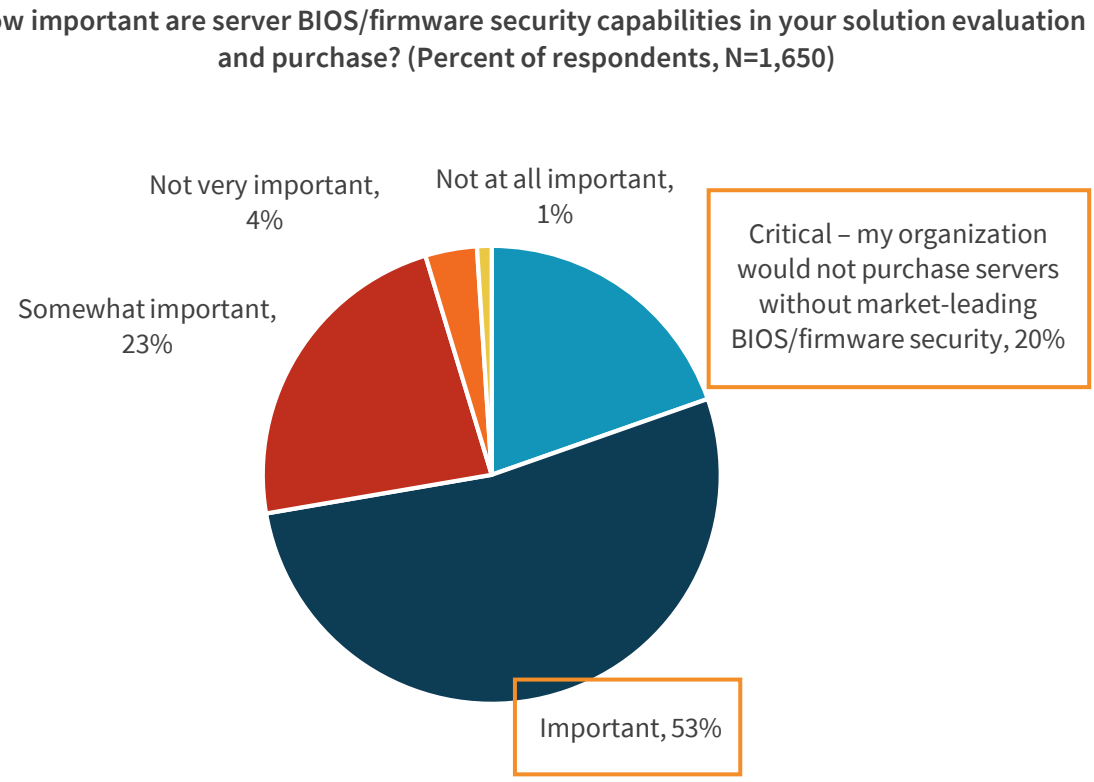
Source: Enterprise Strategy Group

Figure 23. Survey Respondents, by Age of Servers



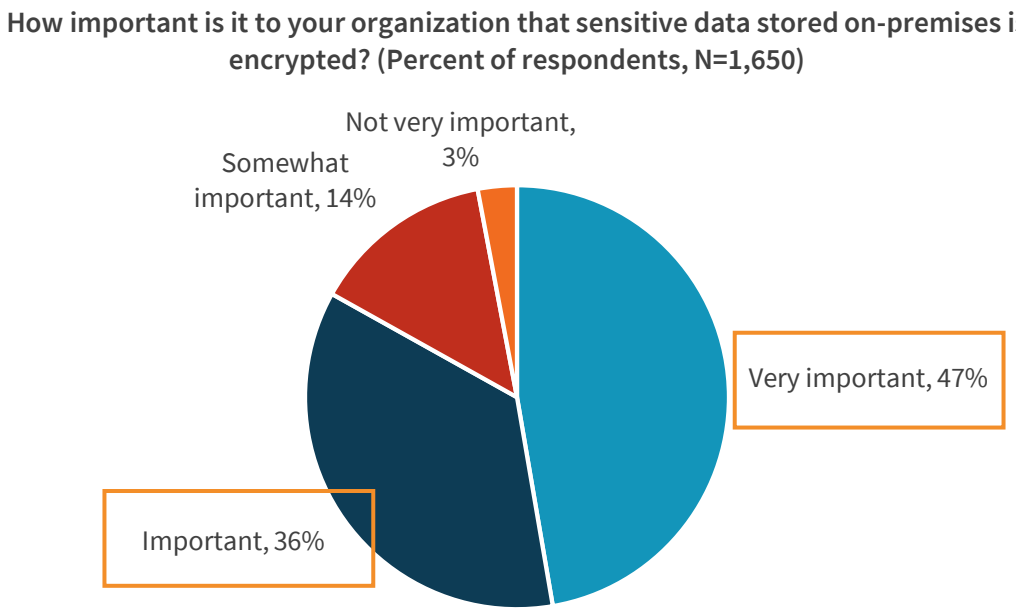
Source: Enterprise Strategy Group

Figure 24. Survey Respondents, by Criticality of Server Firmware Security Capabilities



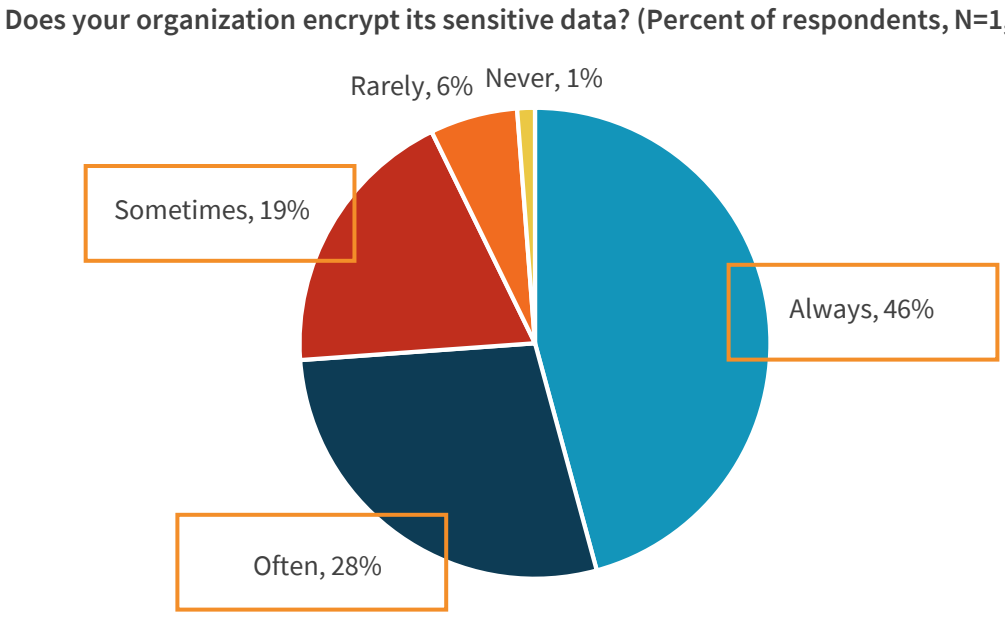
Source: Enterprise Strategy Group

Figure 25. Survey Respondents, by Perceived Importance of Encryption



Source: Enterprise Strategy Group

Figure 26. Survey Respondents, by Actual Encryption of Data



Source: Enterprise Strategy Group

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188