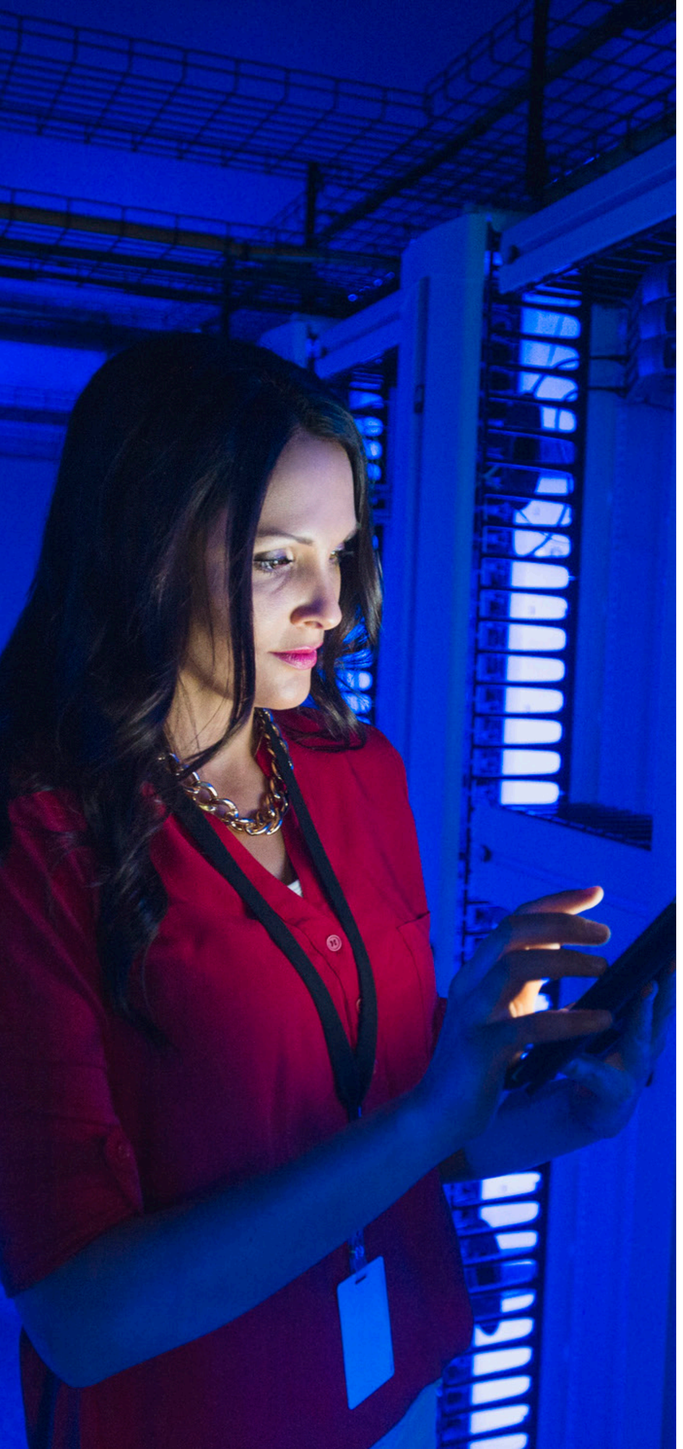
The Trusted Data Center and Server Infrastructure:

Best Practices and Business Results for Mid-Market Organizations

Insights from Dell Technologies & Intel Corporation's Global Survey of Mid-Market IT Leaders

NOVEMBER 2019



When Security Is At The Core, Everything Else Falls Into Place: The Trusted Data Center Maturity Model

Many mid-market organizations struggle to deliver the data center security and reliability demanded in this highly competitive segment of the market. Both line-of-business and IT stakeholders acknowledge room to improve:

38%
of line-of-business executives have serious concerns about IT's security capabilities and controls.
This is the most frequently cited issue line-of-business respondents have with IT.

46%
of IT practitioners feel they have a problematic cybersecurity skills shortage.
This is the skills shortfall most frequently cited by IT respondents.

Why Does Leading in Data Center Trust Matter?

By prioritizing the security and dependability of their IT environments above all else, mid-market organizations with trusted data centers experience very real and quantifiable business and technology outcomes that give them the edge and agility to win in today's highly competitive marketplace.

Data center risk has the potential to hurt organizations relative to competitors:

- Outages can disrupt customer service, leading to customer churn or negative reviews.
- Downtime also has direct financial implications. ESG's research shows the average hourly cost of downtime for **surveyed firms is between $30,000 (median) and $38,000 (mean).**
- Compliance violations often have direct financial consequences. For example, a GDPR violation could **result in a fine of up to 4% of an organization's annual revenue.**

This eBook is grounded in peer-based primary market research and is intended to highlight the behaviors and performance of organizations leading the market in data center trust **specifically as they relate to on-premises server infrastructure.**

What It Means to Be a Trusted Data Center Leader

Dell Technologies, Intel Corporation, and ESG recently completed a survey of 1,650 IT executives and strategists at organizations with less than 1,000 employees. The research showed that just **7% of mid-market organizations could be categorized as trusted data center Leaders** that were in alignment with a broad set of best practices spanning different aspects of infrastructure, security, and data protection. On the other end of the spectrum, **33% of mid-market organizations were categorized as trusted data center Laggards,** in alignment with half or less of the best practices assessed.

Trusted Data Center Best Practices:

Refresh/retire data center infrastructure regularly

- Average server age is <3 years at all Leader organizations
- Average storage system age is <3 years at all Leader organizations

Believe strongly that trusted technologies matter

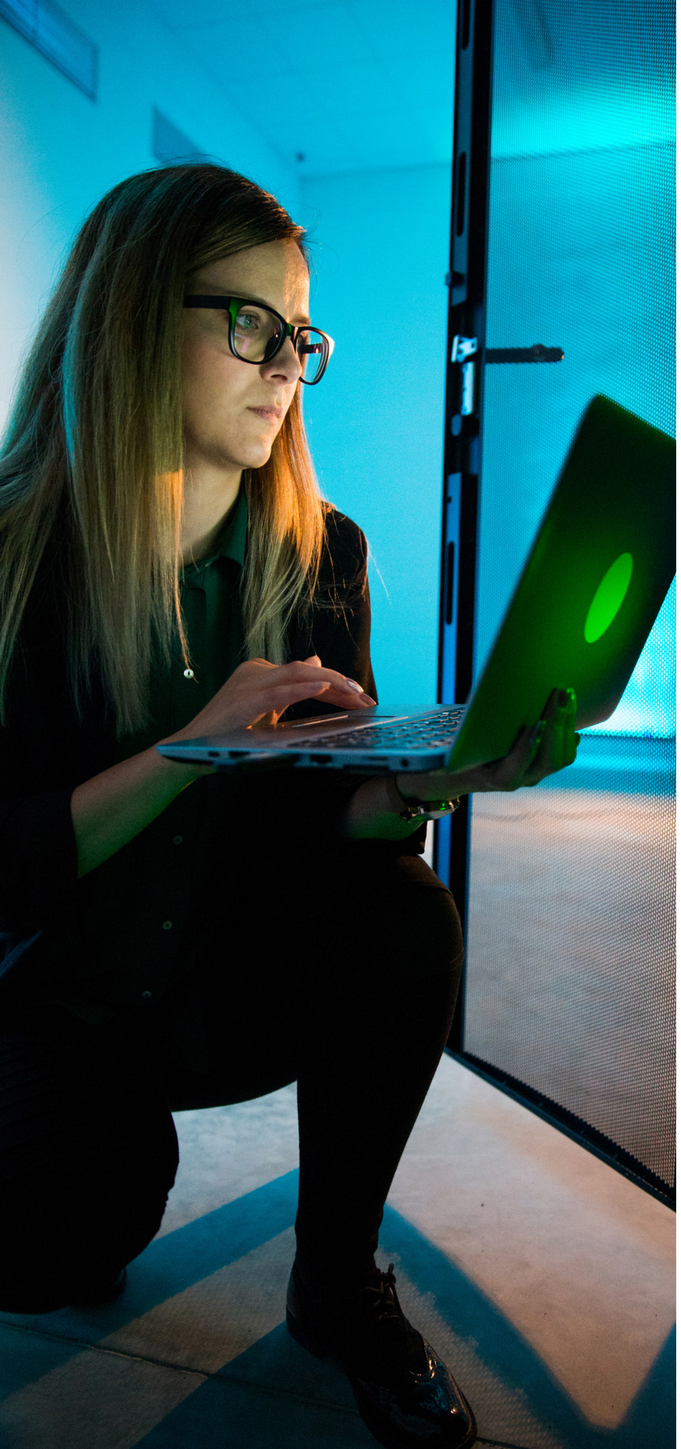
- All Leader organizations believe it is important to encrypt sensitive data
- All Leader organizations believe “built in” secure infrastructure is important

Act on beliefs by using trusted technologies

- All Leader organizations actually encrypt sensitive data
- All Leader organizations replicate most/all sensitive data to secondary systems

Download the full report for more information

DOWNLOAD REPORT

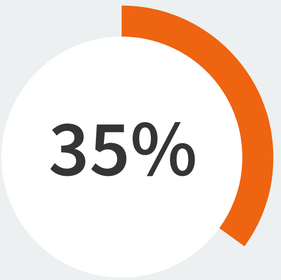


How to Become a Leader: Prioritize Market-Leading BIOS/Firmware Security

Leaders evaluate embedded BIOS and firmware security with greater scrutiny and prioritize best-in-class **capabilities when making server purchases. They do this because:**

1. It ensures that their server environment is built on a rock-solid security foundation.
2. The BIOS is a critical vulnerability: With access to the BIOS, an attacker can compromise all of a server's endpoint security capabilities.
3. There are a growing number of BIOS-specific attack types and new malware variants that must be mitigated.

Percentage of organizations that rate market-leading BIOS/firmware as critical or important:



Why BIOS/Firmware Security Matters

Based on ESG's research, organizations that prioritize BIOS/firmware security capabilities (i.e., rate them as critical/important) performed better across several metrics compared to those that do not.

THEY EXPERIENCE FEWER SECURITY INCIDENTS

On average, organizations prioritizing BIOS/firmware security **experience 26% fewer security incidents** like data loss caused by insiders or external bad actors and outages due to cyber attacks than those that do not.

THEY EXPERIENCE FEWER TOTAL APP OUTAGES

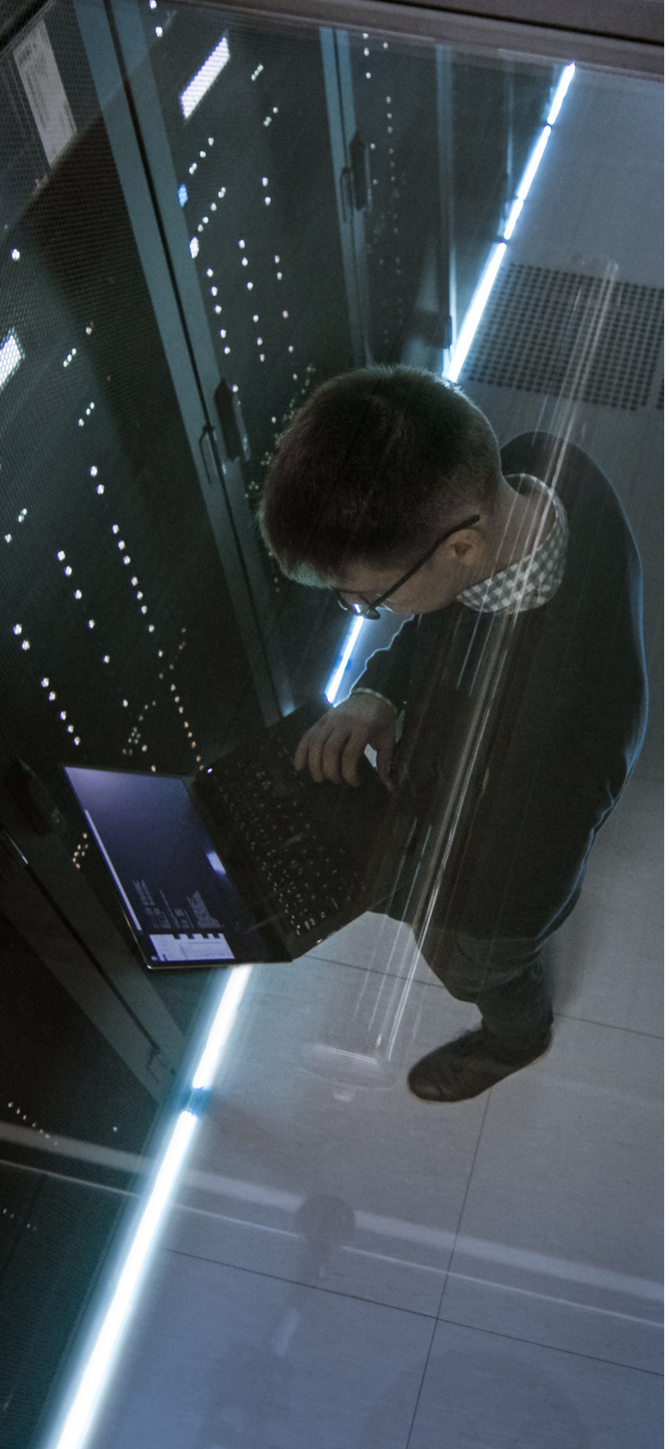
Organizations prioritizing BIOS/firmware security **experience 42% fewer application outages** compared to those that do not.

THEY ACHIEVE HIGHER ROI ON SECURITY SPEND

Organizations prioritizing BIOS/firmware security **are 2X more likely** than those that do not to say security technologies they invest in deliver higher than expected ROI.

THEY EXPERIENCE REDUCED RISK EXPOSURE

Organizations prioritizing BIOS/firmware security **are 1.7X more likely** than those that do not to say their security investments have greatly reduced risk exposure.

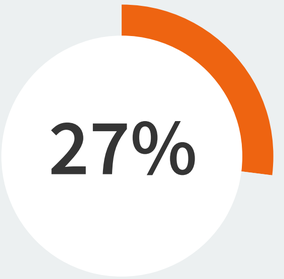


How to Become a Leader: Refresh Server Infrastructure Frequently

Leaders refresh servers more often than their counterparts, allowing them to:

1. Take advantage of new hardened and multi-layered security capabilities that may not be present on older generations of technology.
2. Eliminate aging infrastructure that is more susceptible to failures that cause outages / downtime.
3. Keep devices secure and in compliance with enterprise and government specifications, since upgraded servers have the latest firmware and patching updates.

Percentage of respondents reporting the average age of servers is <3 years old:



For Leaders, Newer Servers + Prioritized Embedded Security = A More Feature-Rich Server Environment

ESG asked respondents about key integrated server security and data protection features. Leaders were much more likely than Laggards to report that all of their servers had each capability:

CRYPTOGRAPHICALLY SIGNED FIRMWARE

Ensures that firmware running servers is authorized through cryptographic signatures. **Leaders are 1.9X more likely than Laggards** to report all servers include this feature.

SECURITY LOCKDOWN MODE

Automatically detects and prevents negligent or malicious configuration changes. **Leaders are 2.2X more likely than Laggards** to report all servers include this feature.

COMPLETE AUTOMATED DATA WIPE CAPABILITIES

Provides organizations with the ability to invoke a complete and automatic data wipe of all internal drives when servers are repurposed or retired. **Leaders are 2.1X more likely than Laggards** to report all servers include this feature.

Quantifying the Value of Refreshing Server Infrastructure Frequently

Due, in part, to their newer servers, organizations that operate a modern server footprint experience fewer application outages that are resolved faster. Combining this data with the average cost of downtime reported, **organizations with modern server environments save as much as $14.3M/year in avoided downtime compared to organizations with legacy servers.**

41% reduction in downtime cost

	OUTAGES ACROSS ALL APPS PER MONTH		MONTHS		HOURS PER OUTAGE		COST PER HOUR		TOTAL ANNUAL COST OF DOWNTIME
Modern Servers (average server age <3)	9.4	×	12	×	4.9	×	$38K	=	$21M
Legacy Servers (average server age 3+)	10.2	×	12	×	7.6	×	$38K	=	$35M

How to Become a Leader: Automate Server Management

Beyond its innate simplification and management advantages, automation is a clear accelerator for mid-market organizations: it saves precious staff time while eliminating human error that can introduce vulnerabilities or cause outages. **Leaders more aggressively automate a broad range of server management tasks than their less leading-edge counterparts.**

LABOR SAVINGS OF AUTOMATION

By automating server management tasks, **Leaders have saved an average of 10.5 person-hours per week.** For mid-market firms with just a handful of IT FTEs stretched far too thin, these productivity savings can be a game changer.

How Leaders automate their server management:

SERVER PATCHING

Leaders are 2X more likely than Laggards to completely automate server patching.

THREAT DETECTION AND REMEDIATION

Leaders are 2X more likely than Laggards to entirely automate the detection of malicious activities and lock down compromised systems.

VULNERABILITY DETECTION AND REMEDIATION

Leaders are 1.4X more likely than Laggards to entirely automate the detection of system misconfigurations, configuration drift from validated benchmarks, and vulnerabilities caused by unpatched systems.

Why Server Automation Matters: Technology KPI Performance

More than just saving time, automation removes error-prone workflows from IT administrators' plates, improving efficacy **as well as efficiency.** Roughly 10% of respondents reported their organizations had freed up more than 20 hours of administrator time per week due to server management automation. Across the board, organizations who automate drive exceptional technology KPI performance.

Overall Application and System Uptime

By reducing human error and eliminating vulnerabilities, highly automated organizations achieve better overall application and system uptime.

OVERALL APPLICATION AND UPTIME

Highly automated organizations are 30% more likely to deliver highly reliable application and system uptime. In fact, 86% of these organizations deliver excellent or good overall application and system uptime. Additionally, **less automated organizations are 3.7X more likely to report application and system uptime needs to improve.**

Security Incident Reduction

Moreover, highly automated organizations are better able to harden their infrastructure security to make them less vulnerable to exploits. As a result, these organizations experience fewer data loss events.

DATA LOSS INCIDENTS CAUSED BY INTERNAL AND EXTERNAL THREATS

On average, **highly automated organizations reduce data loss events by 71%,** typically experiencing 2 events caused by insiders and external bad actors versus 7 events at less automated organizations.

Why Server Automation Matters: Technology KPI Performance

Improve SLAs Adherence

While highly automated organizations experience fewer issues, because their staff is less bogged down with manual tasks when problems do arise, they are much more responsive compared to less automated organizations, **meeting SLAs 68% of the time on average compared to 59%.**

Why Server Automation Matters: Business Transformation

Gaining an “agility edge”

Highly automated organizations eliminate mundane, manual tasks and can redeploy more IT staff towards more transformational goals. This is apparent when looking at business agility KPIs:

85% of highly automated organizations say they are successful at developing and launching new products and services relative to their competitors and they are **26% more likely to be very successful compared to less automated organizations.**

TOP-LINE REVENUE GROWTH

Ultimately, the benefits achieved from extensive automation of server tasks become visible in a company’s financial performance. **On average, highly automated organizations expect to increase their revenue 1.7X more than less automated organizations.**

Proving the Value of Becoming a Leader: The ROI of Risk Reduction

Investments in infrastructure technologies, like PBDPAs, are made in part to help organizations maximize uptime and availability and minimize security risk. But do Leaders, who make bigger bets on trusted technologies, get more bang for their buck?

92% of Leaders report that investments in infrastructure technologies to maximize uptime and availability and minimize security risk have **met or exceeded ROI forecasts.**

Leaders were also 1.6X more likely than Laggards to report ROI for these investments **has exceeded forecasts.**

Leaders are 2.2X more likely than Laggards to feel their investments in infrastructure technologies to maximize uptime and availability and minimize security risk **have greatly reduced organizational risk.**

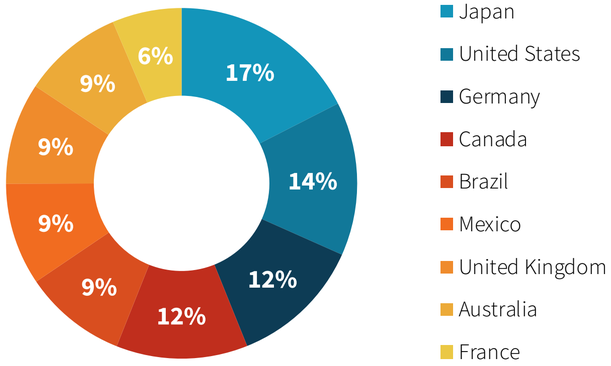
Methodology and Demographics

Data in this eBook comes from a comprehensive online survey of IT decision makers. 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 mid-market: All respondents must have been employed at organizations with between 100 and 999 total employees.

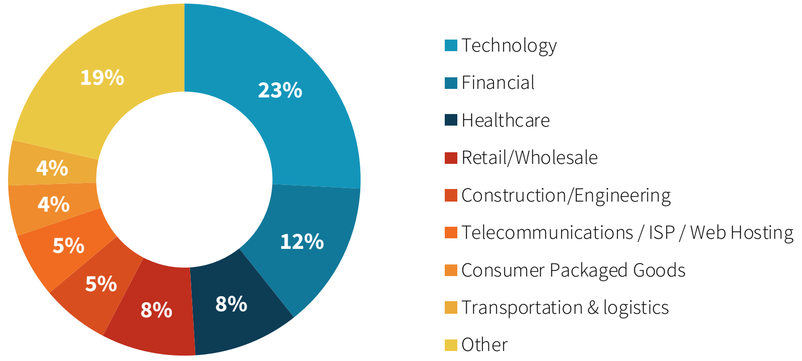
After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 1,650 respondents remained.

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

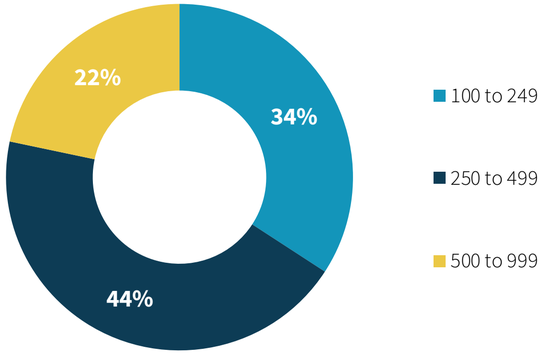
Respondents by Country



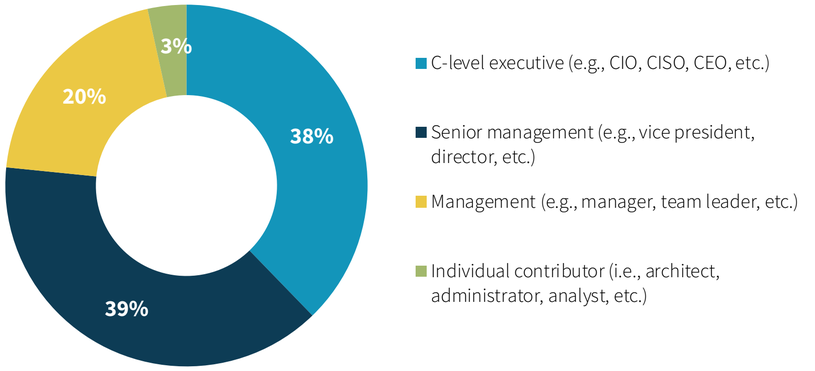
Respondents by Industry



Respondents by Company Size (Number of employees)



Respondents by Job Title/Level



About Dell Technologies:

With the broadest portfolio of trusted infrastructure and data protection solutions, Dell EMC Technologies provides real expertise for end-to-end security, enabling mid-market businesses to adopt transformative technologies to maximize performance, compete, and grow.

LEARN MORE

About Intel®:

Today's organizations face strategic challenges as they modernize data centers and servers. Intel® is driving platform innovation and next-generation capabilities across every infrastructure domain—from compute to storage to network to memory to accelerator technologies. With Intel®architecture-based platforms, you have a clear path forward for the data-centric era.

LEARN MORE