

# Digital Resilience Pays Off

Research reveals every organization suffers from disruption. Investing in critical capabilities enables some to win.



# Executive Summary

Virtually all organizations have experience dealing with outages, system failures and breaches, especially over the last two years. But why were some able to handle them better than others?

To find out, Splunk surveyed over 2,100 security, IT and DevOps leaders at large organizations in 11 countries and across more than six industries. We identified four different stages of resilience maturity — Beginning, Developing, Intermediate and Advanced — and learned how the right investments pay off.

The survey found that organizations that got resilience right are not only able to survive, but thrive. Despite the challenges of a global pandemic and rising economic and political instability, the most advanced organizations save an average of \$48 million a year, according to the survey.

Instead of focusing on narrow aspects of resilience, like disaster recovery or business continuity planning, these organizations developed five critical capabilities: visibility, detection, investigation, response and collaboration.

This study proves the ROI of resilience. Advanced organizations are better at minimizing downtime costs, preparing for change, driving more effective digital transformation, and meeting

or exceeding their financial performance goals. The report identifies where companies can kickstart their resilience journey with key drivers that yielded the most benefit: cross-functional crisis management, automated incident response and collaboration to support accelerated release cycles.

The survey found almost half of all organizations are not fully ready to adapt to disruptions from either a recession (48%) or competitors (50%). In the meantime, macro market events, security breaches, infrastructure outages and other challenges that can bring organizations to a standstill show no sign of letting up. Consequently, CISOs, CIOs and CTOs must prepare today to keep their organizations moving forward.

## Digital resilience

Is the ability to prevent, detect, recover and respond to events that have the potential to disrupt business processes and services.

# The challenge: Disruption is a certainty

The pandemic and other major disruptions have changed the reality of what it means for organizations to operate effectively today. Despite this constant change, customers and users continue to expect secure, seamless, always-on experiences. The pace of transformation and the stakes for organizations to get it right have never been higher.

This is the new normal. And while no one is immune to disruption, organizations that invest in resilience realize immense advantages.

Advanced organizations that get resilience right save on average \$48 million annually in downtime costs, according to our survey. These companies can better manage day-to-day operations, withstand major shocks and embrace transformation.

## Methodology

Researchers conducted a global survey of over 2,100 security, IT, DevOps and leaders across 11 countries in October 2022. Respondents were director-level or above at organizations with at least 1,000 employees.

**11 Countries:** Australia, Brazil, Canada, France, Germany, India, Japan, New Zealand, Singapore, United Kingdom, United States

**7 Key Industries:** Financial services, Healthcare, Manufacturing, Public sector, Retail, Technology, Telecommunications

## Five Key Resilience Capabilities

We asked respondents to answer 26 questions about five key capabilities to assess their resilience maturity. These questions probed on specific aspects of each capability, such as data coverage across hybrid and multicloud environments, alert triage, sharing data across security, IT and DevOps and more.

### Visibility

How well teams can see across their technology environment, including quality and fidelity of data and completeness of coverage

### Detection

How well organizations leverage data to identify potential issues, including detection coverage and alerting

### Investigation

How well organizations use data to search for potential issues and accelerate analysis, including enrichment, threat hunting and searching logs, metrics and traces

### Response

How quickly security, IT and DevOps teams respond to day-to-day issues or incidents

### Collaboration

How well teams and the tools they use facilitate working cross functionally across security, IT and DevOps

Advanced organizations that get resilience right **save on average \$48 million annually** in downtime costs.

## Organizations are rethinking resilience

Historically, leaders have thought of resilience as limited in scope to audit, risk and compliance functions. Disaster recovery and business continuity plans are often seen as a checkbox for management.

In today's world, resilience has become strategic and needs to be embedded into organizations' plans, decisions and technologies.

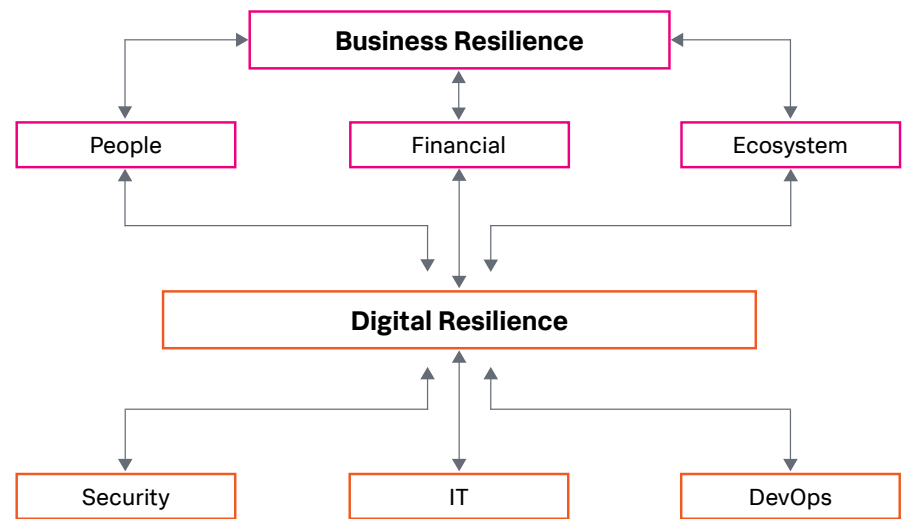
Resilient organizations are able to prevent, recover, survive and thrive amidst disruption and quickly, repeatedly adapt to new operating models. They can not only bounce back, but also move forward in the face of a continuously changing landscape.

## The key to enterprise resilience is resilient digital systems

In the past few years, digital has gone from supporting organizations' operations to being core growth drivers. That means that as enterprises experience disruptions, the potential stress and strain on their digital systems have a far greater impact across their organizations.

Even though leaders have to consider many aspects when building a resilient enterprise — finding and retaining the right talent, ensuring healthy financials, having reliable partners and suppliers — underlying it all are their digital resources. As organizations become increasingly digital, they are only as resilient as their digital systems.

## A Framework for Business Resilience



Business resilience has many components. **Digital resilience** unifies security, IT and DevOps as the foundation for business resilience.

This requires involvement from all of their technology teams — across security, IT and DevOps. Disruptions in recent years like outages and breaches have revealed how a traditional, siloed approach across different functions can create risk. Richard M Marshall, principal at Concept Gap, explains that historically, “... You would have the developers build something and throw [it] over the walls to the operations people who were expected to make it work and the security people would sit off on the other side and nobody would talk to them.”

Forward-thinking organizations know this approach doesn't work. Today's effective organizations are building a unified resilience strategy spanning multiple functions so they can manage and overcome disruptions.

## Stages of resilience maturity

A new approach means technology and security leaders must revisit how they assess their resilience posture. They must now be able to articulate the value of their investments in resilience and show progress along a maturity curve to their boards of directors and the rest of the C-Suite.

According to Sean Crabtree, managing director at Accenture, “Every business in the future will be a technology business if they are not one already ...

Building resilience into the capabilities that enable your business products, [and] your people who are driving those capabilities is absolutely essential.”

The survey found organizations are at various stages of their maturity. One in five of them are at the beginning of their journey and one in six are considered Advanced. Most, however, are in the middle of the pack — strong in some areas and running up against challenges in others.

The research showed Advanced organizations have the capabilities they need to win, particularly during times of disruption [[see Methodology](#)]. For example, these organizations have superior visibility, with coverage across different data sources in IT, security and DevOps, and stronger response, with the ability to predict and prevent incidents using machine learning and auto remediation. Ultimately, these capabilities drove better business outcomes, including top and bottom line results.

## Stages of Resilience Maturity

Beginning

20%

Developing

29%

Intermediate

35%

Advanced

16%

# Key Findings

Investing in resilience pays off in four ways. Compared to their peers, we found Advanced organizations have more success:

- Minimizing downtime costs
- Preparing for change
- Driving effective digital transformation
- Achieving financial performance goals



# Minimizing downtime costs

## All companies experience a significant amount of downtime

**Downtime happens.** Whether from an outage, breach or other event, unplanned downtime that negatively impacts customer experience, revenue or productivity is inevitable for almost all organizations. Respondents reported an average of 240 hours of downtime — or ten days — each year. This finding was consistent across each stage of maturity — Beginning, Developing, Intermediate and Advanced.

Regardless of how prepared organizations are, they will have to contend with unplanned downtime. When asked what type of threats or events have the greatest potential to disrupt their organizations, one in four survey respondents said infrastructure outages and one in five cited ransomware.

The stakes are high. Each hour of downtime costs about \$365,000, which means an organization can expect to face an average of \$87 million per year in downtime costs from lost revenue and productivity.

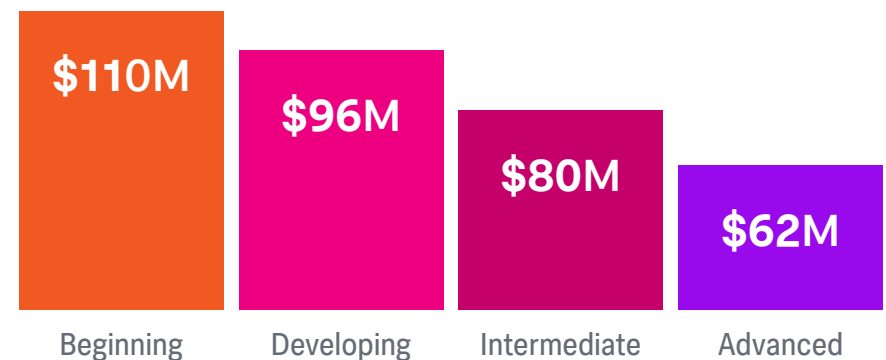
Organizations face an average of **\$87 million per year** in downtime costs from lost revenue and productivity.

## Advanced organizations minimize the impact of outages, saving about \$48 million per year

In this reality, dealing with significant unplanned downtime is a matter of “not if, but when.” However, organizations that invest in resilience are able to mitigate the impact of disruptions and save big compared to their peers. Our research showed the Advanced group incurred significantly less downtime costs annually (\$62 million) when compared to the Beginning group (\$110 million).

What might be going on here underneath the hood? With greater visibility and more powerful investigation capabilities, Advanced organizations are able to prioritize their responses according to organizational impact — to focus on getting their revenue-generating app back up and running, for example, and worry about getting an internal collaboration tool used by just a few teams back online later.

## Unplanned Downtime Cost, Per Year



This finding is in line with advice from Marshall that organizations learn to expect the unexpected and focus their efforts on softening the blow:

“You learn to fall safely without hurting yourself. Resilience is about knowing what’s going to go wrong and what could potentially go wrong, and then realizing what you don’t know.”

### Industry Insight: The financial services industry has the highest downtime costs

Downtime has steep consequences across sectors. However, compared to industries such as public sector, technology, telecommunications, healthcare, retail and manufacturing, the cost of downtime for a company in financial services is significantly higher at about \$141 million per year. This finding is in line with high rates of adoption for digital banking and online trading, which incur steep losses during outages.

Financial services organizations face **\$141 million** in downtime costs per year, **\$54 million** higher than the average across industries.

### Key Driver:

## Cross-functional crisis management is critical

Downtime hurts most in times of crisis, such as during the Log4shell or the Colonial Pipeline attacks. These events require teams across security, IT and DevOps to coordinate crisis management cross-functionally, and we found most (96%) organizations do so for at least some of their products or services.

However, those that don't (4%), suffer far more pain — unplanned downtime costs them a whopping \$211 million per year. The research shows crisis management is a critical place to start to implement processes and tools to improve resilience.



# Preparing for change

## Most organizations are not ready to adapt

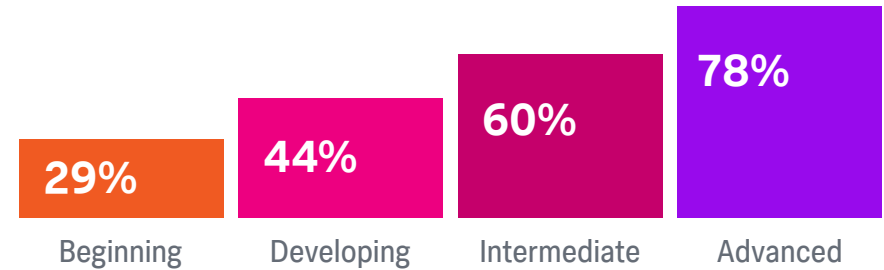
On top of incidents that lead to downtime, larger macro events continue to threaten organizations — from an economic recession to industry disruption. Organizations that fail to adapt will cease to exist.

Only half of organizations strongly agree they are prepared to change how they operate and engage with customers during times of major disruption, either to address the demands of a recession (52%) or in response to competitors (50%).

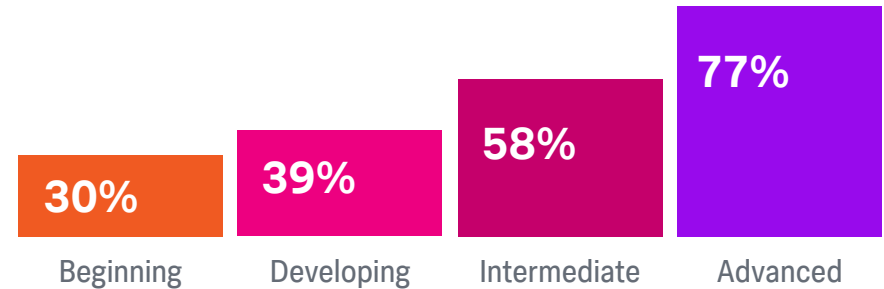
## Advanced organizations are 2.5 times more likely to be prepared

When those results are broken out by resilience maturity stage, the findings are revealing. Over three quarters of Advanced organizations say they are prepared both to adapt to meet the demands of a recession (78%) and disruptions from competitors (77%), while about a third of Beginning organizations (30%) can say the same.

## Prepared for Demands of a Recession



## Prepared for Disruption by Competitors



Building resilience capabilities gives organizations a foundation of reliability and security so they can spend more time innovating. In other words, Advanced organizations can focus on developing new features, finding new ways to deliver products and services or expanding to new markets to capitalize on opportunities.

Winners in times of change are able to rapidly adapt and take advantage of shifts in market forces. For instance, workforce solutions company ManpowerGroup is a \$19 billion business that works with 400,000 clients and 3.4 million associates each year. They rose to the challenge of addressing talent shortages during the pandemic. Their CISO, Randy Herold, highlighted the impact of investments in resilience for his company to continue to stay ahead. “Visibility is extremely important to our day-to-day operations,” he said. “It’s important to our long-term strategies. That’s important to our innovation.”

## Key Driver:

### Automation helps organizations stay lean

Times of change also leave organizations more vulnerable. When resources are constrained, organizations need to be smarter and more efficient. Enter automation.

Lean organizations use automation to save money, time and do more with less. Advanced organizations adopt automation at higher rates than their peers, with 75% reporting at least half their workflows are automated compared to 39% for Beginning organizations. Specifically, machine learning and auto remediation help these organizations predict

and prevent incidents. Self-healing systems automatically perform tasks, such as restarting applications when they run out of memory, while automated playbooks can isolate hosts infected with malware or suspend accounts suspected of malicious activity. Companies that adopt machine learning and auto remediation across all their products and services are twice as likely (66%) to be prepared for the demands of a recession, compared to those that do not (34%).

# Driving effective digital transformation

## Organizations struggle to extract value

Digital transformation is the name of the game for technology leaders, but it's not easy to get it right. Most respondents (61%) reported less than half of their digital transformation projects had a positive, sustained impact in the last two years.

Large-scale projects, from refactoring code to overhauling infrastructure, introduce complex challenges. For instance, in cloud environments, the attack surface to protect is exponentially larger, and the number of services to monitor is far greater.

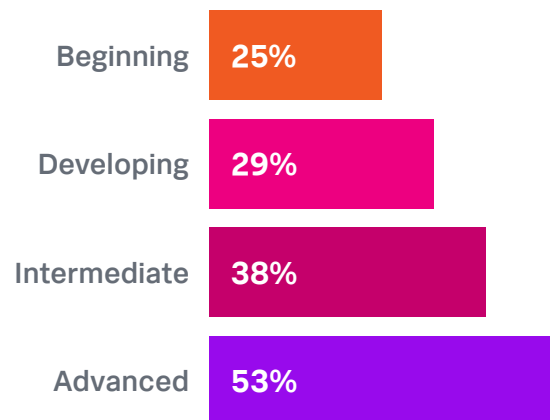
## Advanced organizations are two times more likely to succeed

Advanced organizations are separating themselves from the competition when it comes to digital transformation — they (53%) are significantly more likely than Beginning organizations (25%) to have had a majority of digital transformation projects be successful over the last two years.

Advanced organizations have capabilities that give them flexibility and scalability. For instance, on average they reported 64% of their workloads run in the cloud.

## Digital Transformation Project Success

Organizations that reported the majority of their digital transformation projects had a positive, sustained impact in the last two years.



## Industry Insight: Public sector and telecommunications industries lag behind

Organizations within the public sector (19%) and telecommunications (16%) industries are least likely to report successful digital transformation projects. Lack of investment and reliance on sprawling legacy technology environments make it harder for these organizations to modernize their services. Consequently, these resource-strapped organizations are often more vulnerable to threats. Each ransomware incident costs K-12 organizations an average of \$2.7 million, compared to \$1.8 million for the private sector, [according to the Splunk Public Sector Predictions 2023 report](#).

## Digital Transformation Project Success by Industry



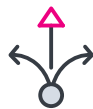
19%

Public Sector



16%

Telecommunications



35%

All Other Industries

### Key Driver:

## Accelerate release velocity with support from security and IT

During software releases, security and ITops teams can be seen as blockers or the voice of “no.” Yet collaboration is important for organizations to have successful digital transformation efforts. Companies where security and IT teams support initiatives to accelerate the release cycle across all products and services are two times more likely (39%) to find digital transformation success, compared to when these initiatives were absent (21%).

Faster, higher-quality releases fuel digital transformation. This finding underscores that organizations need all their technology teams working toward the same goals — at speed — to be successful.

# Achieving financial performance goals

## Expectations are intensifying

Organizations should invest in resilience to mitigate downtime, adapt to macro changes and execute on digital transformation. But organizations must also show ROI in their financial performance for investors.

Recent market volatility combined with budget cuts and inflation create significant financial pressures. Meeting investor expectations in this environment is no easy task.

## Advanced organizations outperform others in top line results

We saw advanced organizations surpass their peers, with a 17 percentage point difference between Advanced and Beginning organizations in terms of having met or exceeded their growth goals in the last fiscal year.

For publicly traded companies included in the study, we saw similar results when looking at stock price growth. Advanced organizations (82%) are significantly more likely than Beginning organizations (70%) to have seen stock price growth since January 2020.

## Stock price growth

Publicly traded organizations reported changes in stock price from the period January 1, 2020 through January 1, 2022

**82%**  
of Advanced organizations  
reported growth

**70%**  
of Beginning organizations  
reported growth

These findings suggest two things: not only are advanced organizations making the right investments in resilience, but they are also seeing significant value from their resilience capabilities. As economic pressures continue to intensify, technology and security leaders should move from treating resilience as a cost to an investment that supports positive returns.

# Build a foundation of resilience for tomorrow

The findings of this study make it clear that investing in resilience has high ROI. Advanced capabilities in visibility, detection, investigation, response and collaboration yield massive payoffs in:

- Minimizing downtime costs
- Preparing for change
- Driving effective digital transformation
- Achieving financial performance goals




Given the never-ending potential for disruption, technology and security leaders should invest in strengthening each of these capabilities to advance their organizations' maturity. Organizations can kickstart their efforts by improving cross-functional crisis management, leveraging machine-learning and auto remediation, and empowering security and IT to accelerate release velocity. By building a strong foundation of resilience, leaders can ensure their business is prepared to adapt to anything.

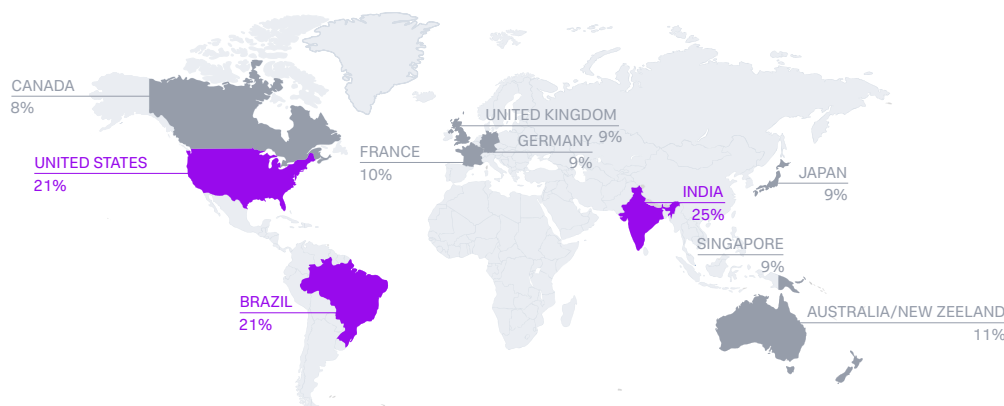


# Appendix

## Which countries are most Advanced?

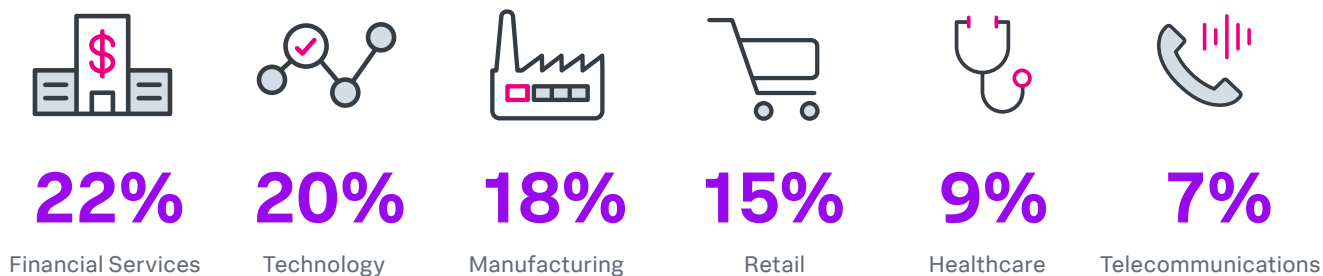
Of the eleven countries included in the study, India, Brazil and United States have the highest percentages of Advanced organizations

-  More Advanced organizations
-  Less Advanced organizations
-  Not surveyed



## Which industries are most Advanced?

Of the industries included in the study, financial services, technology and manufacturing have the highest percentages of Advanced organizations



[Learn more](#) about Splunk's perspective and how we help organizations improve digital resilience.

