IDC

ANALYST CONNECTION

Sponsored by: Splunk

Business resilience depends on comprehensive visibility spanning infrastructure, data, and applications to enable consistent, proactive security and performance across the organization.

Visibility into Digital Operations Powers Business Resilience

September 2022

Questions posed by: Splunk

Answers by: Mary Johnston Turner, Research Vice President, Future of Digital Infrastructure

Q. What are digital leaders telling IDC about their business resilience priorities?

A. IDC's research shows that business leaders around the world are working every day to enable digital business transformation and maintain business resilience in the face of rising cyberthreats, rapid digital innovation, high inflation, extended supply chain disruptions, and ongoing geopolitical uncertainties. These decision makers understand they need to create and maintain highly resilient digital systems that can handle a wide range of unexpected situations. They need to be able to respond to business, economic, climate, and security threats on the fly. They also need to be in a position to rapidly pivot resources and adapt workflows as needed while maintaining high levels of security and performance.

Beyond just keeping the business going, these digital leaders recognize they need to invest in platforms and services that support ongoing business transformation using DevOps, AI/ML, and advanced automation to adapt existing processes and to create new revenue streams. During the pandemic, the organizations that were most resilient were able to rapidly stand up online delivery platforms or enable work-at-home capabilities without disrupting critical business processes. In a recent IDC survey, 80% of decision makers worldwide identified the resilience of their digital infrastructure — spanning datacenters, public clouds, and edge resources for computing, storage, data management, and networking — as being important or mission critical to achieving key business goals. These goals include faster digital business innovation and agility, improved sustainability, better quality of data-driven decision making, and greater customer satisfaction and employee productivity. These organizations recognize that digital resilience is the foundation for ensuring business resilience.

Q. What are some of the technology challenges organizations face while building business resilience?

A. As business becomes more digitized, business applications and data are becoming more distributed across mobile systems, campus, and edge platforms as well as datacenters and multiple public clouds. Data integration, protection, and security are increasingly complex. Often, individual teams make independent decisions about security, software, and cloud services. This strategy enables rapid time to market but can result in pockets or silos of resilience where the security and performance of different technologies, data platforms, and applications are managed and protected by disconnected tools and uncoordinated groups of people and processes.

Competing policies, tools, and operational workflows can make it difficult to consistently secure and optimize resources in different locations and business groups. Making things worse, these disconnected operational environments often rely on poorly documented, inconsistent, ad hoc manual processes and depend on slow, time-consuming change control boards, ticket request systems, and similar error-prone approaches to detecting and remediating performance problems and security risks between systems and applications.

Given that agile digital business depends on an organization's ability to quickly access, analyze, and share data between multiple decision makers and business applications, anything that creates barriers to comprehensive and consistent data access, security, and compliance will negatively impact business performance. For instance, inconsistent implementation of data management and data protection policies can put the business at risk by leaving back doors open for hackers.

Q. What strategies can enterprises adopt to overcome complexity and break down monitoring and security silos so they can achieve consistently high levels of business resilience?

A. Organizations are investing more than ever in the core infrastructure, compute, storage, data management, and network architectures needed for effective data-driven decision making in the face of a rapidly changing business landscape. IDC's recent worldwide survey of digital infrastructure decision makers shows that 80% of organizations worldwide are planning to invest in new, high-performance computing for new data-intensive workloads; 77% also noted the need for better connection with edge, campus, and work-from-home locations. These trends are driving major changes to networking architectures and interconnection strategies — two top priority areas identified by over 50% of organizations.

As enterprises expand the scale and scope of their digital business footprints, it becomes almost impossible for traditional monitoring and security tools to efficiently handle the rising volumes of operational data. Traditional domain-specific tools or point solutions provide limited visibility across these dynamic modern environments because they are generally designed to work with specific types of monitoring data and may not be able to fully assess end-to-end workflow and data analytics dependencies. To provide full digital business resilience, IT operations staff, skills, tools, and processes must adapt to a new strategy. They need to be able to pull together and analyze monitoring, security, and performance data in context on an end-to-end basis. This type of comprehensive visibility enables organizations to integrate operational workflows and automation to manage the environment consistently on an end-to-end basis, regardless of whether the managed resources are deployed in datacenter, edge, or public cloud platforms.

Comprehensive visibility and understanding of dependencies, health, security, and performance across multiple platforms, applications, and services are required to be able to efficiently optimize digital business performance and to ensure consistent data protection, privacy, and compliance.

Q. Can you say more about the people and process side of business resilience? Do organizations need to make changes to current practices?

A. Even the best-trained staff will struggle if forced to rely on manual processes and disconnected management solutions across today's interconnected digital business environments. Maintaining visibility across diverse platforms, services, and applications depends on having access to comprehensive management data, analytics, and automation. To improve productivity and ensure consistent business performance, all technology teams across IT, security, and DevOps need access to a unified platform that can ingest, correlate, search, analyze, and take action on large volumes of logs, traces, and metrics in the shared context of the organization's security and performance policies and business KPIs.

IDC's research shows that the most effective organizations simultaneously modernize governance approaches to better align security, IT and cloud operations, DevOps, and data management with top priority business outcomes such as increasing time to market or improving customer engagement and personalization. Many are evolving traditional change control boards and ticket-driven operations to become more agile and policy driven. As predictive analytics become more robust, organizations can improve business resilience by allowing selected workflows and operational IT changes to execute dynamically based on event-driven triggers.

Q. What are the most important technology trends organizations should consider as they seek to ensure resilience in the long term?

A. We know that the trend toward complexity isn't going to change. Workloads and infrastructure are going to become more and more distributed. New computing capabilities such as non-x86 high-performance computing platforms will be introduced, and most organizations will continue to rely on multiple public clouds. Simultaneously, end users expect access to more real-time automated self-service capabilities and developers will continue to innovate using cloud-native containers and microservices-based approaches. And of course, existing datacenters and VM and bare metal workloads continue to be important to the delivery of critical business services.

Maintaining performance, compliance, and security across this constantly evolving infrastructure depends on having consistent comprehensive visibility, predictive analytics linked to actionable policies, and AI/ML-driven operations. Highly resilient digital business environments will need to proactively detect potential security threats or unexpected changes in performance and act quickly to remediate these situations in order to prevent and/or reduce the impact of disruptive and potentially damaging events.

A highly resilient organization is able to withstand more volatility and potential threats if it is equipped to predict and automatically respond to issues. Organizations should be working today to break down operational silos, align operations with business priorities, and implement a more unified, predictive approach to ensuring consistent security, compliance, and performance across their digital business portfolio.

About the Analyst

Mary Johnston Turner, *Research Vice President, Future of Digital Infrastructure*

Mary Johnston Turner is Research Vice President, Future of Digital Infrastructure, part of IDC's Future Enterprise research team. She analyzes how enterprise IT and business strategies are taking advantage of ubiquitous, autonomous cloud infrastructure solutions deployed across dedicated datacenter and shared public service environments. Her practice emphasizes the voice of the enterprise customer, based on surveys and in-depth analysis of best practices related to how enterprises are changing the ways they source, secure, and optimize digital infrastructure solutions. Her research emphasizes consideration of how pay-as-you-go consumption-based subscriptions, cross-cloud control planes, and collaborative enterprise infrastructure governance models are enabling enterprises to better align infrastructure investments with critical business outcomes and innovation priorities.

MESSAGE FROM THE SPONSOR

Resilience requires visibility. Splunk lets you see everything so you can act fast and adapt to anything.

Get the end to end visibility you need to understand the impact of any change in your environment. Power rapid time to action with robust investigation and automation, and enhance detection and collaboration across teams with a unified security and observability platform.

With Splunk, security and technology leaders can build resilience at all levels – from managing day to day operations to withstanding major shocks. Organizations can turn resilience into a competitive advantage by using Splunk to move beyond reacting to change to embracing transformation. Find out more about building resilience with Splunk.

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.