IDC

SPOTLIGHT

Sponsored by: Cisco

Digital resilience is a growing focus for C-suite executives, but it remains challenging to deliver. Enterprises need good data on system performance and behaviors to drive fast detection, investigation, and resolution of issues.

Digital Resilience Is a Data Problem

May 2025

Written by: Duncan Brown, Group Vice President, Software, Services, Cloud, Security, Sustainability, Digital Business, and IPDS

Introduction

Digital resilience is a key priority for organizations. IDC's 2024 *CEO Survey* revealed that digital resilience is a top focus for executives and, by extension, their CIOs. Despite this clear focus, less than half of organizations believe that they are sufficiently resilient to effectively maintain service levels, security, and costs in the face of unexpected events.

So, what will it take to change this situation?

Organizations must address the key challenges related to digital resilience, which cluster specifically around data, and manifest as a trio of distinct, but related, issues:

- **Location and source issues:** Network, security, and application data exist in disparate systems, each generating their own formats and maintaining separate records, making it historically impossible to establish a unified source of truth for system health and performance.
- **Organizational and workflow problems:** Specialized teams operate within technical silos, using domain-specific tools and processes that aren't designed to share critical information across functional boundaries, resulting in fragmented visibility and response capabilities.
- **Analytical and contextual challenges:** Despite abundant data collection, organizations lack the correlation mechanisms to connect related events across domains, leaving teams struggling to extract meaningful patterns and identify root causes from disconnected metrics and alerts.

In the past, teams may have coped with this by throwing resources (e.g., time, money, and technology) at maintaining resilience, but today's economic, regulatory, and technology pressures mean that organizations must change the way they think about digital resilience.

AT A GLANCE

KEY TAKEAWAYS

- Digital resilience is primarily a data problem. The ability to harvest and analyze data across the enterprise, and to extract insights from it, is essential in assessing and managing risk and in detecting and remediating risks impacting business.
- Technology solutions that address digital resilience have data management features to integrate with multiple sources of data, whether through direct ingestion or federation. They also have strong analytical capabilities that provide real-time insights on risk exposure.

They must be:

- Proactive in preventing issues — detecting threats, avoiding lateral movement, and catching misconfigurations
- Responsive when things go wrong — finding the problem quickly and remediating automatically where possible
- Efficient and effective across all system elements — including network and applications

The Core Components of Digital Resilience

Building digital resilience requires visibility and insights across an organization's entire footprint. Digital resilience requires good data, but that data is hard to access — data is typically dispersed across an organization, with no application of a coherent or cohesive structure to relevant data sources. Data that may be pertinent to an organization's resilience includes network traffic analysis, IT topologies, configuration data, and security vulnerabilities and risks, as well as a host of outputs, such as logs, metrics, events, and traces. Typically, the main sources of data will be in network operations (NetOps), security operations (SecOps), and IT operations (ITOps). These teams are often in silos, with little data transfer or commonality between workflows. This lack of collaboration is usually less about organization structures and more about incompatibilities between tooling in each of the three areas.

To enable digital resilience through data, organizations need to:

- See what is happening across the organization
- Act on what is visible
- Automate the activities that make an organization resilient through AI and real-time monitoring

See What's Happening

Observability allows an organization to understand its state and system behavior based on the collection and analysis of a variety of system information. Evolved from system monitoring, observability identifies sources of problems by providing a view of performance based on real-time or near-real-time data, enables fast troubleshooting, and identifies paths to resolution. It can also help in detecting potential problems before they materially impact users.

It's important to extend this level of visibility to network infrastructure on which organizations depend, even those elements of connectivity that are not owned by that organization. Seamless connectivity across cloud, internet, and enterprise networks is required to deliver assurance of applications and services.

Enterprises also need visibility of the full range of security telemetry that establishes the foundation for threat detection, investigation, and remediation.

Acting on Data — Delivering Resilience

The provision of good data through observability and security analytics platforms allows organizations to quickly identify issues, which they can then remediate. For example, if a particular cloud service goes offline, it is important to understand whether it is a network connectivity issue, a cloud service provider outage, an API call misconfiguration, or another source of interruption.

Once the organization has correctly identified the issue, it is crucial that it responds quickly and effectively, preferably in an automated fashion. It should also take preventative action to eliminate future occurrences.

Of course, internal problems are not the cause of all issues. Organizations are continually susceptible to external security threats, as well as network, cloud, and SaaS app outages, but these can be dealt with in a similar way, identifying threats, vulnerabilities, and outages that need investigation and quick remediation. Again, having good visibility of system behavior is essential to fulfilling this process.

Automating Resilience

Effective management of IT and network systems requires the application of automation, again founded upon reliable data sources. Real-time monitoring, including AI-enabled detection of problems, can help drive automated workflows. Ideally, these workflows should span across NetOps, SecOps, and ITOps in a seamless manner while preserving individual teams' ability to maintain control of the tools and systems they rely on.

Complexity Reshapes Digital Resilience

Digital resilience covers a wide range of disciplines and concerns. IDC's 2024 *CIO Sentiment Survey* reported that resilience includes varied aspects, such as application uptime and availability, cybersecurity incident response, physical infrastructure failures, and supply chain disruptions.

The reliance on IT and networks for business operations and a commensurate exposure to downtime have been the primary drivers of the focus on digital resilience in recent years. External factors can further exacerbate this — we have seen a pandemic, wars, and trade disputes all influence business operations in recent times, as they impact resource availability, the likelihood of cyberattacks, and even the supply of power.

In many cases, organizations are mandating digital resilience while the supporting IT and network estates increase in complexity. Cloud, remote working, and AI are examples of drivers of increased IT and network complexity. In such an environment, the requirement to have real-time data on system behavior is critical.

Considering Cisco's Approach to Digital Resilience

Cisco delivers assurance primarily via its ThousandEyes product, aimed at network and IT teams. It helps ensure the delivery of reliable connectivity across owned and unowned assets by diagnosing potential points of failure. For example, it spans cloud resources and network infrastructure, including the internet and enterprise networks. Cisco has integrated ThousandEyes across its entire portfolio, offering comprehensive coverage, even including networks beyond the enterprise boundary.

The ability to baseline network performance and establish benchmarks allows fast diagnosis of performance issues outside the expected performance parameters. It also enables predictions of network performance and a path to optimization.

Observability

Cisco's observability capability is provided primarily by the company's Splunk Observability Cloud product, ThousandEyes, and the AppDynamics application performance monitoring product, which is now integrated within the Splunk family. Data can feed from these sources into the Splunk platform, which can then drive the IT Service Intelligence capability.

With a broad portfolio that provides end-to-end service visibility, it is possible to detect service performance issues instantly. For example, in the case of a system failure, ThousandEyes can verify network paths, Splunk Observability Cloud can validate cloud resources, and AppDynamics can confirm the availability of impacted applications and databases. With this information in hand in real time, response actions can initiate automatically.

Security

Cisco's security operations portfolio is extensive and comprises Splunk Enterprise Security (a security incident and event management [SIEM] product), Cisco XDR, and Splunk SOAR, plus Splunk Asset and Risk Intelligence and the Splunk Attack Analyzer investigative product. Collectively, the portfolio addresses threat detection, investigation, automated response, and the management of security operations.

Together, the security portfolio enables the real-time monitoring of an organization's entire estate. Using AI, it can reduce noise and detect live threats, helping security teams prioritize genuine incidents. Automated incident investigation drives down response times and helps optimize SOC efficiency in an integrated manner.

Challenges

In its acquisition of Splunk, Cisco has added substantial security capability to its portfolio. The primary challenge with any acquisition is integrating the portfolios into a cohesive platform, not just in terms of market positioning but in terms of workflow integration, data sharing, and automation across the portfolio. While the open nature of Splunk makes this task easier than it might otherwise be, there will be an inevitable lag between full integration across the portfolio and market expectations. However, many capabilities inherited from Splunk are designed to be vendor and data type agnostic, which makes integration challenges more straightforward than they otherwise might be.

Security teams typically deploy a wide range of tools. While IDC's research shows that there is a growing trend to reduce the number of security vendors and security products, most organizations are in the early stages of this transition. Pragmatically, SecOps teams need an integrated set of products able to share data and automate workflows. To provide a fully resilient IT and network estate, Cisco must demonstrate an ability to integrate with other security tools, especially those outside the network domain. This would include identity and access management solutions and data protection products.

On a wider scale, most enterprises have a heterogeneous environment. Delivering 100% visibility across the entire estate will always be a challenge for any organization. Although the Cisco observability portfolio is strong, it depends upon the ability of third-party products to share data, APIs, and other integration features.

Conclusion

Digital resilience is a key focus for many enterprises and has the attention of CEOs. Delivering digital resilience depends on the availability of and access to data regarding the performance and behavior of IT and network systems. That data then drives the detection of issues and the subsequent remediation of those issues, often in an automated response. Digital resilience hinges on data and visibility across the IT and network estate, and Cisco's extensive portfolio in this area positions the company well in this regard.

Digital resilience hinges on data and visibility across the IT and network estate.

About the Analyst

Duncan Brown, *Group Vice President, Software, Services, Cloud, Security, Sustainability, Digital Business, and IPDS*

Duncan Brown leads European research for the Software, Services, Cloud, Security, Sustainability, Digital Business, and IPDS areas, as well as the Channel Partner and Ecosystems research teams. He is also responsible for IDC's European research into the Future of Work, Future Consumer, and Smart Office areas. He has a strong focus on team development and thought leadership, as well as working with sales, marketing, and consulting to help build IDC's European business. Brown leads IDC's pioneering EMEA Chief Information Security Officer (CISO) outreach program.

MESSAGE FROM THE SPONSOR

Digital resilience is the ability for an organization to keep their business securely up and running in the face of any disruption. This involves proactively preventing, detecting, investigating, and responding to potential issues. Cisco helps organizations build digital resilience by providing visibility and insights across the entire digital footprint, uniquely combining the power of the network with security, observability, and assurance.

With Cisco, organizations are able to prevent incidents from becoming major issues, remediate quickly if something does happen to minimize business impact, and be in a position to adapt to anything and take advantage of new business opportunities.

Learn more about how Cisco delivers Digital Resilience.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2025 IDC. Reproduction is forbidden unless authorized. All rights reserved. CCPA