CONTINUITY SOFTWARE

Hybrid Is In.
Outages Are Not.

An Integrated, Proven Approach to Handling Outage Risks and Cyber Threats

Table of Contents

Introduction: IT Environments are Always Evolving

Hybrid IT environments are the new normal

During the past decade or so, IT environments have changed profoundly and as a consequence, the challenges of keeping them resilient have grown greater. Not that long ago IT enterprise infrastructure consisted of physical datacenters. Not anymore. Today, in addition to on-premises equipment, they have evolved to also include multiple private clouds and public clouds, circumstances which make most enterprise IT environments hybrid.

The technological evolution that occurred and which continues is, in a large part, due to cloud computing. When the public cloud first emerged in about 2006[1], it played a miniscule role, with about two percent of all workloads worldwide being managed there.

Since then, the industry has recognized the many technological, growth, agility, economic, and other advantages of cloud computing and in response, the cloud landscape has evolved dramatically. In its 2019 "State of the Cloud," Right Scale reported[2] that 94% of their respondents use the cloud, run applications on an average of five clouds, and nearly 60 percent of enterprises have a hybrid cloud strategy.

The parallel growth of "Software, Infrastructure, Platform as a Service" solutions, containers, Kubernetes, and IT sprawl

In and of themselves, complex, hybrid IT arrangements would be challenging enough to maintain so as to ensure that applications and services are always available. Complicating this reality further is the use of containers to run applications, which is becoming standard, as is Kubernetes or other orchestration solutions and the fact that many enterprises use hosted cloud services for critical components such as infrastructure, platforms and of course, business applications. These shifts toward the virtual and the software-defined require IT teams to use a different set of tools and skills than in the past when enterprises had their own software and managed their workloads on physical, on-premises datacenters.

Complexity enables simplicity

There is a plus side to growing IT environment complexity because its ultimate objective is to provide increasing simplicity and responsiveness to end users. No matter the type of enterprise – from financial institutions to retail organizations to airlines, and others - more and more data, information, ability to conduct transactions, provide services, and other essential activities are at the fingertips of business users within the organization. And, by extension, these capabilities are employed in order to allow the business to be agile and respond more quickly to user needs.

> The big and urgent question is how to technologically support these hybrid/ modern IT environments and ensure they are resilient and secure.

1. VMware, "Balancing Freedom and Control: Evolution of the Cloud – 2006-2030," October 2016.
2. RightScale "2019 State of the Cloud Report": https://www.rightscale.com/

Assuring Resilience is an Evolving Challenge

Gone are the times when IT was responsible for resilience only in its own backyard – i.e., the enterprise's physical datacenter. Today's hybrid IT environments reside in multiple physical and virtual locations; infrastructure, platforms and software are hosted virtually; and applications operate out of containers orchestrated on Kubernetes platforms.

Despite such "decentralization," responsibility for the environment's resilience and availability still lies with the enterprise's IT operations team. And while it's clear that these types of setups are agile and responsive to business needs, they present formidable challenges to assuring resilience. Multiple in-house, third party and vendor teams are involved in carrying out system maintenance, updates and upgrades, which makes it all the more difficult to effectively monitor IT environments. IT teams are required to have "a granular view of business processes across applications and the supporting components, while understanding the dependencies on integrations and data that might exist across an IT environment." Under the circumstances that prevail today, that's a very tall order, especially in a "complex, patchwork IT environment."[3] where IT owns

Security of core data systems – a growing resilience concern

Ensuring the security of an enterprise's IT environment presents another immense and urgent challenge. Increasingly, enterprises report having been the victim of a malicious attack or of an incident in which data was lost and not recoverable. Close to 100% of enterprises have experienced an incident that impacted data, 17% of which were "severe."[5] In fact, IDC estimates that currently, "as many as 50% of organizations could not survive a disaster event. Many organizations do not have properly protected and staged offsite data, have not tested the DR environment, or do not have automated DR processes as part of documentation and planning."[6]

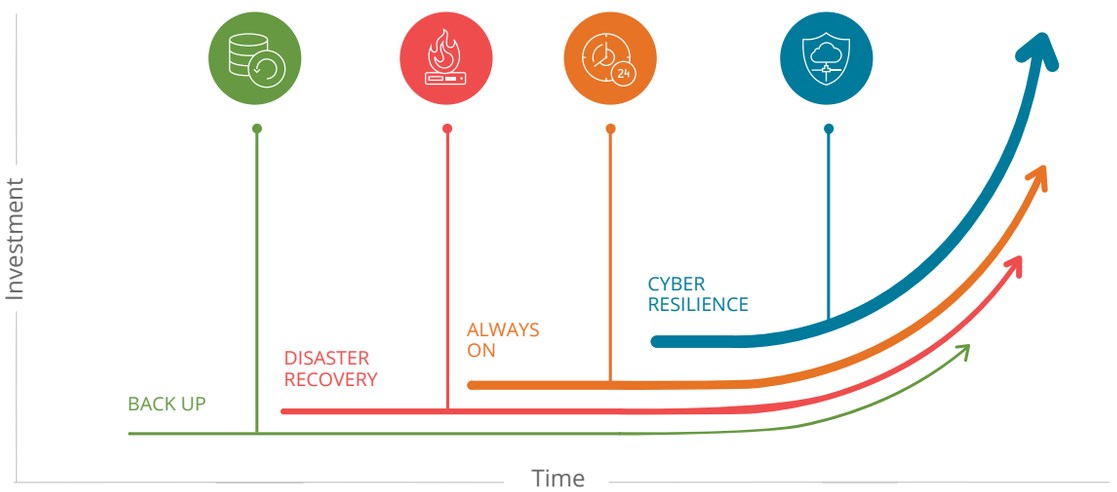
Always-on, no matter what

With the immediacy of IT responsiveness now the status quo, enterprise IT environments are not only required to be "always-on," but in the event of a disruption or an attack, they are expected to be back in operation within diminishing amounts of time, no matter what fault must be repaired, service restored, or data recovered. This is another challenge which places additional pressure on IT teams to do whatever it takes to get the system back up ASAP and only afterwards to look for the root cause that triggered the problem. In this sense, end users are relentless and also impatient, insisting on their routine access to the tools and data they use to perform their work and serve the myriad consumers of their services – both inside and outside the enterprise.

3. Gartner – Transitional Data Services. Welcome to the Age of Digital Transformation, October 2018. http://info.transitionaldata.com/gartner-market-guide-itro
4. VMware, ibid.
5. IDC: Goodwin, P and Smith A. The State of IT Resilience, August 2018. https://www.zerto.com/the-state-of-it-resilience-2018/.
6. IDC, ibid.

Is the Increasing Investment in Resilience Paying Off on all Fronts?

The circumstances described above have led to a change in the challenge of assuring the resilience of IT environments; needs have expanded and are more diverse. Until recently, the resilience mandate meant working to keep IT infrastructure healthy and available. But now, IT environments have evolved, are more complex and include more moving parts so that new factors impact the maintenance of IT resilience. At the same time, the realization has hit that cyberattacks are a likely scenario for enterprises, making cyber resilience now more important than ever. What are the key challenges to maintaining resilience today? And why is it that despite an ever-growing investment in resilience, organizations continue to experience outages and downtime, and are also at risk of a cyberattack on their under-protected, high-value data assets?



Increased investment in resilience: IT teams increasingly required to deliver more

Increasing levels and dimensions of complexity pose new IT and cyber resilience challenges

Addressing the basics first: IT environments. They are hybrid and reside on several clouds and employ diverse technologies; this is sometimes referred to as “chaos architecture.” Maintaining their continuous availability is an increasingly growing challenge for IT teams.

This is due to their complexity – multiple clouds, multiple technologies (such as microservices and containers), multiple layers, connections and dependencies, and because environments are always changing - for example, moving from a monolithic architecture to one based on microservices presents a major resilience challenge. Adding to the “chaos,” alongside the private and public clouds, there are still many enterprises that continue to work with legacy and on-prem systems, and now need to maintain the resilience of this mixed hybrid architecture.

The speeding pace of change

Thousands of new features, improvements, services and capabilities are introduced annually to cloud environments. For example, in 2017, Amazon's AWS added 1,403 new features; the trend continues into 2019 – at times with 10 or more announcements of new capabilities or services per day[7]. Multiply that by the number of cloud providers used by the enterprise, and the implications of keeping up with that number of changes and updates to IT environments are clear, though admittedly hard to grasp. Changes must be seamlessly and properly implemented, assuring they do not upset the equilibrium of configurations in the environment.

The knowledge gap impacting resilience of IT environments

Assuring these decentralized, sprawling and evolving IT environments run glitch-free at maximum uptime is a gargantuan task. IT environments are maintained by multiple teams of specialists – in-house, and those from vendors and solution-providers. The two major issues here are: (1) as with any large operation, communication and coordination are essential; these are often lacking in dynamic IT maintenance efforts where each team may work on their own set of tasks in isolation from others; and, (2) teams working on the environment are not necessarily aware of best practices and inadvertently introduce risks into the works.

Furthermore, because so many changes to IT environments take place, vendor best practices also change, accordingly. It is unrealistic to expect that even the most professional of (human) IT teams be aware of all the latest changes, to know what other teams have done, and to keep up with implementing all the necessary configuration changes to the systems. This set of circumstances lays the groundwork for misconfigurations that can lead

Insufficient controls and measures of resilience

The massive number of changes made to IT environments are not sufficiently tested for their impact on reliability before going live. Ideally, it should be a matter of course to test changes and understand their impact on resilience before moving to production. Today, this is not standard practice and not an integral part of a modern CI/CD process. Teams are uncertain of the health of their IT environment and whether new apps and updates will improve, or rather harm, its current state. This lack of visibility and knowledge can lead to high costs for the enterprise such as disruptions to availability, outages, or vulnerability of core data storage.

Complexity

Hybrid / multi cloud environments are the new normal: multi-layered, complex and dynamic.

Ongoing changes

New improvements, innovative features, capabilities and services introduced at a pace we've never seen before.

Knowledge gap

Thousands of ever evolving best practices Multiple teams / vendors / solution providers.

Insufficient controls

No easy path for continuous improvement: resilience should be injected into every process and changes should be fully tested before going live.

7. See: https://aws.amazon.com/about-aws/whats-new/2019

The Next Generation of Resilience Assurance Solutions

We've seen that maintaining the IT resilience of the modern enterprise has evolved into a mixed and diverse set of demands, objectives and expectations. IT professionals realize that and consequently, enterprises are investing more in resilience. Yet, despite growing investment, outages and downtime continue. Likewise, the consensus that cyberattacks on enterprises are inevitable is making the resilience of high-value data storage systems a major concern. Yet, it is obvious that existing resilience assurance tools are lacking. Acknowledging this state of affairs and in response to the challenges described above, we have developed our next generation of resilience solutions. They tackle the modern enterprise's resilience challenges with respect to outages and cyber resilience, and by extension, address users' expectations

Our solutions: Available as SaaS or private instance

- Includes public cloud risk analysis
- Downtime and data loss risk detection for traditional and modern workloads: Public Cloud / IaaS /PaaS / CaaS / SaaS / Hybrid
- New architecture and design for continuous analysis, modern workloads, CI/CD integration and more

- Automated security configuration risk analysis for data storage systems (on-prem / cloud)
- Identifies vulnerabilities and non-compliance
- Identifies vendor and community-driven best practice violations
- Detects; cyber-recoverability

A single platform powers our resilience solutions

The solutions focus on:

Preventing downtime, data loss and cyber resilience risks in hybrid IT infrastructure

Continuity Software's solutions build on expertise grown for nearly a decade and a half. They directly respond to IT teams' expanding needs in their handling of resilience demands under increasingly high-stakes circumstances of no tolerance for outages for any reason, and of requirements to be agile, robust and resilient. The AvailabilityGuardNXG™ resilienceassurance solution, used by leading enterprises worldwide, has been shown to reduce unplanned infrastructure outages by an average of 80%. Its demonstrated method and technology have been extended to the new Data Security Advisor™ solution that ensures the cyber-resilience of core data storage systems.

Both solutions are powered by a single Resilience Assurance Platform which is:

Designed for modern workloads; it helps prevent downtime, data loss and cyber risks in hybrid IT and multi-cloud environments (covering on-prem, legacy, private cloud and public cloud environments, and any mix of them)

Based on a new architecture that supports agile business requirements such as proactive resilience validation as part of modern CI/CD processes

A single unified platform for cyber and IT resilience assurance

Built with a modern UI that provides a single pane of glass for resilience status

The integrated and holistic view of ITand cyber resilience made possible by the platform gives IT and security teams the tools they need to rapidly grasp, manage and assure resilience on its expanding fronts.

Continuous and proactive resilience assurance for hybrid and multi-cloud environments

Our next generation of resilience assurance solutions are designed for today's complex hybrid and multi-cloud environments, covering every type and combination of environment (legacy, on-prem, private cloud, public cloud, and hybrid) and the various technologies used in modern environments (software-defined infrastructure, containers, etc.). A key feature of the solutions is proactive scanning of the entire IT stack to detect misconfigurations and potential single points of failure which can lead to service disruptions and/or outages, or to mission-critical stored data being vulnerable to a cyberattack, and/or to data being unrecoverable.

Deep and broad knowledge

Potential problems and misconfigurations are discovered by comparing the scanned configurations against the information in a proprietary, dedicated knowledgebase, the largest of its kind and constantly growing. Comprised of nearly 8,000 vendor and industry best practices, it is further supplemented by user input, all concerning the recommended and demonstrated methods for maintaining IT environment resilience. The cyber resilience solution interacts with its own knowledgebase of industry and vendor best practices, further supplemented by valuable user input, for assuring the cyber resilience of the enterprise's mission-critical data storage systems.
These scan and compare processes result in a running audit of the status of the environment's resilience to service disruptions and to cyberattacks.

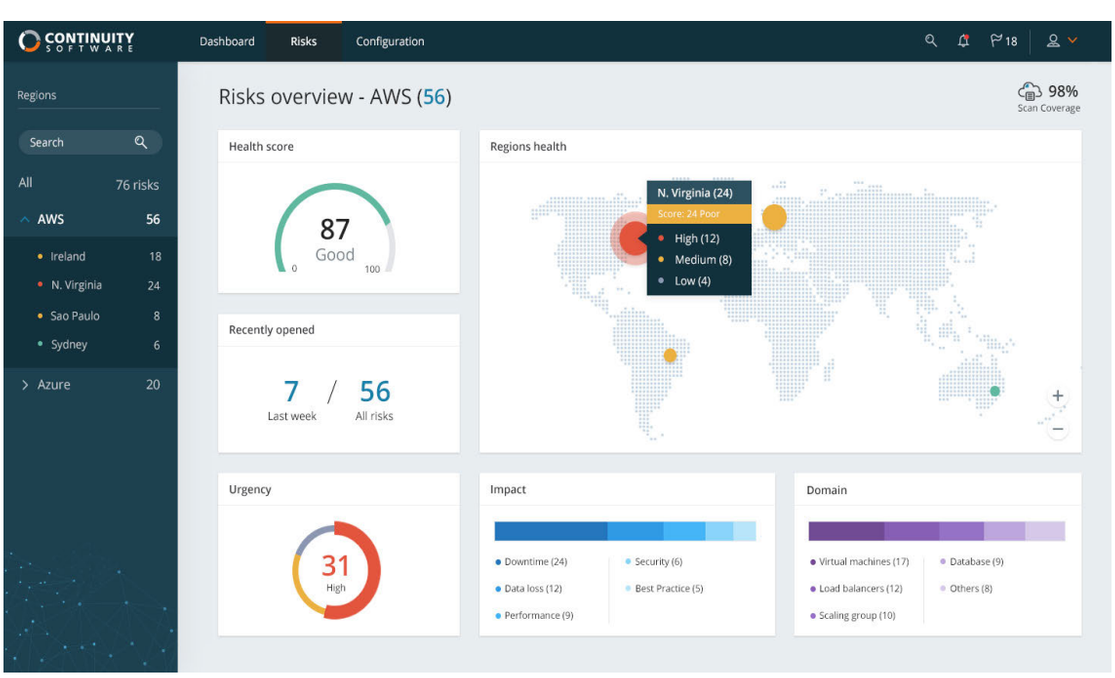
Visibility and control over resilience

Deviations from best practices and policies are detailed both on a dashboard and in automatically-generated reports.

The dashboard is clear and intuitive, providing a single pane of glass through which the enterprise can see, understand and manage its resilience activities and status across the entire IT stack. It includes details on parameters affecting resilience, with their urgency ranked in terms of impact on/risk to the business. Drilling down into a problematic region or a more vulnerable application provides additional information. Incident tickets are delivered to subject-matter experts.

They list all misconfigurations that must be corrected, along with guidance on how to correct them. The incidents can be integrated with existing ITSM tools to facilitate automatic incident generation and assignment for remediation.

The information provided through the dashboard and the reports leads to visibility and greater understanding of the environment's overall IT configuration health. This process of resilience validation is also significant in its contribution to operational excellence, generating improvement of service KPIs.



Dashboard view of resilience risks and status. Drilling down on parameters provides greater detail.

Summing Up

We've seen how the landscape of resilience challenges has grown and become more diverse, in paralleling to the growing complexity of IT environments. Continuity Software's enterprise-grade solutions – AvailabilityGuard NXG™ and Data Security Advisor™ - powered by a new Resilience Assurance Platform, offer singular tools that successfully protect enterprises from outages and from vulnerability to cyberattacks.

Our integrated, proactive approach to resilience is rational and has proven highly effective.

CONTINUITY SOFTWARE

About Continuity Software

Founded in 2005, Continuity Software helps the world's leading organizations, including 6 of the top 10 US banks, to achieve resilience in every type of IT environment. Our solutions proactively prevent outages and data loss incidents on critical IT infrastructure. As a result, unplanned infrastructure outages are reduced by an average of 80% and configuration errors are resolved before they turn into costly service incidents. Our proven technology and methodology now encompass cyber resilience. Our solutions protect mission-critical data residing in vulnerable storage systems against cyberattacks, prevent data loss, and ensure data recoverability.