WHITE PAPER

Ensure Resilient and Compliant Enterprise Networks

With Automated Testing

KEYSIGHT

Introduction

Even the most resilient enterprise networks can be surprisingly vulnerable. A single weak link, when exploited, can jeopardize critical commercial services and sensitive data, and such failure can quickly become headline news. Every industry has experienced this reality with outages and security and data breaches occurring at banks, governments, and large enterprises, impacting millions of customers and driving major revenue losses.

While cyberattacks are always top of mind, they are not the only cause for concern. IT supply chains have become increasingly complex, with third parties making frequent updates to networks, solutions, and offerings. Software and configuration bugs can have wide-ranging ramifications, as seen in the July 2024 CrowdStrike outage [1], where a software update error crippled 8.5 million Microsoft Windows systems globally. For days, airlines, hospitals, financial services, and media broadcasts worldwide were impacted. Parametrix [2] estimated the financial fallout at $5.4 billion for the Fortune 500 (excluding Microsoft) and $10 billion globally. Nearly 17,000 flights were cancelled over 72 hours. The healthcare and banking sectors had estimated losses of $1.94 billion and $1.15 billion, respectively, as important services remained unavailable. Beyond financial losses, the incident also underscored the significant reputational damage and erosion of consumer confidence that can result from such failures.

Ensuring operational network resilience is crucial for mitigating risks to enterprises and the global economy. Given the world's reliance on digital networks, enterprises and consumers expect always-on, reliable, and secure digital services as a baseline requirement. In response, governments are creating regulations that mandate and monitor resilience through vulnerability assessments and testing.

A major bank executive participating in a Spirent-led forum reported their top-level focuses as running the business with zero downtime, maintaining continuity via ongoing infrastructure maintenance, and continually changing the business environment to accommodate new technologies without risking service interruptions.

To achieve operational resilience, enterprises are prioritizing continuous, automated testing across lab and live networks while ensuring software updates are tested before deployment into production. The goal is to ensure networks are resilient to security threats, peak traffic impacts, and rainy-day conditions, and are able to recover rapidly when failure events occur.

This white paper addresses enterprise network resiliency concerns and challenges, highlighting the importance of resiliency testing. It provides a vision and a plan for modernizing and automating network testing to achieve operational resiliency, as well as case study results.

[1] https://hbr.org/2025/01/what-the-2024-crowdstrike-glitch-can-teach-us-about-cyber-risk
[2] https://www.parametrixinsurance.com/crowdstrike-outage-impact-on-the-fortune-500

Enterprise Network Complexity Poses New Concerns

As enterprises pursue digital transformation initiatives and networks become more distributed with workloads and storage dispersed across premises, remote data centers, and multiple clouds, operational network resilience becomes a moving target. These new architectures, the evolving threat landscape, and the ICT complexity and rate of change are all outsized stressors for enterprise networks, creating fragility.

Networks are incorporating complex supply chains that depend on third parties for public cloud, SASE (Secure Access Service Edge), CDNs (Content Delivery Networks), and telco connectivity. Third-party dependencies, growing threat sophistication, and the lack of a defined perimeter reduce visibility and control and make the network harder to defend. Instead of trusted users and applications within a confined network, cybersecurity must now, by default, assume zero trust and verify all users and devices that seek access to the network.

Importantly, the complexity and frequency of changes continuously deployed into data centers, branch sites, and hosted sites magnify the opportunity for errors and poses an increased risk to network resilience. As networks contend with supply chain complexities, security vulnerabilities, and an accelerated pace of change, their stability becomes increasingly fragile.

As a result, enterprises face mounting challenges in ensuring business continuity and maintaining infrastructure with zero downtime. This challenge is further amplified when integrating network transformations and new technologies into an already complex environment, where any disruption can have significant operational and financial implications.

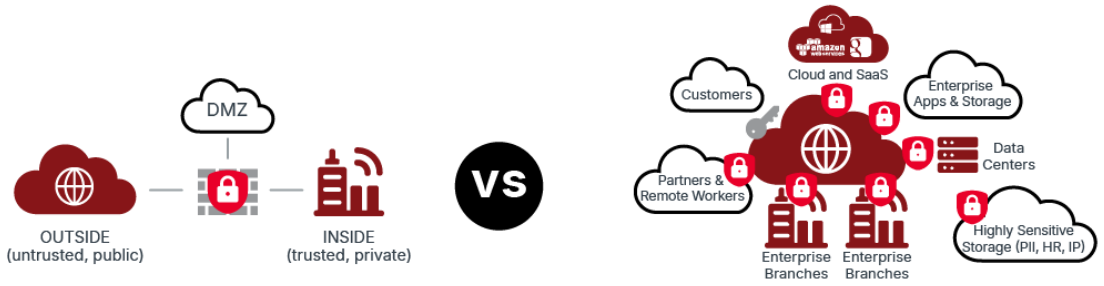
More than half of respondents in a survey [3] by Enterprise Strategy Group have experienced downtime of public cloud infrastructure (IaaS/PaaS) resources caused by a misconfiguration, outage, or other non-attack event. Modern enterprise network teams express the following major concerns:

- Difficulty integrating consistent security solutions across multiple cloud providers
- Data breaches
- Insufficient visibility into network traffic and threats
- Compliance and regulatory challenges
- Inability to keep up with upgrades across multiple clouds
- Vulnerabilities in shared infrastructure and virtualization layers
- Lack of visibility across the environment

Proactive network testing is crucial to identifying and resolving these issues before they impact customers and services. This is especially vital for critical sectors such as finance, insurance, and cloud providers, where regulatory bodies increasingly emphasize the need for built-in network resilience and stability. Consequently, stringent regulations are being introduced to safeguard the reliability of critical infrastructure.

[3] https://www.techtarget.com/esg-global/survey-results/multi-cloud-networking-trends/

The Evolution of Enterprise Networks



DORA Requirements

DORA, the European Digital Operational Resilience Act, requires global financial institutions to report incidents within hours and to provide operational security resiliency testing. Fines for non-compliance can be as much as two percent of total revenues.

DORA also defines compliance testing requirements and recommends operational resilience test methodologies ranging from vulnerability and network security assessments to end-to-end information and communication technology (ICT) testing. Partial or delayed testing risks fines, remediation, and violation reports.

DORA Compliance Testing Requirements & Recommendations

Requirements as per DORA Articles 24-27

- Vulnerability Assessments
- 3rd Party & Open-Source Software / Service Analysis
- Network Security Assessments
- End-to-End ICT Testing
- Gap Analysis & Process Review

Recommended Operational Resilience Test Methodologies

Penetration Testing & Red Teaming	Performance & Capacity Testing
Security Efficacy & Effectiveness Validation	High-Availability Testing
Chaos Testing	Impact of Updates/Patches & Policies/Configurations
End-to-End SLA & QoE of ICT	Disaster Recovery & Geo Redundancy

Assuring Resilient Enterprise Networks Requires a New Approach to Testing

The digital transformation of enterprise networks demands a transformation in how networks are tested. Traditionally, enterprises relied on monolithic vendors to test solutions before deploying them to data centers, branches, or hosted sites. However, with modern supply chains comprising many vendors delivering continuous updates, a change in mindset is needed. Enterprises can no longer rely solely on vendor testing and must take responsibility for the end-to-end resilience of networks. Ensuring the operational resilience of enterprise networks not only reduces risk but provides quality of service as a competitive edge.

As enterprise networks grow in complexity, so does the challenge of validating and testing them. Modern networks demand rigorous testing across a constantly evolving landscape of software versions, updates, patches, configurations, policies, traffic patterns, and threat signatures.

However, current test methodologies fall short in ensuring enterprise network resiliency due to:

- **Siloed testing environments.** Testing is conducted in isolated labs by different teams focusing on specific areas, resulting in the lack of a unified approach to managing changes in critical infrastructure.
- **Redundant resources and efforts.** Multiple labs and teams perform overlapping tests, leading to inefficiencies.
- **Static, infrequent testing.** Testing follows a rigid, waterfall-style process, conducted sporadically rather than continuously. By the time updates are released, other dependent network changes may have already occurred.
- **Slow, manual test execution.** Manually created test cases and lengthy testing cycles take months, increasing the risk of incidents and outages.
- Limited testing capacity. Personnel and lab resources are insufficient to cover all necessary scenarios.
- **Lack of automation.** Testing is not integrated into a CI/CD pipeline, preventing seamless validation of changes.
- **Inefficiency and scalability challenges.** Ineffective processes result in cost overruns and delays, making large-scale testing impractical.
- **Narrow test coverage.** Current methodologies focus only on functional validation, neglecting performance, resilience under varying loads, chaotic conditions, and security threats—critical factors for network stability.

Manual test methods are not scalable and impractical for providing complete test coverage. New tools are needed to efficiently and cost-seffectively test the operational resilience of the massive test loads generated by today's complex and rapidly changing enterprise networks. The best way to manage this rapid change and complexity is through complete automation and continuous testing.

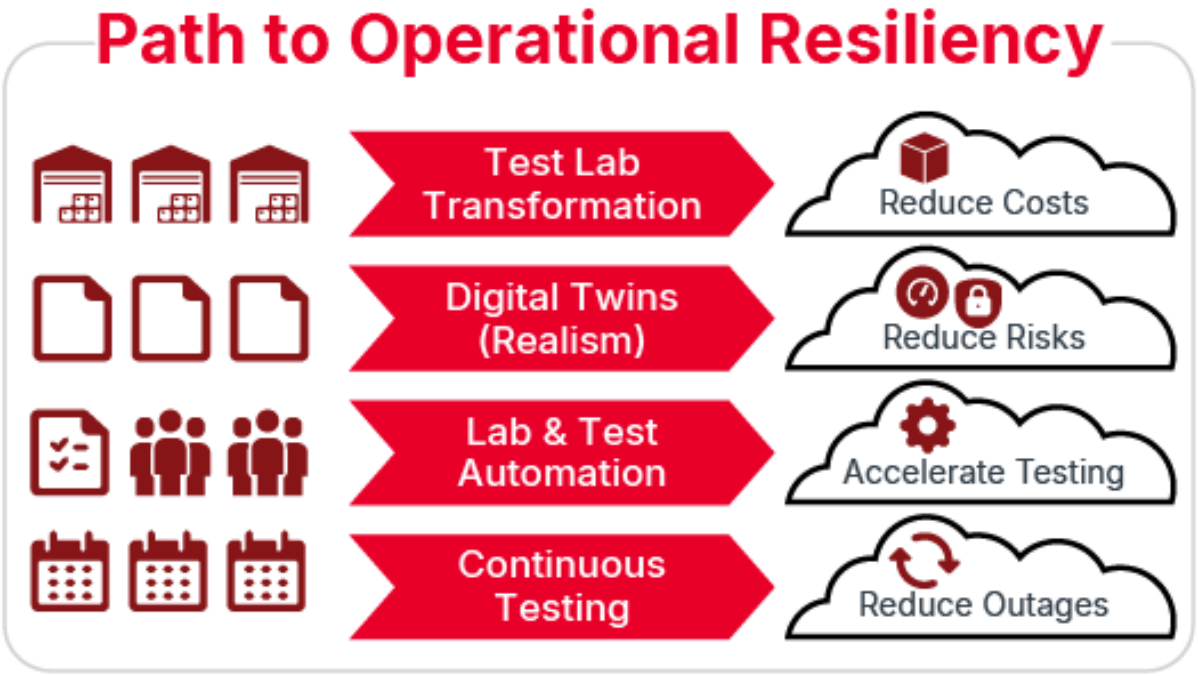
A Path to Operational Resiliency

Ensuring operational resiliency requires a network test automation platform that minimizes costs, risks, and outages while accelerating the testing process. An effective platform should:

- Automate end-to-end delivery across the design, certification, and deployment lifecycle
- Replicate real-world scenarios to test infrastructure resilience and reduce risk
- Perform resilience and non-functional testing
- Accelerate certification of patches and software releases, thereby shortening deployment intervals
- Perform continuous testing to minimize outages
- Enhance quality and significantly reduce defects by promoting new releases into production with consistent deployment and validation mechanisms

Test process automation is critical for delivering the test speed, capacity, variability, and accuracy needed to support an enterprise's distributed, complex environment. Automation makes it feasible to test many different scenarios and to test continuously.

Without test automation, conducting resiliency testing in the lab—such as stress tests that evaluate how a network responds to and recovers from security threats, unexpected disruptions, traffic surges, and other performance challenges—is impractical.



An Automated Operational Resilience Test Framework

Keysight's recommended approach for achieving operational resiliency is continuous, automated testing from lab to live. This is important because any change in the network across the complex supply chain could disrupt operations and should be tested automatically, in the context of the entire network, before being deployed in the production network.

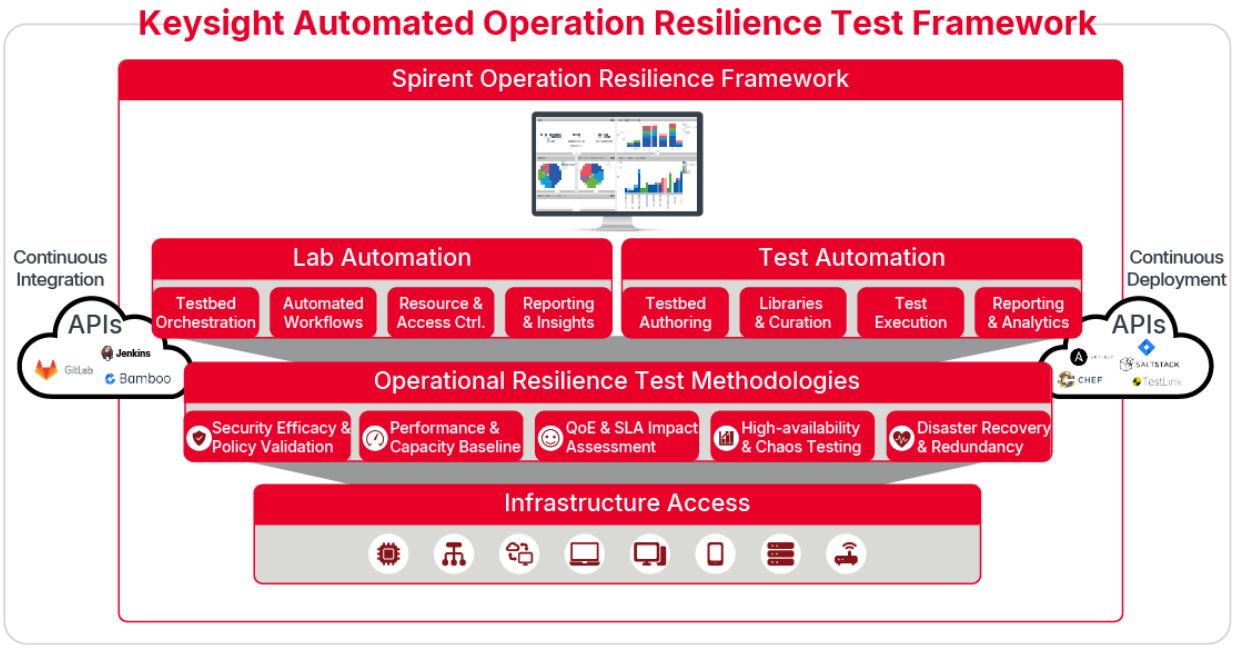
An automated resilience test framework should support the continuous flow of changes, provide continuous testing and continuous deployment, while:

- Running any type of test on any kind of infrastructure
- Emulating specific types of traffic for tests
- Automating test setups through APIs
- Automatically running tests and communicating results to the appropriate teams

Traditional test scripts and technologies are not designed to test network and infrastructure resilience. Specialized tools, such as emulators and digital twins, are essential to test for operational resilience. Digital twins provide realism by recreating real-world scenarios to test actual operational resilience and reduce risk. Emulations make it easy to vary test traffic without needing to purchase and create the network in the lab.

A Solution Blueprint for Achieving Operational Resilience

An automated operational resilience test framework uses a layered approach to provide a complete testing blueprint to achieve operational resilience and reduce costs.



Automated infrastructure access federates labs and enables all teams to leverage all resources remotely.

Operational resilience test methodologies run any functional or non-functional tests on any infrastructure. Automated test setups and continuous functional and nonfunctional testing leverage emulated traffic scenarios and digital twins. Operational resilience tests span security efficacy, performance, quality of experience, chaos, and disaster recovery.

Lab and test automation enable continuous lab-to-live test automation as well as integration with CI/CD (continuous integration/continuous delivery) processes. This complete CI/CD/CT (continuous testing) integration accelerates testing and reduces outages. Lab automation includes testbed orchestration and automated workflows. Test automation leverages extensive test libraries, including operational resilience tests. Flexible reporting and analytics facilitate easy communication of detailed results to other teams.

Continuous integration APIs instantiate the topology and infrastructure required for a test.

Continuous deployment of tested updates to the production network is managed via APIs.

This layered approach provides a blueprint for a complete operational resilience testing framework with continuous automated testing.

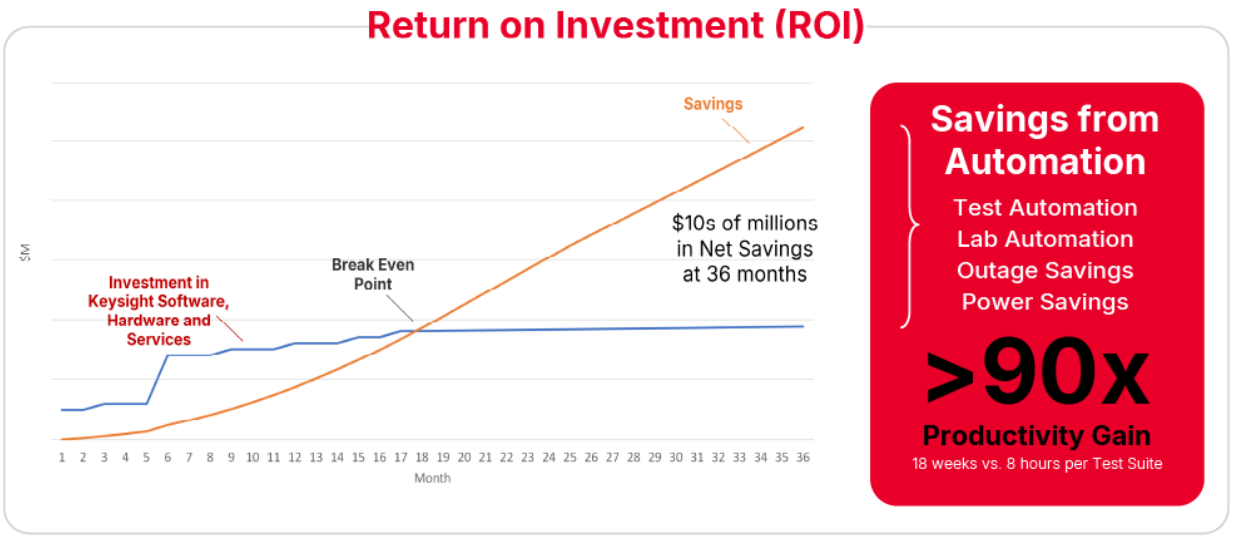
AI is playing an emerging role in continuous, automated operational resilience testing, providing benefits such as:

- Increased efficiency by making smart test selections that optimize which test cases should be run for a specific situation or change
- Driving root cause analysis and reducing mean-time-to-repair by quickly pinpointing the root cause of failures and communicating the cause and associated artifacts, such as logs, to the person responsible for repair
- Predicting future failure patterns before they occur

Proactive, Continuous Testing: Accelerating Value, Driving Innovation, Reducing Risk

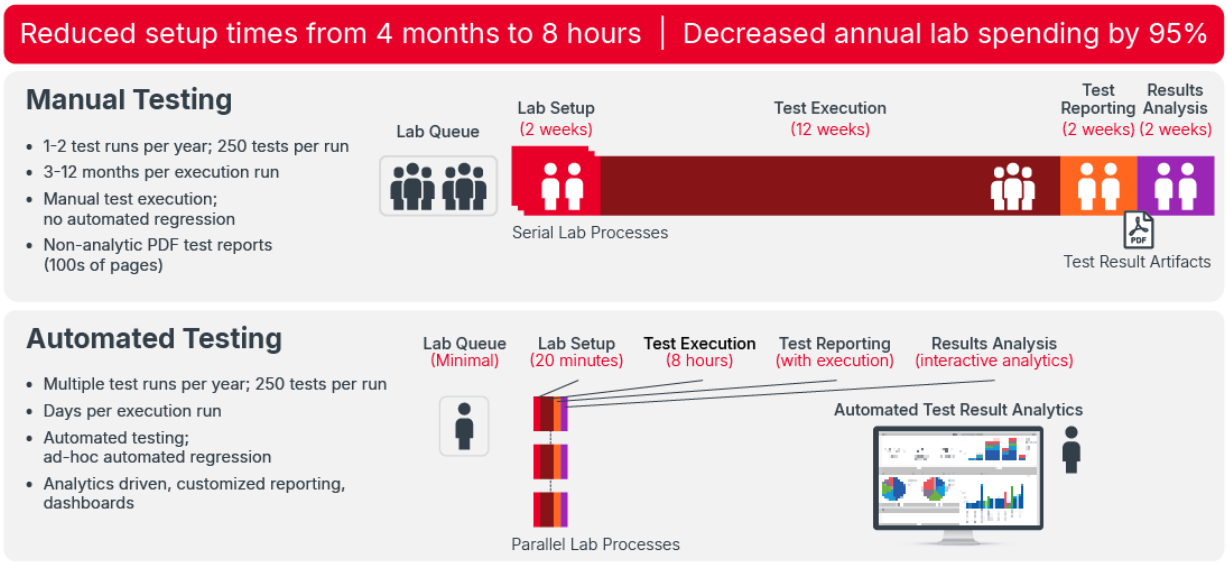
Comprehensive, automated, and continuous operational resilience testing helps enterprise staff sleep well, knowing risks have been mitigated and customer experiences remain unaffected. Enterprises can run the business, perform ongoing infrastructure maintenance, and incorporate new technologies without causing downtime.

Enterprises are already realizing the operational efficiency benefits of test automation, achieving 90x productivity gains and an 18-month return on investment, leading to tens of millions of dollars in net savings after three years.



Top Bank Cuts Test Times and Slashes Capex

Automation at a top-ten bank reduced test setup times from four months to eight hours and the time to execute a test suite from months to days. Automation reduced annual lab spending by 95 percent. Additional benefits were achieved, including automated regression testing and customized reports.



The time to execute individual test cases dropped from hours and days to minutes. The implementation of automated 24/7 test execution increased productivity, simplified test suite creation and management, and gave web-based access to all test resources.

Post-Implementation Results

Customer-Reported Improvements and Benefits

- **Time & Cost Savings –** Tests run continuously, even during non-work hours, increasing productivity and output
- **Enhanced Test Coverage –** Automated traffic creation across test cases
- **Web-Based Lab Access –** Single location for all test sources and automation assets
- **Test Suite Management –** Create and run test suites, schedule reservations
- **Comprehensive Reporting –** Store and manage automated test reports, facilitating tracking results over time

Program results (excerpt)

Function	# of Test Cases	Time to Execute Manually	New time
Firewall	28	16 hrs	18 mins
Gateway	78	40 hrs	55 mins
Other	20	25 hrs	8 mins
Total	126	81 hrs	1h 21min

60X faster than Legacy!!!

Accelerate Value, Drive Innovation, and Reduce Risk

Proactive, automated, and continuous operational resilience testing, from the lab to the live network, is helping enterprises reduce outages and keep pace with innovation, mitigate risk and meet compliance mandates with proof points, and deliver business continuity, consistent security, and value to users and customers.

Enterprise teams can operate with confidence, knowing their networks remain resilient during routine maintenance and large-scale transformations.

KEYSIGHT

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.