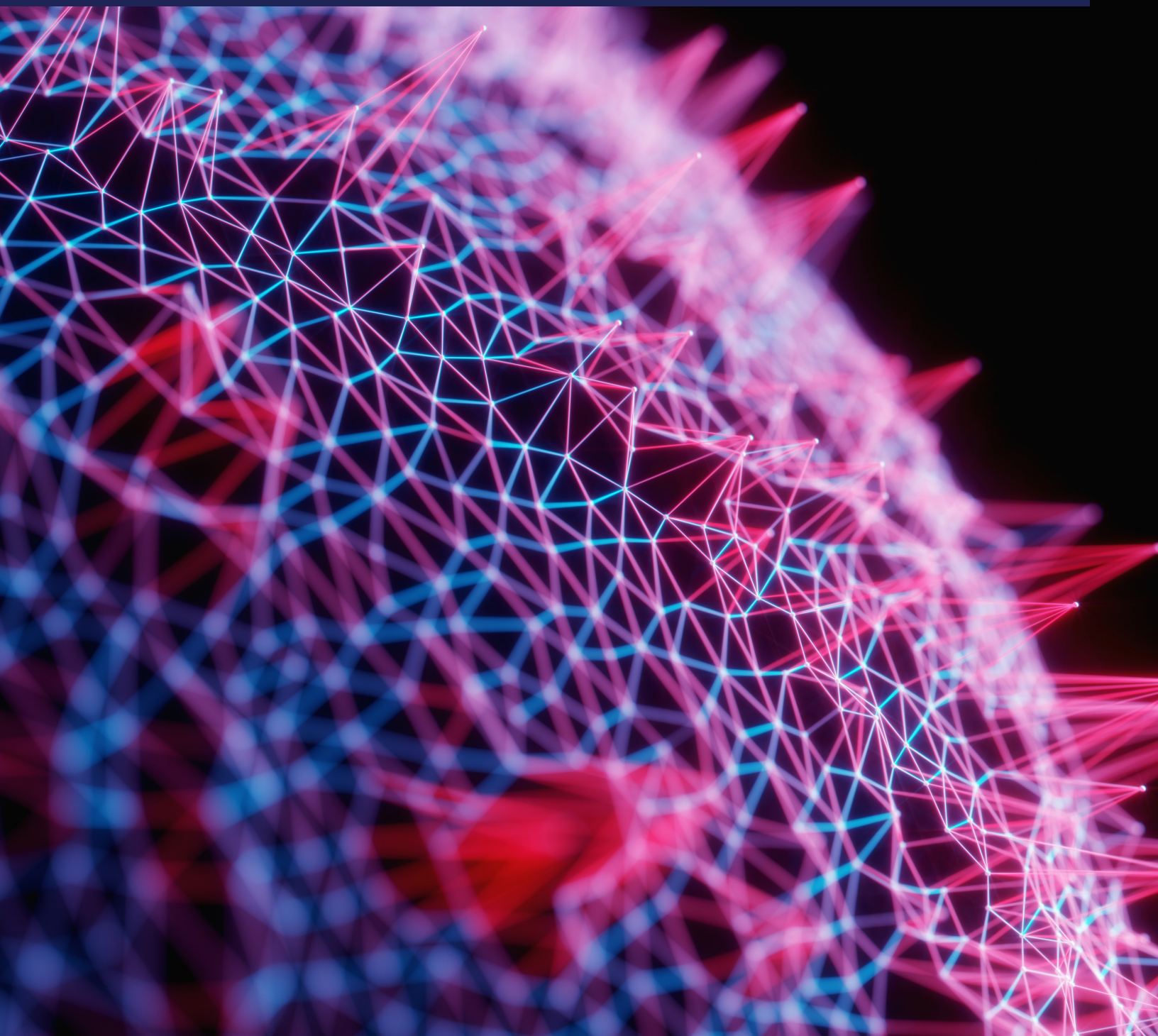
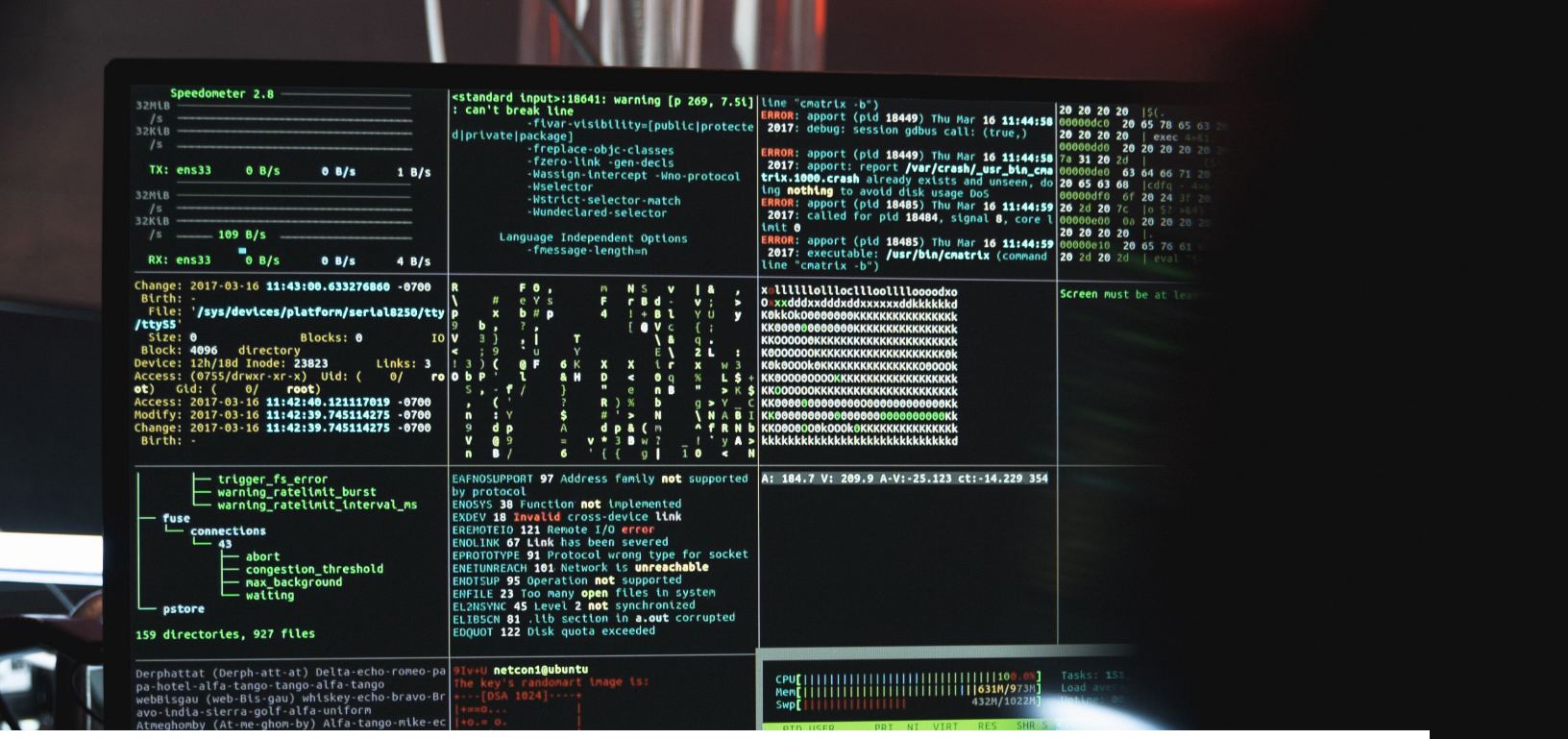
Persistent

Solution Brief

Persistent Intelligent Cyber Resilience





Cyberattacks have been rated as the fifth top rated risk in 2020 and are expected to double by 2025. World Economic Forum's 2020 Global Risk Report states that the rate of detection (or prosecution) is as low as 0.05 percent in the U.S.

As the attacks keep becoming more sophisticated and stronger, Cyber Resiliency is moving to the top-of-mind on the agenda for most CEOs and CISOs. Organizations are becoming aware that they cannot detect, protect, or predict 100% of the incidents. Hence, the focus is now on absorbing the shock within their ecosystem with minimal disruption, minimum loss of data, and minimum loss to reputation. This can only be achieved by incorporating Cyber Resilience best practices — processes, technology, and people. It is not enough just to protect your primary data center assets and infrastructure from cyber-attacks originating from outside the firewall. Many of the attacks originate from inside of the organization using compromised credentials. In these cases, the destruction is already ongoing before anyone is aware of the breach. Cyber Resilience provides the opportunity to recover the applications and data even in the event of a successful ransomware attack. But the recovery stage needs to have a robust and secure environment and architecture to allow for the remediation and recovery of the most recent clean data and elimination of the malware for the resumption of production activities Traditional backup and DR solutions are susceptible to ransomware attacks and were not designed for the recovery process necessary after an attack. These solutions were designed for fast recovery time after a physical disaster or error.

It takes more than just a product for Cyber Resilience recovery. Persistent, together with Google Cloud, has created a cyber resilience offering to deal with recovery from cyber-attacks. The approach includes customized process development, use of cutting-edge technologies leveraging Actifio, Google Cloud Platform and Persistent IPs and ongoing and managed recovery and operations. This offering, Persistent Intelligent Cyber Resilience (PiCR) provides an environment for secure recovery and return to operations leveraging network isolation, immutable storage and Intelligent analysis and detection of anomalies.

PiCR Includes

Early detection of a ransomware attack

An isolated and secure recovery environment with point-in-time server images from Actifio Go that can be accessed quickly

A safe environment to analyze and clean infected image

Regular recovery testing

Processes to recover after an attack and return to production

Use Cases

1. Existing Actifio customers looking for a CR solution
2. Google Cloud Platform users needing an end-to-end ransomware recovery solution
3. Enterprises using a DR or Backup product without a complete Cyber Resilience solution

Persistent Intelligent Cyber Resilience (PiCR) solution builds a comprehensive multi-disciplinary cyber resilience solution including:

An assessment of the current state and creation of a recovery strategy

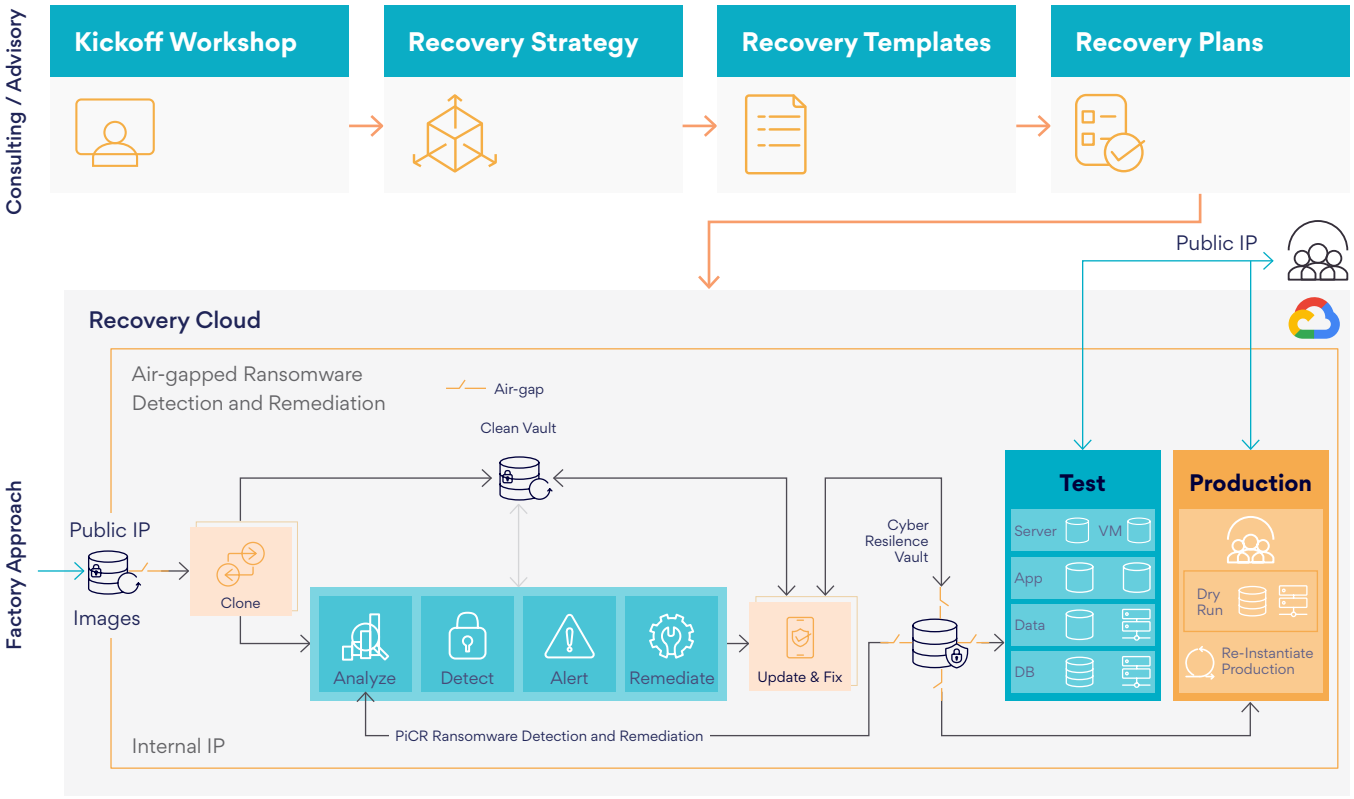
Creation of detailed plans for all operations and a pilot to validate the solution

Rollout of the protection and cyber resilience recovery infrastructure and technologies

Managed recovery and operations

PiCR is architected to deliver faster detection, remediation, and recovery of applications and data.

PiCR — Deployment Overview



The PiCR Solution

This solution contains the following components to address the ransomware and malware attack problem

Recovery Strategy and Plan

Through an advisory consulting process, Persistent works with organizations to create a recovery strategy and execution plans to run the Cyber Resilience Recovery. The recovery strategy aligns with an organization's business priorities and structure based on SLAs, response team, security considerations and the required business outcome. The execution plan codifies the operations and processes for the implementation and operations approach.

Protect

Actifio GO: For protection of production servers with point-in-time images secured in immutable object storage in GCP.

Internal IP address-based network isolation from Public Network: A Private IP address-based internal network is used to prevent any direct exposure of the PiCR assets to the external public network. All data and control traffic and the infrastructure for remediation and storing of the clean images are limited to the internal network. The connections to the external network are fenced using the VPC settings and service account settings.

Automated air gap from internet: The Recovery Images, Test infrastructure and Cyber Resilience Production infrastructure are not reachable from the internet or a public unsecured network since the network switches connecting to the outside world are switched off by default. The system makes sure that the Cyber Resilience Vault is isolated when the resources connected to the external network are being accessed from the internal network.

Automated air gap from the Test Environment: The images are recovered into the testing environment. Before the test systems and data are brought up, the air gap between the test environment and the PiCR internal network is enabled. After the testing is completed, the testing environment is deleted in isolation thereby, purging all resources and data, including ransomware and malware if present.

Identity and Function based Access Control: Resources across the internal network are accessed only by functional modules that need to access using specific service accounts. The service accounts have the lowest level of privileges to get the work done. For example, the service account that writes data to a vault cannot delete any data. The deletion of the images can only be done by the retention manager which is an internal service that uses a completely different service account that cannot be used by any other function.

Automated need-to-access time-period: By default, the network connectivity is turned off. This completely isolates the Cyber Resilience site from the public internet. When connectivity is needed between two endpoints, the connectivity is purposefully restored. Once the access needs are satisfied, the connection is again turned off.

Immutable Images: All the images are immutable. They can be deleted only by the retention manager based on a retention policy. The images can be configured never to be expired and hence never be deleted.

Versioned Images: All images are versioned in chronological order. Timestamp and other details are maintained so that the images can be quickly searched on-demand to locate the right image to be used for testing or production.

Analyze

Inline and scanning methods generate multiple metrics for analysis using machine learning. The files that have changed or have been newly added are also analyzed for ransomware and malware.

Detect

Continuous detection of ransomware attacks: High-risk changes are detected and flagged on the PiCR dashboard for review by the security team. A weighted risk scoring system generates actionable warnings and alerts when risk thresholds are exceeded.

Remediate

Readying clean point-in-time images without the ransomware or malware: PiCR identifies the latest point-in-time images in the Cyber Resilience Vault that can be recovery candidates. These images might have ransomware or malware in them, but they have might not have triggered. The recovery candidate images are copied to the Clean Vault, and all the unique changes are reanalyzed based on additional information and risk profile. The security team can review and flag risky changes on the dashboard. The flagged changes are backed out from the image and quarantined. A new clean recovery image is created and stored in the Cyber Security Vault.

Recovery

The newly cleaned images are recovered and tested in parallel in an isolated testing environment and are monitored for any suspicious activity. After successful testing, the production recovery runbook is executed, and the system automatically recovers the images into the production environment, and the applications are up and running to execute real workloads.

Cyber threats are not a question of 'If' but 'When'. Take the necessary steps to protect your organization from ongoing and emerging cyber threats with an intelligent solution for faster recovery and limited downtime.

Want to make Cyber Resilience a lot less challenging?

Contact Us

About Persistent

With over 14,500 employees located in 18 countries, Persistent Systems is a global services and solutions company delivering Digital Engineering and Enterprise Modernization. We combine deep technical expertise and industry experience to help our clients anticipate what's next and develop solutions that create unique competitive advantage. Persistent was named to the Forbes Asia Best Under a Billion 2021 list, representing consistent top-and bottom-line performance as well as growth.

India
Persistent Systems Limited
Bhageerath, 402
Senapati Bapat Road
Pune 411016
Tel: +91 (20) 6703 0000
Fax: +91 (20) 6703 0008

USA
Persistent Systems, Inc.
2055 Laurelwood Road, Suite 210
Santa Clara, CA 95054
Tel: +1 (408) 216 7010
Fax: +1 (408) 451 9177
Email: info@persistent.com

Persistent

www.persistent.com