IBM Resilient Incident Response Platform Enterprise on Cloud delivers orchestrated and automated incident response processes

Table of contents

<table>
<thead>
<tr>
<th>1</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Key prerequisites</td>
</tr>
<tr>
<td>2</td>
<td>Planned availability date</td>
</tr>
<tr>
<td>2</td>
<td>Description</td>
</tr>
<tr>
<td>2</td>
<td>Program number</td>
</tr>
<tr>
<td>3</td>
<td>Publications</td>
</tr>
<tr>
<td>3</td>
<td>Technical information</td>
</tr>
<tr>
<td>4</td>
<td>Ordering information</td>
</tr>
<tr>
<td>5</td>
<td>Terms and conditions</td>
</tr>
<tr>
<td>7</td>
<td>Prices</td>
</tr>
<tr>
<td>7</td>
<td>Order now</td>
</tr>
</tbody>
</table>

Overview

IBM(R) Resilient Incident Response Platform (IRP) on Cloud is one of the leading platforms for orchestrating and automating incident response processes. Resilient IRP, a product that was acquired from Resilient, an IBM company, can quickly and easily integrate with your organization's existing security and IT investments to:

- Make security alerts ready for use near instantly.
- Provide valuable intelligence and incident context.
- Enable security teams to help eliminate or streamline critical steps.

Resilient IRP offers a robust response to the daily events that can require actions from your security teams. This is a growing challenge that is shared globally by organizations of all sizes and across all industries. Responding effectively in the face of a cyber crisis becomes harder as the stakes get higher and the actors more sophisticated.

Resilient IRP provides dynamic action plans for many different types of incidents and best practices for responding to virtually all incident types, which include malware, distributed denial-of-service (DDoS), and lost devices. This extensive knowledgebase can help lead your team through the most effective response, while also capable of being customized to your team's standard operating procedures. Team members can quickly access data from more than a dozen, cyber-threat-intelligence feeds and other integrated cyber security and IT systems.

Incident response teams can manage and collaborate on their response directly within the platform. Unlike ticketing systems and other general-purpose IT tools, Resilient IRP is fully configurable and purpose-built for incident response. Comprehensive analysis, customizable dashboards, and robust reporting features can help ensure that senior leadership can access key information when needed.

In May, 2016, IBM acquired Resilient Systems Inc., a leading provider of incident response solutions. With this acquisition, IBM is positioned to provide the industry's first integrated, end-to-end Security Operations and Response Platform offering that spans the entire lifecycle of an attack, from protection and detection to response.

Key prerequisites
Resilient IRP on Cloud requires an internet connection and a workstation with a browser.

For specific browser requirements, refer to the Technical information section.

**Planned availability date**

November 1, 2016

**Description**

Resilient IRP on Cloud can help automate and orchestrate the processes for dealing with cyber incidents, such as breaches and lost devices. It can enable businesses to respond to a security incident by categorizing the incident and implementing best practices, or playbooks, to respond accordingly.

With a number of integrations with established security systems, which include IBM Security QRadar® SIEM, Resilient IRP can share data and trigger actions within those systems to help:

- RemEDIATE security incidents.
- Offer additional context on actionable items.
- Suggest best practices to help prevent future incidents.

This offering includes a knowledge base of global data breach notification regulations that is maintained and updated by privacy professionals at Resilient, an IBM Company. This knowledge base can be used by team members to help understand breach notification compliance requirements that may apply to a security incident.

**Reference information**

For information on the IBM acquisition of Resilient Systems, Inc, refer to the IBM News room.

For additional information on Resilient IRP as an on-premise offering, refer to Software Announcements 216-430, dated November 1, 2016, and 216-271, dated June 14, 2016.

For additional information on IBM Security QRadar, refer to Software Announcement 215-088, dated May 26, 2015.

**Program number**

<table>
<thead>
<tr>
<th>Program number</th>
<th>VRM</th>
<th>Program name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5737-C07</td>
<td>SaaS</td>
<td>IBM Resilient Incident Response Platform on Cloud</td>
</tr>
</tbody>
</table>

**Education support**

Not applicable

**Offering Information**
Product information is available on the IBM Offering Information website.

More information is also available on the Passport Advantage® and Passport Advantage Express® website.

**Publications**

For product documentation, contact your IBM representative.

**Services**

**Software Services**

IBM Software Services has the breadth, depth, and reach to manage your services needs. You can leverage the deep technical skills of our lab-based, software services team and the business consulting, project management, and infrastructure expertise of our IBM Global Services team. Together, we provide the global reach, intellectual capital, industry insight, and technology leadership to support a wide range of critical business needs.

To learn more about IBM Software Services or to contact a Software Services sales specialist, go to the IBM Software Services website.

**Technical information**

**Specified operating environment**

**Hardware requirements**

Resilient IRP on Cloud requires:

- A workstation that supports one of the web browsers as listed in the Software requirements section
- A direct, internet connection

**Software requirements**

Resilient IRP on Cloud requires one of the following supported web browsers:

- Microsoft™ Internet Explorer V11
- Mozilla Firefox, latest version for your operating system and ESR 38
- Google Chrome, latest version for your operating system
- Safari, latest version for Mac

The program's specifications and specified operating environment information may be found in documentation accompanying the program, if available, such as a readme file, or other information published by IBM, such as an announcement letter. Documentation and other program content may be supplied only in the English language. Such information is provided subject to the following terms. IT system security involves protecting systems and information through prevention, detection and, response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated, or misused, or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service, or security measure can be completely effective in preventing improper use or access. IBM systems, products, and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products, or services to be most effective.
Important: IBM does not warrant that any systems, products, or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

Planning information

Packaging

This offering is delivered through the internet. There is no physical media.

Ordering information

This product is only available through Passport Advantage. It is not available as shrinkwrap.

Product Group: Security

Product: IBM Resilient Incident Response Platform on Cloud (5737-C07)

Product Category: Resilient Incident Response Platform

Passport Advantage

<table>
<thead>
<tr>
<th>Program name/Description</th>
<th>Part number</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Resilient Incident Response Platform on Cloud Instance per Month</td>
<td>D1QRILL</td>
</tr>
<tr>
<td>IBM Resilient Incident Response Platform on Cloud Instance Overage</td>
<td>D1QRJLL</td>
</tr>
<tr>
<td>IBM Resilient Incident Response Platform on Cloud Authorized User per Month</td>
<td>D1QRKLL</td>
</tr>
<tr>
<td>IBM Resilient Incident Response Platform on Cloud Authorized User Overage</td>
<td>D1QRLLL</td>
</tr>
<tr>
<td>IBM Resilient Incident Response Platform Non-Production Environment on Cloud Instance per Month</td>
<td>D1QVILL</td>
</tr>
<tr>
<td>IBM Resilient Incident Response Platform Non-Production Environment on Cloud Instance Overage</td>
<td>D1QVHLL</td>
</tr>
<tr>
<td>IBM Resilient Incident Response Platform Standard on Cloud Instance per Month</td>
<td>D1QRMLL</td>
</tr>
<tr>
<td>IBM Resilient Incident Response Platform Standard on Cloud Instance Overage</td>
<td>D1QRNLL</td>
</tr>
<tr>
<td>IBM Resilient Incident Response Platform Standard Authorized User per Month</td>
<td>D1QRPLL</td>
</tr>
<tr>
<td>IBM Resilient Incident Response Platform Standard Authorized User Overage</td>
<td>D1QRQLL</td>
</tr>
<tr>
<td>IBM Resilient Incident Response Platform Integration Services for Cloud Engagement Remotely Delivered Service</td>
<td>D1QRFLL</td>
</tr>
<tr>
<td>IBM Resilient Incident Response Platform Design Session for Cloud Engagement Remotely Delivered Service</td>
<td>D1QRHLL</td>
</tr>
</tbody>
</table>

Charge metric

<table>
<thead>
<tr>
<th>Program/service name</th>
<th>Program number</th>
<th>Charge unit description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Resilient IRP on Cloud</td>
<td>5737-C07</td>
<td>Authorized User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Engagement</td>
</tr>
</tbody>
</table>
Authorized User

Authorized User is a unit of measure by which the program can be licensed. An Authorized User is a unique person who is given access to the program. The program may be installed on any number of computers or servers and each Authorized User may have simultaneous access to any number of instances of the program at one time. Licensee must obtain separate, dedicated entitlements for each Authorized User given access to the program in any manner directly or indirectly (for example, through a multiplexing program, device, or application server) through any means. An entitlement for an Authorized User is unique to that Authorized User and may not be shared, nor may it be reassigned other than for the permanent transfer of the Authorized User entitlement to another person.

**Note:** Some programs may be licensed where devices are considered users. In that case, the following applies. Any computing device that requests the execution of or receives for execution a set of commands, procedures, or applications from the program or that is otherwise managed by the program is considered a separate user of the program and requires an entitlement as if that device were a person.

Engagement

Engagement is a unit of measure by which the services can be obtained. An Engagement consists of professional and/or training services related to the IBM SaaS. Sufficient entitlements must be obtained to cover each Engagement.

Instance

Instance is a unit of measure by which the IBM SaaS can be obtained. An Instance is access to a specific configuration of the IBM SaaS. Sufficient entitlements must be obtained for each Instance of the IBM SaaS made available to access and use during the measurement period specified in Customer’s Proof of Entitlement (PoE) or Transaction Document.

Terms and conditions

The information provided in this announcement letter is for reference and convenience purposes only. The terms and conditions that govern any transaction with IBM are contained in the applicable contract documents such as the IBM International Passport Advantage Agreement, the International Passport Advantage Express Agreement, the Cloud Services Agreement and associated Service Descriptions, or the IBM SaaS Terms of Use.

This product is only available through Passport Advantage. It is not available as shrinkwrap.

Subscription

The IBM International Passport Advantage Agreement and the IBM SaaS Terms of Use or the IBM Cloud Services Agreement (CSA) and the Service Description govern your use of this offering.

Technical support

Technical support is provided for IBM SaaS and enabling software, as applicable, during the subscription period. Any enhancements, updates and other materials provided by IBM as part of any such technical support are considered to be part of IBM SaaS or enabling software, as applicable, and therefore governed by the SaaS Terms of Use or the CSA and associated Service Description. Technical support is included with IBM SaaS and is not available as a separate offering.
Refer to additional technical support information in the IBM Software as a Service Terms of Use document for the program.

**Terms of Use**

The program's *Terms of Use and CSA Service Description* document is available on the Software as a Service terms website.

**Limited warranty**

If warranted, refer to the warranty as stated in the Terms of Use document or the Cloud Services Agreement for this offering.

**Money-back guarantee**

No

**Volume orders (IVO)**

No

**Passport Advantage applies**

Yes, information is available on the Passport Advantage and Passport Advantage Express website.

**Software Subscription and Support applies**

No

**IBM Operational Support Services - SoftwareXcel**

No

**Other support**

Passport Advantage

**System i Software Maintenance applies**

No

**Variable charges apply**

No

**Educational allowance available**

Not applicable.

**Statement of good security practices**

IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, or misappropriated or can result in misuse of your systems to attack others. Without a comprehensive approach to security, no IT system or product should be considered
completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products, or services to be most effective.

**Important:** IBM does not warrant that any systems, products, or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

---

**Prices**

**Passport Advantage**

For Passport Advantage information and charges, contact your IBM representative. Additional information is also available on the [Passport Advantage and Passport Advantage Express](https://www.ibm.com) website.

**IBM Global Financing**

IBM Global Financing offers competitive financing to credit-qualified customers to assist them in acquiring IT solutions. Offerings include financing for IT acquisition, including hardware, software, and services, from both IBM and other manufacturers or vendors. Offerings (for all customer segments: small, medium, and large enterprise), rates, terms, and availability can vary by country. Contact your local IBM Global Financing organization or go to the [IBM Global Financing](https://www.ibm.com) website for more information.

IBM Global Financing offerings are provided through IBM Credit LLC in the United States, and other IBM subsidiaries and divisions worldwide to qualified commercial and government customers. Rates are based on a customer’s credit rating, financing terms, offering type, equipment type, and options, and may vary by country. Other restrictions may apply. Rates and offerings are subject to change, extension, or withdrawal without notice.

Financing from IBM Global Financing helps you preserve cash and credit lines, enables more technology acquisition within current budget limits, permits accelerated implementation of economically attractive new technologies, offers payment and term flexibility, and can help match project costs to projected benefits. Financing is available worldwide for credit-qualified customers.

---

**Order now**

To order, contact the Americas Call Centers or your local IBM representative. To identify your local IBM representative, call 800-IBM-4YOU (426-4968). For more information, contact the Americas Call Centers.

Phone: 800-IBM-CALL (426-2255)

Fax: 800-2IBM-FAX (242-6329)

For IBM representative: callserv@ca.ibm.com

**Mail:**

IBM Teleweb Customer Support
ibm.com Sales Execution Center, Americas North
3500 Steeles Ave. East, Tower 3/4
Markham, Ontario
Canada L3R 2Z1

**Reference:** YE001
The Americas Call Centers, our national direct marketing organization, can add your name to the mailing list for catalogs of IBM products.

**Trademarks**

IBM, Passport Advantage, QRadar, Express, System i and ibm.com are registered trademarks of IBM Corporation in the United States, other countries, or both. Microsoft is a trademark of Microsoft Corporation in the United States, other countries, or both. Other company, product, and service names may be trademarks or service marks of others.

**Terms of use**

IBM products and services which are announced and available in your country can be ordered under the applicable standard agreements, terms, conditions, and prices in effect at the time. IBM reserves the right to modify or withdraw this announcement at any time without notice. This announcement is provided for your information only. Additional terms of use are located at:

- [Terms of use](#)

For the most current information regarding IBM products, consult your IBM representative or reseller, or visit the IBM worldwide contacts page

- [IBM United States](#)