Resilient Incident Response Platform

Accelerate your response with an advanced, battle-tested platform for incident response orchestration

Highlights

The IBM Resilient Incident Response Platform for automated incident response helps reduce the time to find, respond to, and remediate complex cyber threats.

- Security module provides dynamic playbooks, integrated threat intelligence, and customizable analytics dashboards
- Action module orchestrates and automates incident response processes
- Privacy module provides an instant, configurable platform for data breach preparation, assessment, and management

The IBM Resilient® Incident Response Platform (IRP) is a leading platform for orchestrating and automating incident response processes. Security organizations can significantly drive down their mean time to find, respond to, and remediate using the platform. It quickly and easily integrates with your organization's existing security and IT investments, allowing a single intelligent hub to drive fast and intelligent action. The platform's advanced orchestration capabilities enable adaptive response to complex cyber threats.

Whether you're managing a large-scale security operations center (SOC) or a smaller security operation, the IBM Resilient platform is designed to meet the specific needs of organizations of all sizes and complexities, and built to scale as your incident response program evolves.

"The Resilient IRP was the only choice that was capable and customizable enough to help me build a modern incident response practice. Our mean time to discovery, recovery, and closure dramatically improved using the Resilient IRP."

— Head of Cyber Security Incident Response, Leading Medical Center and Research Facility

Resilient IRP can be customized to specific needs

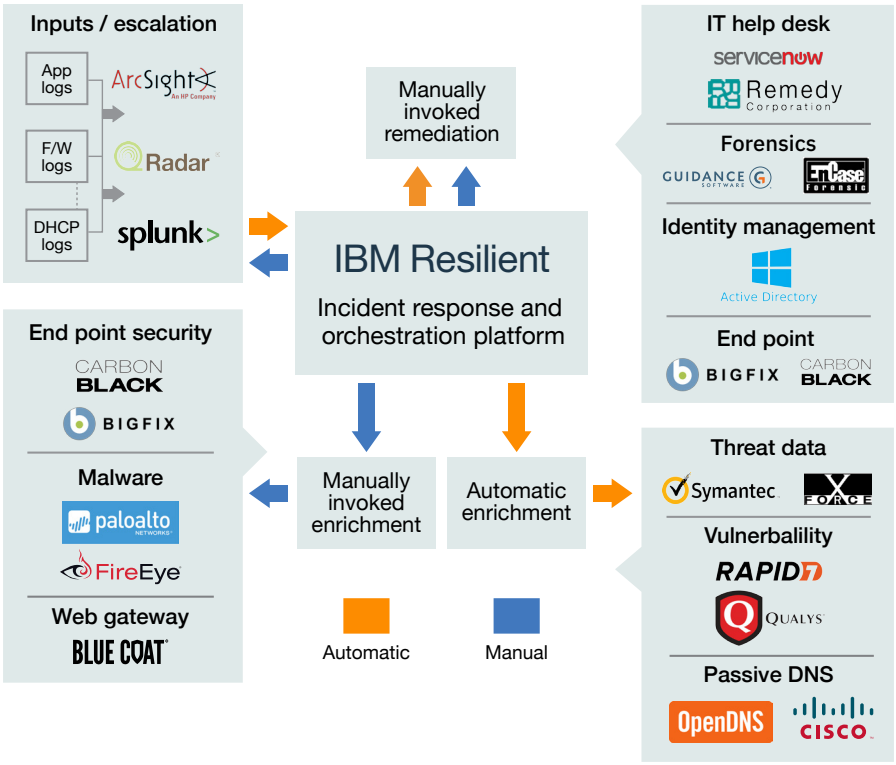

Figure 1: By integrating with your existing IT security solutions, the Resilient IRP open architecture provides a centralized platform for cyberattack investigation and remediation. Unlike ticketing systems and other general-purpose IT tools, the Resilient IRP is purpose-built for incident response, and can be customized quickly and easily to fit your team's specific needs.

Benefits of the Resilient Incident Response Platform by audience

Outside the SOC	Inside the SOC
For the Organization	**For the Director or SoC Manager**
• Documents that repeatable processes and SOPs are in place • Improves accountability by demonstrating post-incident what was done to rectify the situation • Records and benchmarks response time performance • Documents evidence (system of record) of abiding to rules and regulations for compliance audits	• Measures and improves SOC productivity • Automatically adapts response process to meet the attack • Enforces SLAs and improves mean time to resolve (MTTR) • Elevates staff effectiveness with tools to help them focus on the right tasks (addresses skills gap) • Demonstrates consistency of cyber response execution across regions/departments
For the CISO	**For the Analyst**
• Provides access and visibility into incident response program via dashboards and reporting (incident, staff, tool effectiveness metrics) • Provides measurable time-to-value of security spend • Increases ROI of security tools and demonstrates security's value to the business	• Helps analysts focus on investigation and response instead of pivoting between tools • Automates triage and enrichment tasks

Figure 2: This chart provides the benefits of the Resilient IRP advanced orchestration by audience.

Resilient IRP enables cyber resilience across the organization

Security module
Dynamic playbooks. Instant intelligence. Robust analytics
The Resilient IRP security module arms organizations with a powerful, dynamic platform for managing and resolving all incident types quickly and efficiently. With dynamic playbooks, integrated threat intelligence, and customizable analytics dashboards, the Resilient IRP security module helps organizations react faster, coordinate better, and respond smarter to security incidents.

"If we're responding to an incident, we need to be in the same tool, collaborating, with visibility, understand requests, and understand our roles in the response."

— Director of Cyber Security, Global Pharmaceutical Company

How the Resilient IRP security module benefits your organization

Security analyst:
Guided response
- Provides incident playbooks that guide analysts through a response, outlining their exact roles and responsibilities and providing guidance and deadlines
- Enables incident and artifact enrichment through built-in integration with a wide range of cyber threat intelligence feeds, such as IBM X-Force®

The Resilient IRP analytics dashboard will benefit many members of your team:

IR manager and SOC director:
Advanced dynamic playbooks
- Provides dynamic playbooks, which automatically adapts the response process to meet the attack and ensure that the right analyst is working on the right tasks with the right tools
- Enables fast and easy incident creation and tracking, to ensure all incidents are captured and followed through to resolution

CISO:
- Response simulations
- Provides incident simulation and reporting capabilities, enabling teams to test response plans, identify gaps, and refine response processes
- Analytics and reporting
- Includes analytics dashboards that display incident metrics across the organization, including incident levels by category, severity, and duration

Entire organization:
- Collaboration and communication
- Enables central collaboration to ensure all units across the organization understand their role when needed in a response, including IT, legal, marketing, HR, and the executive team

Resilient IRP dashboard

Orchestrate IR with Dynamic Workflows

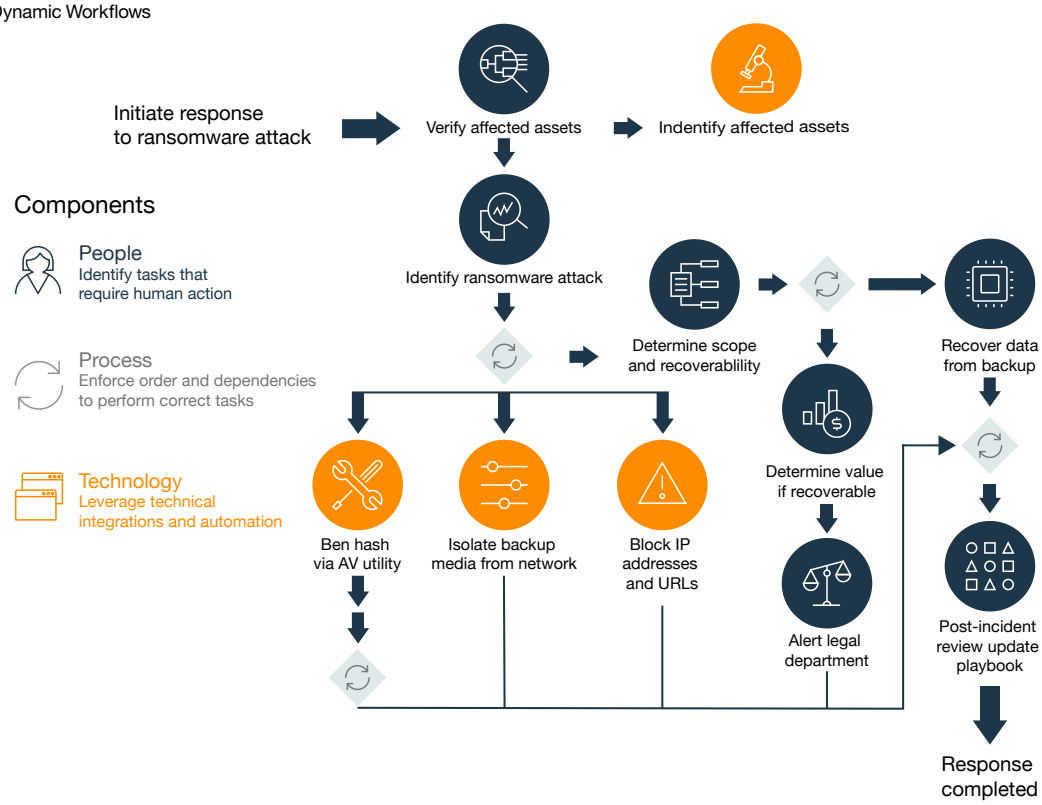

Figure 3: The Resilient IRP process responds quickly to a ransomware attack. This flowchart shows each phase of the response and where human action becomes involved.

Resilient IRP dashboard

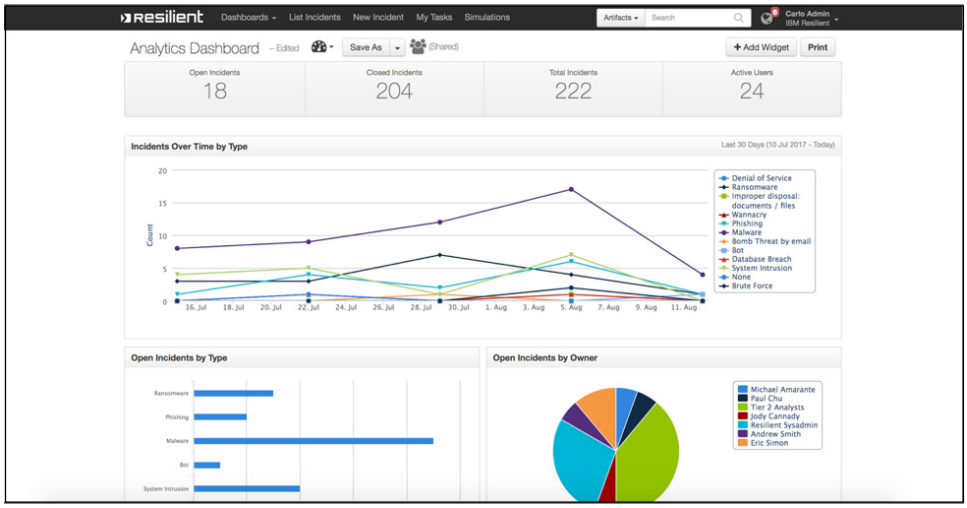

Figure 4: A real-time dashboard provides key information about security incidents within your organization.

Action module:

Integrated security hub for incident response orchestration and automation

Your IR team needs to be empowered to act beyond repetitive and basic tasks. The Resilient IRP action module streamlines your IR team's workload by orchestrating and automating incident response processes. By streamlining or eliminating repetitive and time-consuming steps, the action module allows users to focus on more strategic tasks and resolve incidents faster and more effectively.

With the Resilient IRP action module, users can build their own custom integrations with the IBM Resilient IRP open API framework or leverage its existing and proven deployments, as well as integrations built and delivered by the IBM Resilient partner ecosystem.

"We invested two years in improving our security. The Resilient Incident Response Platform was the capstone to that project—the critical piece that empowered all others"

— Chief Information Security Officer, Top Three Credit Card Network

How the Resilient IRP action module benefits your security analyst:

Faster and more efficient response

- Automates basic, repetitive tasks allowing analysts to spend more time on more strategic tasks
- Streamlines investigative tasks by pulling data and information from connect systems, such as SIEMs, firewalls, and endpoint security tools such as CMDB and LDAP, to bring context and help analysts prioritize their work
- Features incident visualization, which enables analysts to uncover broader, more complex attacks by seeing the relationships between artifacts and incidents in their environment

Incident visualization

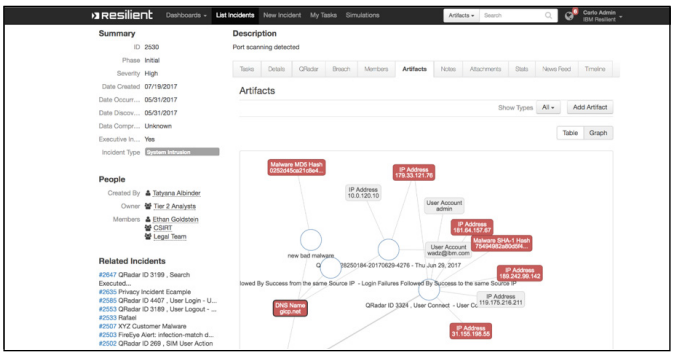

Figure 5: Example of Resilient IRP reporting of an incident occurring within an organization.

IR manager and SOC director:

Workflow visualization

- Enables IR managers and SOC directors to quickly and easily build and refine their teams' IR workflows with no coding.

Workflow visualization

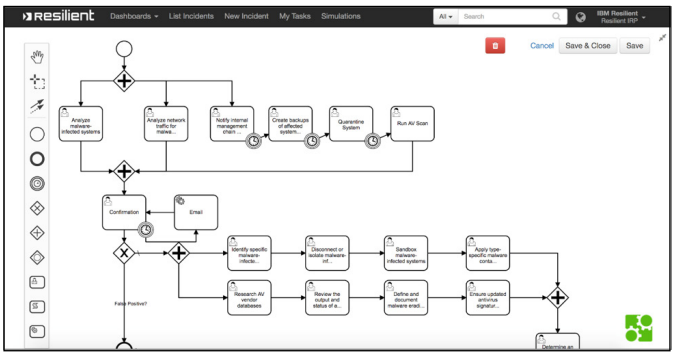

Figure 6: Resilient IRP enables simplified workflow creation and alteration.

Members your team will benefit from the Resilient IRP workflow visualization:

CISO:
Increased ROI

- Increases the ROI of existing security infrastructure by effectively enlisting other tools in the response process

Entire organization:
Skills gap relief

- Alleviates the skills gap by improving the effectiveness of existing staff, capturing institutional knowledge, and reducing staff burnout

Privacy module

An instant, configurable platform for data breach preparation, assessment, and management

When an incident occurs, it can take hours—if not days—to sort through the multitude of constantly shifting global regulatory obligations and planning out response processes. You can be left unsure if your response is complete. The Resilient IRP privacy module transforms the process into one that is fast, efficient, and compliant.

The privacy module is built on an industry-leading knowledge base of global regulatory requirements and is continually updated in real time by the IBM Resilient team of privacy and legal experts.

"The Resilient Platform is well vetted; I do not need to worry about re-reading every code section of each of the states. I have confidence in the system—that it will tell me what I need to do, when I need to send something out, and who I need to inform"

— Dickson Leung, Chief Privacy Officer and General Counsel, Health Equity

How the Resilient IRP privacy module benefits your organization

An instant, configurable platform for data breach preparation, assessment, and management

Legal associate:
Guided data breach notification

- Provides data breach response plans that map to the latest regulation—taking the complexity out of tracking privacy breach legislation, industry regulations, company-specific obligations, third-party requirements, and industry best practices.

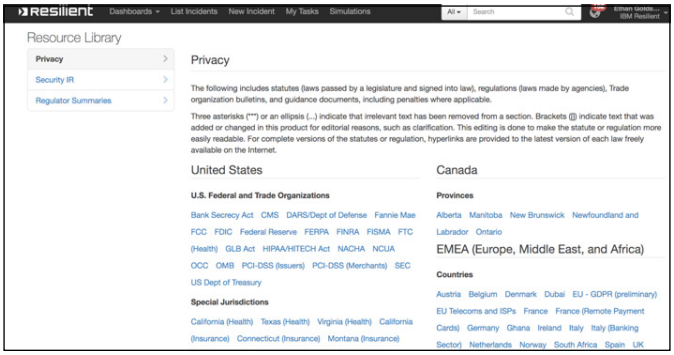

Figure 7: Resilient IRP provides up-to-date information about regulations worldwide

General Counsel or Chief Privacy Officer:

Up-to-date processes

- Ensures that data breach notification processes are always up-to-date, even in the face of frequently shifting legal landscapes

GDPR preparation

- Helps fulfill GDPR regulatory obligations and streamline incident response and breach notification time to remain compliant and avoid penalties

General Counsel or Chief Privacy Officer:

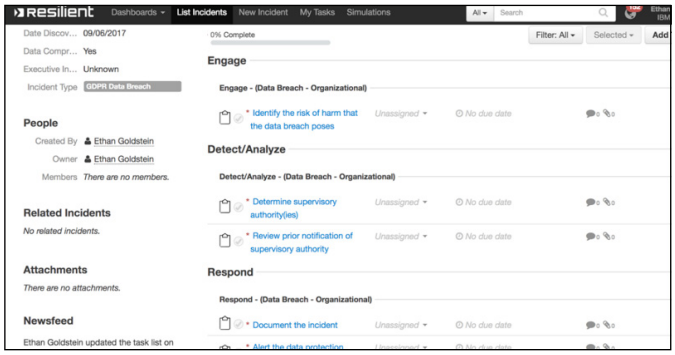

Figure 8: IBM Resilient provides guidance on proactively preparing for GDPR's impending requirements.

Improved incident management

- Provides a timeline of all recent activity which, in a rapidly unfolding incident, helps the privacy team identify any new updates to a response plan, and ensure incidents are successfully managed to completion.

Entire organization:
Privacy threat intelligence

- Includes reporting tools, which provide a clear picture of the specific threats businesses face most often—helping to identify areas of the business and incident types that require additional attention, and informing updates to company policies and procedures

Orchestrate your response and empower your security team to act faster and more intelligently.

For more information

To learn more about the IBM Resilient Incident Response Platform, contact your IBM sales representative or visit: **ibm.com**/us-en/marketplace/resilient-incident-response-platform

IBM Corporation
Security Group
Route 100
Somers, NY 10589

Produced in the United States of America
December 2017

BUO03065-USEN-00