The Guardium Integration Application for IBM Security Resilient

Connect IBM Security Guardium Data Protection with IBM Security Resilient for quick data incident response

Highlights

- Connect security operations with database management
- Accelerate incident investigation with automation and data visibility
- Take remediation actions from IBM Security Resilient
- Stay on-top of the complex data breach regulation environment and address notification requirements

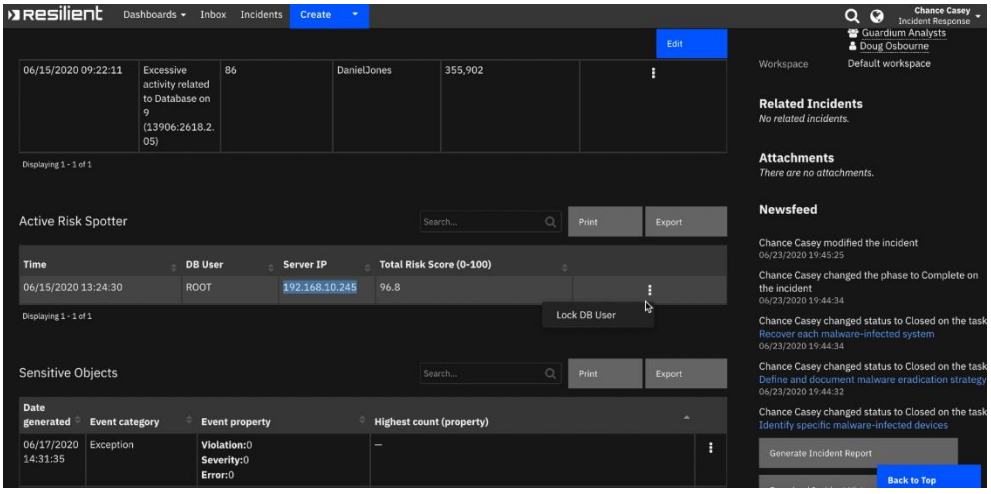
Overview

Businesses today are embracing hybrid multicloud-based IT deployment models at an increasing rate to improve agility and gain a competitive advantage. However, expanding your data footprint across on-premises and cloud environments increases your organization's attack surface, which can result in new data security challenges.

Security teams are compelled to protect their organization's data, while struggling with limited visibility and reporting abilities. Making matters more difficult, they can become inundated with data and cybersecurity point tools--each of which focus on specific environments or use cases, adding significant operational complexity. Without a solution that can contextualize insights from multiple security tools, and separate the signal from the noise, threats and vulnerabilities can go undetected, leaving organizations exposed to a potential security breach and data exfiltration.

A security breach comes at a high cost to organizations. According to Ponemon, the average total cost of a data breach is $3.92 million, which takes into consideration multiple factors ranging from legal to brand equity, to loss of customers, among others (Ponemon Institute, 2019). For this reason, organizations benefit from taking a proactive approach to data security and from having an incident response team and plan in place to help mitigate risk and reduce hacker dwell time in the case of a security incident. The deployment of security tools that use automation, such as a Security Orchestration, Automation, and Response (SOAR) platform, can help mitigate risk and costs.

The Guardium Integration Application for IBM Security Resilient connects the data activity monitoring capabilities of IBM Security Guardium Data Protection with the incident response and automation capabilities of IBM Security Resilient, a SOAR platform. With this integration, you can empower your security team to respond fast to incidents that may put your data at risk, like insider threats or data breaches, by automatically enriching incidents with information from your databases and taking remediation actions directly from Resilient.

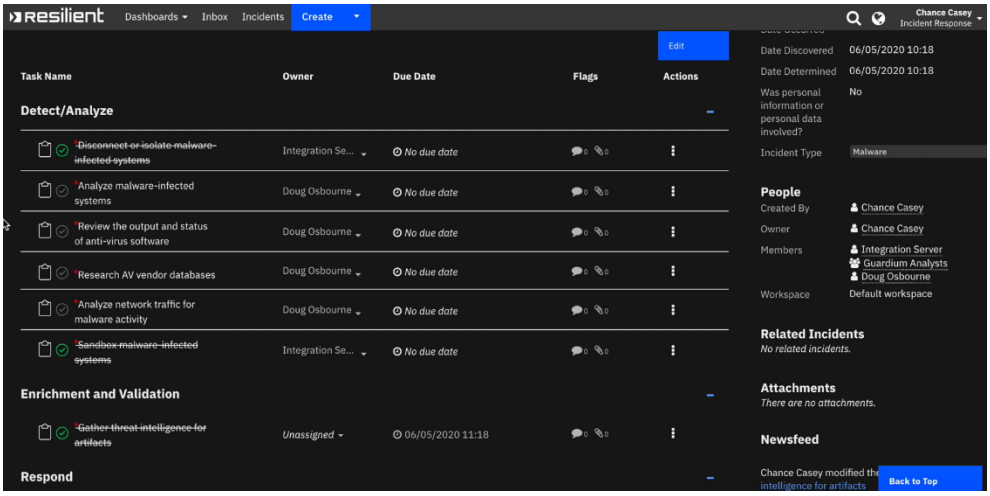


Guardium Activity Report in the Data Source Check Tab in IBM Security Resilient

Enable consistent collaboration across your database and security operations

As more organizations try to find innovative ways to make Security Operations Centers more effective and efficient to make up for the shortage of skilled security talent, building bridges that connect siloed teams across the organization and that improve communication between the different teams is critical.

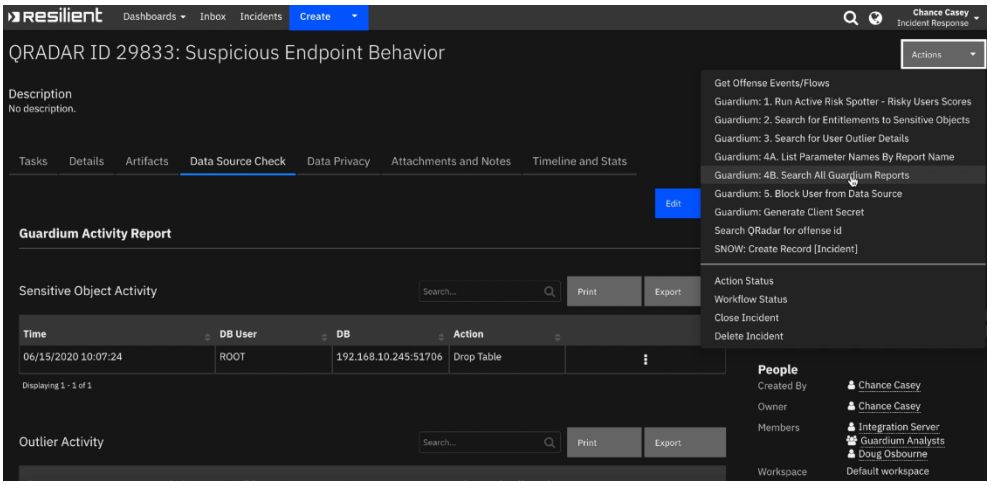
With the case management capabilities of IBM Security Resilient, you can help your security and privacy teams collaborate with consistency. You can assign tasks and due dates, manually or automatically, which triggers notifications for team members to complete their tasks. Communications can also extend beyond the SOC to include key stakeholders across the organizations, such as database managers, legal, human resources, etc.



List of tasks to be completed by incident response team in IBM Security Resilient

Reduce investigation time with automated incident enrichment from Guardium Data Protection

Resilient's orchestration and automation capabilities are designed to allow you to maximize your security investments by connecting with tools like Guardium Data Protection, and to save time by automating repetitive tasks such as incident enrichment. This new application is pre-configured so that Resilient can access, manually or automatically, standard and custom Guardium Data Protection reports to get additional insight into data at risk or the nature of privacy data breach if that's the case. For instance, leveraging Guardium's Risk Spotter feature, Resilient can automatically enrich incidents with the riskiest database users. With this information readily available to provide context to the incident, security analysts can make decisions fast and start remediation.

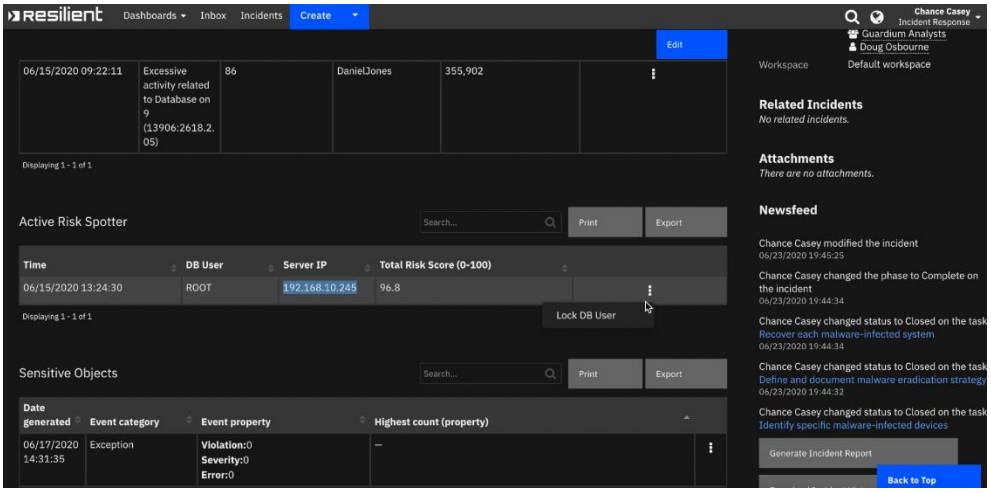


Enrich incidents with reports from IBM Security Guardium Data Protection

Begin incident remediation and response to data privacy breaches

Once a suspicious alert becomes an incident, security analysts need to act fast to contain and remediate the threat. The Guardium Integration Application for IBM Security Resilient allows incident responders to take actions from Resilient, such as blocking users.

The application gives security analysts visibility into sensitive data entitlement and activity reports, which provide insight into who has access to the database. If a bad actor is identified, then the analyst can revoke access for that user without having to go into Guardium Data Protection.



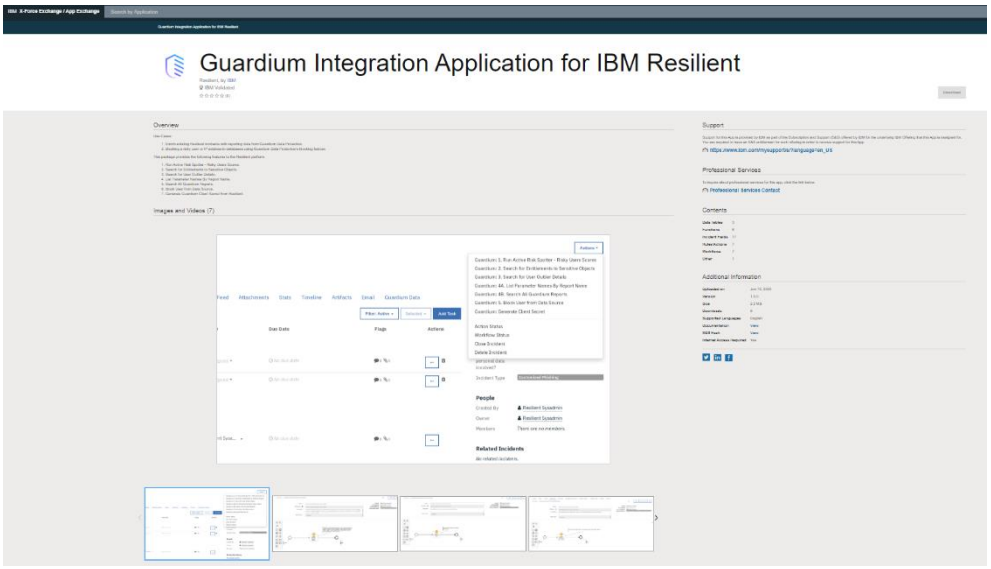
Lock user in IBM Security Guardium Data Protection from IBM Security Resilient

If a data privacy breach is determined during an incident, security analysts can pivot to IBM Security Resilient with Privacy, which integrates privacy use cases into Resilient's security case management. It supports security and privacy teams throughout the complex breach notification process. With the Global Privacy Regulations Knowledge-base at the heart of the solution, Resilient can alert to over 170 global regulations, including GDPR, PIPEDA, HIPAA, CCPA and all 50 stated breach notification rules to guide security and privacy teams throughout the complex breach notification process and help your security and privacy teams as they address compliance.

Deploy and install the application in minutes

The Guardium Integration Application for IBM Security Resilient is available to download from the IBM Security App Exchange. With

AppHost, Resilient's integration server, once you download the application, you can install it from the user interface with a guided installation process, which allows for editable settings and configurations.



Download the application from the IBM Security App Exchange

With this new integration, your organization will take a step towards a more robust zero-trust strategy, and your security team will be well positioned to respond to incidents that put your data at risk.

Visit the IBM Security App Exchange for more information on this app.

Sources: 1. Ponemon Institute. 2019 Cost of a Data Breach Report. June 2019

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

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. 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.

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

To learn more about IBM Security Resilient and IBM Security Guardium Data Protection, please contact your IBM representative or IBM Business Partner, or visit the following websites:

ibm.com/products/resilient-soar-platform
ibm.com/products/ibm-guardium-data-protection

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: ibm.com/financing