DATA SHEET

ARCHER

Archer® Cyber Incident & Breach Response

Use Case for IT & Security Risk Management

The Challenge

Identifying potential security issues and responding to cyber incidents are the first lines of defense in preventing a significant event. While many organizations have deployed security information and event management (SIEM) and log collection tools in their infrastructure to track events and provide alerts, these systems produce an overwhelming amount of data for the security team to review. Additionally, security response processes managed through spreadsheets and email can negatively impact the ability of the organization to respond.

Lack of sound methods to prioritize actionable security events, combined with manual, inconsistent operational response procedures, increases the overall risk that the organization will not adequately respond in time. Poor handoffs between security functions and IT teams leave little visibility into remediation efforts to close declared cyber incidents. They can also weaken the overall process to the point that it breaks down when needed most, namely during a breach.

Overview

Archer® Cyber Incident & Breach Response enables you to centrally catalog organizational and IT assets, establishing business context to drive incident prioritization and implement processes designed to escalate, investigate and resolve declared incidents effectively. The use case is designed for teams to work through defined incident response and triage procedures in preparation for response to a potential data breach.

Built-in workflows and reporting are designed for security managers to stay on top of the most pressing issues and to streamline processes. Issues related to a declared incident investigation can be tracked and managed in a centralized portal that provides full visibility and reporting. If an incident escalates into a data breach, prebuilt workflows and assessments are designed to help the broader business teams work with the security team to respond appropriately.

With Archer Cyber Incident & Breach Response, declared cyber and security events can be escalated quickly and consistently. Advanced workflow and insight to declared cyber and security incidents allow more efficient utilization of security team resources, resulting in faster response, analysis and closure rates for critical security incidents. With improved processes and capabilities, the security team can more effectively leverage existing infrastructure—such as SIEMs, log and packet capture tools, and endpoint security technologies—to focus on the most impactful incidents. These capabilities improve security team preparedness in the case of serious incidents involving potential data breaches, increasing the return on infrastructure investments while lowering overall security risk.

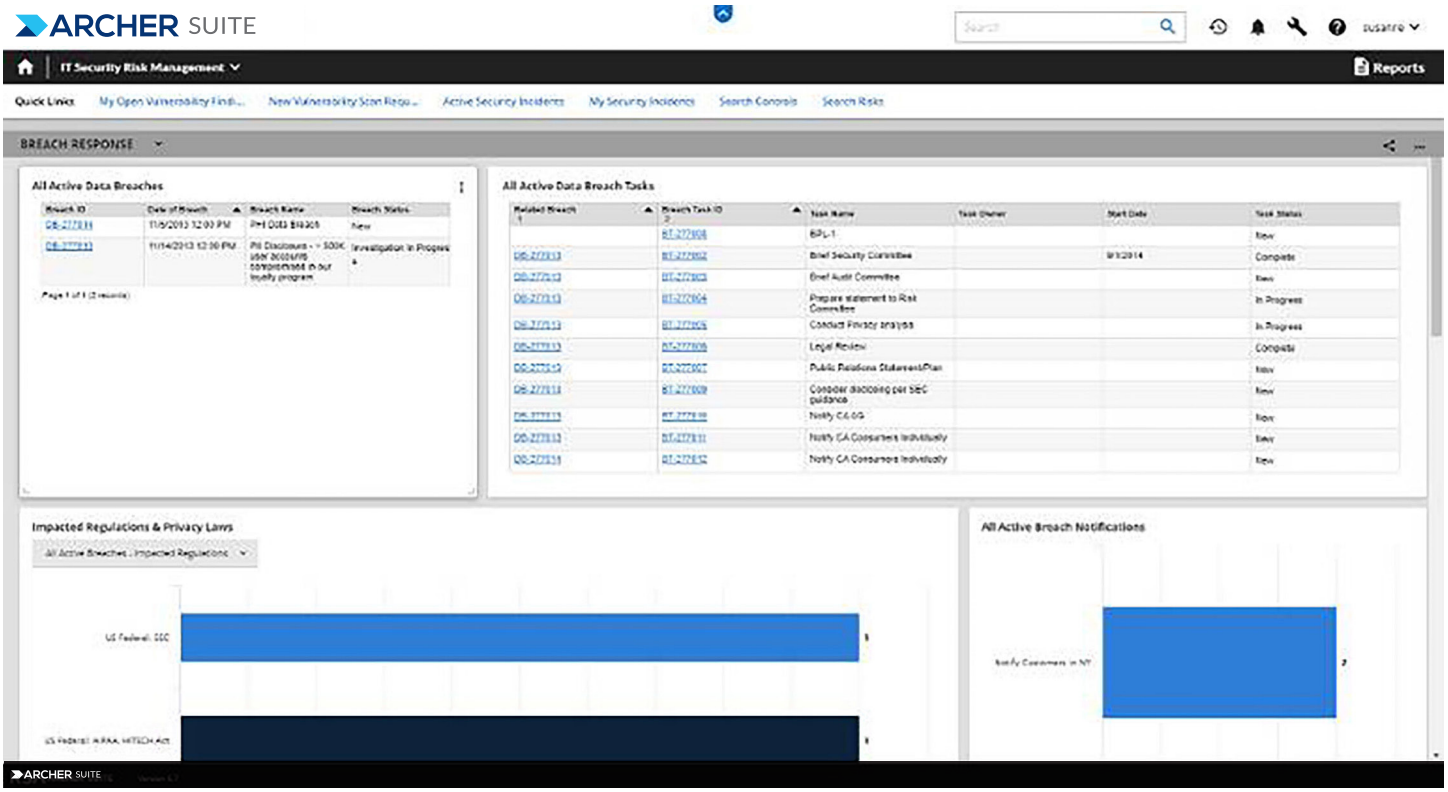
Key Features

- Centralized catalog of organizational and IT assets.
- Defined incident response lifecycle support with advanced workflow, escalation and response procedures.
- Central repository and taxonomy to manage processes related to security alerts.
- Integration with SIEM/log/packet capture infrastructure.
- Investigation support including incident journals and forensic analysis tracking.
- Issues management for IT operations
- Breach risk assessments.

Key Benefits

With Archer Cyber Incident & Breach Response, you can:

- Reduce effort to triage and remediate incidents.
- Improve accuracy of consolidated incident analysis and reporting.
- Reduce time and effort for security staff to escalate and respond to security alerts.
- Improve posture for breach response readiness.
- Lower security risk.



Discover More

Archer, an RSA company, is a leader in providing integrated risk management solutions that enable customers to improve strategic decision making and operational resiliency. As true pioneers in GRC software, Archer remains solely dedicated to helping customers understand risk holistically by engaging stakeholders, leveraging a modern platform that spans key domains of risk and supports analysis driven by both business and IT impacts. The Archer customer base represents one of the largest pure risk management communities globally, with over 1,500 deployments including more than 90 of the Fortune 100.

ARCHER
An RSA Business

©2020 RSA Security LLC or its affiliates. All rights reserved. RSA and the RSA logo are registered trademarks or trademarks of RSA Security LLC or its affiliates in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. 11/20 Data Sheet, H17003-2 W398052.