gemalto
security to be free

SOLUTION BRIEF

Adding Security Intelligence to Enterprise Key Management:

IBM Security QRadar and Gemalto SafeNet KeySecure

Modern networks have become so large and complex that they produce billions of data points daily and are increasingly difficult to protect. Encryption protects data in the event of a security breach but remains only as secure as the management surrounding the cryptographic keys. Protecting against abuse from privileged insiders adds an extra layer of complexity and administration to an already unwieldy set of enterprise security responsibilities.

Add regulatory requirements to these concerns, and annual audits that necessitate detailed reports, and the task of securing the network becomes overwhelming.

The Solution: Security Intelligence and Enterprise Key Management with IBM Security and Gemalto

IBM® QRadar® Security Intelligence Platform integrates with Gemalto SafeNet KeySecure to include encryption key logs in its Security Information and Events Management (SIEM) system. Combining QRadar and KeySecure allows administrators to consolidate key data and visualize key logs in a convenient graphical user interface (GUI) for closer, comprehensive monitoring of the enterprise key management infrastructure. KeySecure gives organizations the security and administrative advantages of centralized key management, while QRadar provides a tool that unlocks additional value from KeySecure's tracking features.

Key Benefits

Easily demonstrate compliance

> Out-of-the-box reports, automation, and key logging reduce the amount of timte needed to produce reports for auditors.

Stop insider risks

> SafeNet KeySecure's log integration with QRadar means that changes to encryption keys are recorded and monitored in real time, making it difficult for insiders to abuse their privileges.

Quick, customizable deployment

> Administrators can immediately use one of five default dashboards–security, network activity, application activity, system monitoring, or compliance. Users can also create new workspaces or customize preconfigured workspaces as needed.

Separation of duties

> Administrators can segregate data access based on job function so no single employee has total responsibility for the entire network's security.

FIPS -level security

> SafeNet KeySecure is available with an embedded FIPS 140-2 Level 3–validated, tamper-proof SafeNet Luna SA hardware security module. Encryption keys are safely stored in hardware so they are protected from potential theft or corruption.

IBM QRadar Security Intelligence Platform

QRadar organizes millions of data points from network security events so security teams can disrupt attacks before they are completed. The platform unifies SIEM, log management, anomaly detection, and configuration and vulnerability management in one solution. Real-time correlation reduces thousands of daily security alerts into a manageable list of actionable security insights worthy of further investigation.

In addition to superior threat detection, QRadar reduces the work involved in compliance reporting. Its out-of-the-box preconfigured reports make pulling audit information quick and easy. In QRadar, security administrators have an easy-to-use security analytics solution that improves threat identification and regulatory compliance, while lowering the total cost of ownership.

Gemalto SafeNet KeySecure

SafeNet KeySecure is an encryption and key management appliance that centralizes the control of an enterprise's disparate encryption solutions. By consolidating the policy and key management of application servers, databases, and file servers, it streamlines security administration. Centralized key management improves security in a number of ways, most notably by making key surveillance, rotation, and deletion easier, while separating duties so that no single administrator is responsible for the entire environment. Additionally, unifying and centralizing policy management, logging, and auditing makes information more readily accessible which, in turn, makes demonstrating compliance with data governance requirements simple.

IBM® QRadar® Security Intelligence Platform also integrates key logs and events from Gemalto SafeNet KeySecure encryption and key management appliance.

Key features

Regulation-specific reporting

To automate and simplify compliance tasks, QRadar provides collection, correlation, and reporting on compliance-related activity, backed by numerous out-of-the-box templates. It includes pre-built reports and rules templates for such regulations and control frameworks as CobiT, SOX, GLBA, NERC/FERC, FISMA, PCI DSS, HIPAA, UK GSi/GCSx, and GPG. Administrators can also create risk policies to evaluate asset and network device configurations, vulnerabilities, and communications—identifying the riskiest assets and pinpointing potential compliance issues. Encryption key information can easily be collected and reported through these features, greatly reducing the amount of time and effort involved with security audits.

Visualize data for improved security

QRadar presents consolidated data in an interactive GUI with "click-and-drill" capabilities that make it easier for administrators to analyze data deeply for patterns and anomalies. Integrating KeySecure and its logs will show changes to certificates and key states, as well as which applications users are accessing and which errors they are experiencing. This global, yet nuanced, view of the key management system makes it easier to identify abuse by privileged personnel or attacks from unauthorized users as they happen and before they cause damage.

Heterogeneous key management

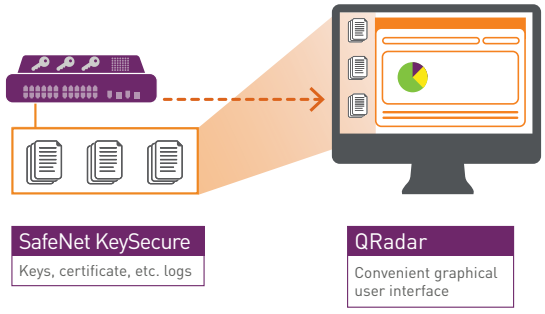
KeySecure manages symmetric, asymmetric, secret data, and X.509 certificates, along with their associated policies, for a variety of encryption products, including self-encrypting drives, tape archives, Storage Area Networks, virtual workloads, applications, and a growing list of vendors supporting the OASIS Key Management Interoperability Protocol (KMIP) standard. Despite the type of key or the encryption deployment, KeySecure logs and audit tracks in detail all key state changes, and administrator access and policy changes. These state and policy changes, and access events, are stored in data logs that are consolidated and monitored centrally in QRadar to create a more robust overall security posture.

Conclusion: Best-in-Class Security Intelligence and Key Management

Gemalto and IBM Security make securing data easy despite the ever-increasing sophistication of attacks and the growing complexities of IT environments. Together, the solution ensures that data is always secure with encryption and that the environment is thoroughly monitored so potential threats are addressed before they become a problem. Organizations now have a combined tool to sift through the massive amounts of security data in their networks for actionable insights, while also protecting valuable resources through encryption and centralized key management. To learn more, visit www.safenet-inc.com/partners/ibm/.

Monitor privileged user activity to prevent insider abuse

- When encryption key management is centralized with KeySecure, all changes to managed materials are recorded in special logs. Exporting these logs to QRadar allows security teams to closely monitor the key administrator to further protect against threats posed by privileged insiders.
- Unusual trends or inappropriate actions are more easily detectable when the key logs are visualized in QRadar's graphical user interface. The ability to click through different levels of data means that abuse by privileged users is less likely to get lost among the millions of events that are recorded daily.
- Additionally, integrating QRadar takes "separation of duties" one step further by adding a layer of oversight to key management, otherwise difficult to implement. Now, with the KeySecure and QRadar integration, organizations can divide responsibilities so no single administrator is responsible for more than one task – there is no reason to overlap management of the technical infrastructure, the encryption keys, or general oversight of the security system.



About Gemalto's SafeNet Identity and Data Protection Solutions

Gemalto's portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions–from the edge to the core. Gemalto's SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

SafeNet CERTIFIED

Business Partner IBM Ready for Security Intelligence

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com

Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free