A Broadcom Company
technologies

Product Brief

CA Mainframe Security Insights Platform

Key Benefits

- **Interpretation.** Quickly understand the story the data is telling through aggregation, correlation, and interpretation of various data points.
- **Assessment.** Hone in on high risk items using the risk assessment model from Security Insights.
- **Remediation.** Reduce risk with threat remediation. Detailed best-practices remediation options enable fast-tracking to a lower risk state.
- **Simple.** No programming skills required, experience is built-in.
- **Time savings.** No need to manually aggregate, correlate, and interpret data in spreadsheets.
- **Improved efficiency.** Streamlined administrative and reporting functions.

Key Features

- **APIs.** Security Insights uses data through APIs from other products or platform functions. Security Insights aggregates, correlates, and interprets the data and visually represents outcomes as a report and user interface. This data is available direct from each API and made available for organizations to use with additional in house tools such as SOC and SIEMs.
- **Sample output.** Select each use case to see the value of correlation, interpretation and remediation through sample reports before executing remediation.
- **Multi system support.** View Security Insights from multiple systems through a single pane.
- **Secure data output.** Users can only view data to which they are authorized.

At a Glance

Mainframe Security solutions from Broadcom® enables enterprises to use mainframe IT to solve business problems, take advantage of the opportunities that mainframe offers for digital transformation, and ensure a trusted environment for customers. Our solutions provide a foundation that enables the mainframe to connect with your network and hybrid cloud—across your enterprise. You can use this connection to securely deliver vital support for digital transformation.

CA Mainframe Security Insights Platform enables you to interpret and assess the security posture of the mainframe environment. CA Mainframe Security Insights Platform offers remediation steps that are built on experience and best practices to address all risky findings—on an ongoing and ad hoc basis.

Business Challenges

In today's hybrid cloud and hybrid IT environments, mainframes are more connected to enterprise processes than ever before in history. This connectedness changes the security context, opens new threat vectors, and raises the risk level. Access to the mainframe is more open than ever to employees, partners, contractors, and customers. These changes drive a need to understand the risk posture of the mainframe. To ensure the proven high securability of the mainframe, you must identify and address any high-risk areas. It can be challenging to assess the risk posture of the mainframe environment. You must leverage the correct data points—and not just the data points addressed by the auditor's checklist! Vast amounts of data need interpretation, honing of risk, and an understanding of the appropriate remediation actions. These activities can be resource intense and require a skill level built over years of experience.

The average global cost of a data breach is $3.92M, in the United States the average cost is $8.19 M, and the cost for a major business has predictions of more than $150M.[1] Companies cannot afford a lapse in security or compliance standards. Of the more than 8.5 billion records breached in 2019, 86 percent occurred through misconfigured assets—including cloud servers and a variety of other systems.[2] Detailed analysis and a comprehensive understanding of security information can help ensure that your vital data and customer data remain protected. This understanding can also help a business avoid fines and fees, and prevent brand damage that is detrimental or fatal to business operations.

Related Products

- **CA ACF2™ for DB2.** Externalizes security for IBM DB2 without the need for an exit.
- **CA Cleanup.** Find and remove obsolete, unused, redundant, and excessive access rights in CA ACF2, IBM RACF, and CA Top Secret.
- **CA Trusted Access Manager for Z.** Monitor and control privileged users by granting time-bounded just-in-time access to the system, critical resources and regulated data, or resources with 1:1 accountability and auditing.
- **CA Advanced Authentication for Mainframe.** True multi-factor authentication for mainframe users. Supports RSA hard/soft tokens, and radius protocol.
- **CA Compliance Event Manager.** A single source for the collection and monitoring of real-time, compliance-related information and events that occur within the mainframe environment. Has the ability to send information to Splunk or an enterprise SIEM solution.
- **CA Auditor (formerly CA-Examine Auditing).** In-depth auditing, integrity checks, and verification for z/OS.
- **CA Data Content Discovery.** Find and classify regulated and sensitive data to ensure that proper security and privacy controls are in place for the data.
- **CA Compliance Information Analysis (CIA).** Replicate compliance security information from the mainframe security database into a CIA relational data repository for compliance and ad-hoc SQL reporting.
- **CA LDAP Server for z/OS.** A full-function Lightweight Directory Access Protocol (LDAP)-compliant directory server.

Solution Overview

Security and compliance are some of the most critical components of an IT environment today, and have become continuing boardroom conversations. Broadcom continues to evolve its Mainframe Security Portfolio to address modern business requirements. Security and compliance requirements change, both from a threat vector and a platform support perspective. CA Mainframe Security Insights Platform is developed under a continuous delivery model, so the solution is prepared for the future and can adapt quickly to solve evolving business challenges.

Crucial Differentiators

- Broadcom listens to our customer's needs, working together to deliver new solutions to use cases within CA Mainframe Security Insights Platform to root out risks that may not be surfaced through the auditor checklist.
- Data is abundant in every aspect of the world. CA Mainframe Security Insights Platform goes beyond aggregating the data to a level of interpretation that moves security teams a step ahead, and ensures analysis of data to determine and remediate risk.
- CA Mainframe Security Insights Platform has a point and click user interface. No programming skills are required to gain the insight the solution provides.
- CA Mainframe Security Insights Platform implements ongoing innovations from Broadcom engineering staff—no third-party engineering.
- No need for expensive third-party mainframe administrative or reporting front-end software to perform tasks. CA Mainframe Security Insights Platform provides easy to use interfaces for your staff.

CA Mainframe Security Insights Platform Cycle

Related Products (con't)

- **CA PAM Client for Linux for System Z.** A flexible, open-source architecture for user authentication on Linux systems. CA PAM (Pluggable Authentication Module) client support enables CA ACF2 to act as an authentication server for one or more Linux systems, eliminating the need for redundant security administration on a system-by-system basis.
- **CA Distributed Security Integration (DSI).** This standalone daemon runs in the z/OS UNIX environment, independent of the CA LDAP Server. CA DSI allows applications on a Windows platform to issue calls to CA ACF2.

Additional Items for Consideration

Broadcom continues to innovate mainframe security capabilities. We also support the growing mainframe security ecosystem by delivering innovations other areas.

Education

Online education enables your staff to receive training for new features and functionality on demand. Modularized training allows for flexible learning.

Mainframe Vitality Residency Program

We will train your staff, or we will partner with you to find candidates if you are having trouble finding talent. We train new skills through our Vitality Residency Program and your candidates will become CA ACF2 experts. Once the candidate is fully trained with experience in your environment, they are available to transition and become one of your employees. They are fully certified in Broadcom Mainframe Security solutions—all at little to no cost to you.

Security Health Checks

No-cost reviews of key security settings and paid engagements for more in-depth reviews of your mainframe security configurations are available.

MRI Security Essentials

Compare key access control configurations and settings against industry best practices. Executive overviews and dashboards enable simpler reporting.

Communities

Learn, connect, and share with other CA ACF2 users as well as Broadcom product experts that promote peer-to-peer engagement.

Roadmap Sessions

Periodic sessions with the product team to view a showcase of future features and functionality. Your organization can prepare to take advantage of upcoming innovations.

For more information, please visit: mainframe.broadcom.com/security

1. Eye-Opening Data Breach Statistics for 2020, January 27, 2020, https://www.bigcommerce.com/blog/data-breaches/#the-costs-of-a-data-breach.

Ponemon 2019 Cost of a Data Breach report, https://www.ibm.com/security/data-breach.

2. X-Force Threat Intelligence Index Reveals Top Cybersecurity Risks of 2020.https://securityintelligence.com/posts/x-force-threat-intelligence-index-reveals-top-cybersecurity-risks-of-2020/.

https://www.ibm.com/downloads/cas/DEDOLR3W

A Broadcom Company

technologies

For product information and a complete list of distributors, visit our website at: broadcom.com

CA-SIP-zOS-PB100 September 17, 2020