FORCEPOINT
POWERED BY Raytheon

Datasheet

Forcepoint CASB Web Audit and Protection

WEB APPS ARE THE FACE OF YOUR BUSINESS. PROTECT IT THAT WAY.

PROTECTING WEB APPS WITH FORCEPOINT CASB

Many organizations have apps that their customers, partners and suppliers interact with. Keeping these apps secure is a top priority if an organization wants to protect its corporate reputation and bottom line.

However, cyber criminals pose significant risk in that they've become quite adept at leveraging social engineering techniques like spear phishing and pretexting to get their hands on legitimate login credentials. If they get them, they can easily take over a valid user's account to gain access as a privileged user, steal sensitive corporate data and bring an entire IT infrastructure to a standstill.

Matters get even more complex when you factor in regulatory requirements. In particular, organizations are required to provide detailed audit trails of their customers' activities, including logins, updates, downloads and more. If they're unable to provide these audit trails, their customers and partners won't be able to meet their own corporate governance or regulatory obligations.

MONITOR AND PROTECT AGAINST THE MISUSE OF STOLEN CREDENTIALS

Forcepoint CASB enables you to monitor and secure your customer-facing production applications that are running in your corporate data center or in public cloud computing environments like Amazon Web Services (AWS) and Microsoft Azure. Forcepoint CASB performs activity monitoring using a completely transparent deployment model that has no impact on user experience and does not require any changes to the production app itself.

FEATURES AND BENEFITS

- Protect against account takeover and misuse of stolen credentials
- Monitor and detect anomalous behavior (e.g., brute force attacks) in real-time
- Block or enforce risk-based multi-factor authentication for enhanced security
- Receive real-time alerts of suspicious activities
- Log all user activities to meet compliance requirements

Forcepoint CASB utilizes Dynamic User and Device Fingerprinting™ to automatically profile and detect anomalous behavior that might indicate an account takeover. Forcepoint CASB learns normal patterns of legitimate user behavior, including a person's typical endpoint devices and access locations, and continuously monitors for suspicious behavior. For instance, in an AWS environment, if a hacker or malicious insider tried to terminate a server instance or delete a database, Forcepoint CASB can either alert, block the action or apply two-factor authentication in real-time to require individuals to "prove" who they claim to be.

Forcepoint CASB offers several out-of-the-box policies to immediately detect and remediate account-centric threats.

DETECTED BEHAVIOR DETAILS	DESCRIPTION
Suspicious login volume	Number of successful logins within x days exceeds a predefined threshold
Session hijacking	Identical web sessions were detected on two or more different user devices
Anomalous data usage from unusual location	Fingerprint mismatch caused by activity from non-typical location accessing non-typical data
Unusual geography	Fingerprint mismatch caused by activity from unusual geographical location while user is not present in that location
Suspicious endpoint	Fingerprint mismatch caused by activity from non-typical geographic location using non-typical endpoint
Unusual access hours	Fingerprint mismatch caused by activity within non-typical time period
Anomalous data usage from unusual endpoint	Fingerprint mismatch caused by activity from non-typical endpoint accessing non-typical data
Simultaneous access	Simultaneous logins from two different locations within a short time period
Anomalous data usage from unusual location & endpoint	Fingerprint mismatch caused by activity from non-typical location and non-typical endpoint accessing non-typical data

Forcepoint CASB also enables the creation of custom policies in the event your production app must meet unique security and compliance requirements. With these custom policies, you can choose the "who, what, where, when and how" of your desired policy. Additionally, you can select the appropriate response when the policy gets triggered. For instance, you can choose to display an alert, block the specific action that triggered the alert in the first place, block the account outright or apply two-factor authentication to verify an individual's identity.

RETAIN DETAILED AUDIT TRAILS TO AVOID SANCTIONS AND FINES

The ability to track all user activities for compliance purposes is just as critical as protecting the app itself. Regulations such as HIPAA, PCI, DSS and several others are currently enforced across a number of industries. Forcepoint CASB tracks the user and admin activities of your organization's production apps in real-time, ensuring you retain complete audit trails that satisfy the most stringent compliance requirements.

The following table represents a small sample of regulations that require detailed recordings of user activities, including all access and modifications of sensitive data:

REGULATION	SECTION	DETAILS
HIPAA	**164.312(b)**	Audit controls - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
ISO 27002	**9.4.2 (f)**	Log unsuccessful and successful login attempts
PCI DSS	**10.7**	Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis.
NIST	**AU-2(1)(1)**	The information system must be capable of auditing based on a risk assessment and mission/business needs (e.g., account logon events, account management events, logon events, object access, policy change, privilege use, process tracking, and system events)
FFIEC	**Information Security - Appendix A (M)(5)**	Determine whether logs of security-related events are sufficient to support security incident detection and response activities, and that logs of application, host, and network activity can be readily correlated.

Forcepoint CASB generates consistent, normalized access logs that make it easy for you to meet the demands of internal and external auditors. It also provides a consolidated view of all your apps, simplifying and expediting your audit processes. Integration with leading SIEM solutions is available if you wish to track alerts and audit activities as part of your normal network operating center procedures. And finally, Forcepoint CASB provides these audit capabilities out-of-the-box, eliminating the need for custom development work.

WEB PROTECTION	
FEATURE	**DESCRIPTION**
ACTIVITY MONITORING & ANALYTICS	Real-time activity monitoring and analytics by user, group, location, device, application action, data object, time of day, and department
PRIVILEGED USER MONITORING	Real-time monitoring and reporting of privileged users and admins, including data access, configuration changes, user permission modifications, and more
AUTOMATIC ANOMALY DETECTION	Dynamic User and Device Fingerprinting™ continuously monitors behavior & automates detection for anomalous behavior including high-risk insider and external attacks
REAL-TIME THREAT PREVENTION	Stop account-centric threats by applying policy to monitor, block, allow or require identity verification for any app or upon specific actions within the app
MULTI-FACTOR AUTHENTICATION	Built-in capabilities that can be enforced globally, based on endpoint type or location, or automated in response to policy violations
DYNAMIC ALERTS	Receive real-time notifications for any policy violation or activity threshold via SMS or email
CUSTOM POLICIES	Visual policy editor enables easy configuration of granular policies based on any combination of user, endpoint, location, data object, action, time of day and more
WEB AUDIT	
FEATURE	**DESCRIPTION**
DETAILED ACTIVITY LOGS	Capture activity logs of user activities for data center and customer-facing applications
CENTRALIZED AUDIT LOCATION	Single, unified view of all apps for streamlined audits
ENTERPRISE SIEM INTEGRATION	Adaptors to directly feed activity logs into leading SIEM solutions such as ArcSight, Splunk, and Q1 Labs
ENTERPRISE REPORTING	Flexible reporting options, including pre-defined reports with ability to edit and save customized reports

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[DATASHEET_FORCEPOINT_CASB_WEB_AUDIT_PROTECTION_EN]-100057.022217