FORCEPOINT
POWERED BY Raytheon

Hoja de datos

Forcepoint CASB Auditoría y protección de la web

LAS APLICACIONES WEB SON LA CARA DE SU EMPRESA. PROTÉJALAS COMO CORRESPONDE.

PROTECCIÓN DE APLICACIONES WEB CON FORCEPOINT CASB

Muchas organizaciones poseen aplicaciones con las que interactúan sus clientes, socios y proveedores. Mantener seguras estas aplicaciones es una de las prioridades principales si una organización desea proteger su reputación corporativa y sus utilidades.

Sin embargo, los delincuentes cibernéticos constituyen un riesgo importante, ya que se han convertido en expertos en sacar provecho de técnicas de ingeniería social como el phishing dirigido y el pretexto para apoderarse de credenciales de inicio de sesión legítimas. Si lo logran, pueden apropiarse fácilmente de la cuenta de un usuario válido para tener acceso como usuario con privilegios, robar información corporativa sensible y paralizar una infraestructura de TI completa.

Las cosas se complican aún más cuando se tienen en cuenta los requisitos reguladores. En particular, las organizaciones deben proporcionar seguimientos de auditoría detallados sobre las actividades de sus clientes, incluyendo inicios de sesión, actualizaciones, descargas y más. Si no pueden proporcionarlos, sus clientes y socios no podrán cumplir con sus propias obligaciones reguladoras o de gobierno corporativo.

MONITOREO Y PROTECCIÓN CONTRA EL USO INDEBIDO DE CREDENCIALES ROBADAS

Forcepoint CASB le permite monitorear y proteger sus aplicaciones de producción orientadas a clientes que se ejecutan en su centro de datos corporativos o en entornos informáticos en la nube pública, como Amazon Web Services (AWS) y Microsoft Azure. Forcepoint CASB monitorea las actividades mediante el uso de un modelo de implementación totalmente transparente que no tiene impacto en la experiencia del usuario y no requiere ningún cambio en la aplicación de producción.

CARACTERÍSTICAS Y BENEFICIOS

- Protección contra apoderamiento de cuentas y uso indebido de credenciales robadas
- Monitoreo y detección de conductas anómalas (p. ej., ataques de fuerza bruta) en tiempo real
- Bloqueo o aplicación de autenticación de múltiples factores basada en riesgos para una mejor seguridad
- Alertas de actividades sospechosas en tiempo real
- Registro de todas las actividades de los usuarios para satisfacer requisitos de cumplimiento

Forcepoint CASB utiliza la impresión digital dinámica de dispositivos y usuarios (Dynamic User and Device Fingerprinting™) para automáticamente trazar un perfil y detectar conductas anómalas que podrían indicar un apoderamiento de cuentas. Forcepoint CASB aprende patrones normales de conducta de usuarios legítimos, incluidos los dispositivos finales típicos de una persona y las ubicaciones de acceso, y monitorea en forma continua en busca de conductas sospechosas. Por ejemplo, en un entorno de AWS, si un hacker o un empleado con malas intenciones intentara finalizar una instancia de un servidor o borrar una base de datos, Forcepoint CASB puede alertar, bloquear la acción o solicitar la autenticación de dos factores, en tiempo real, para exigir a las personas que "demuestren" quiénes afirman ser.

Forcepoint CASB ofrece diversas políticas predeterminadas para detectar y remediar en forma automática las amenazas centradas en cuentas.

DETALLES DE CONDUCTAS DETECTADAS	DESCRIPCIÓN
Volumen sospechoso de inicios de sesión	La cantidad de inicios de sesión exitosos en "X's" días excede un límite predefinido
Secuestro de sesión	Se detectaron sesiones web idénticas en dos o más dispositivos diferentes de un usuario
Uso anómalo de datos desde una ubicación inusual	Falta de coincidencia en la impresión digital provocada por una actividad procedente de una ubicación no típica desde donde se tiene acceso a datos no típicos
Geografía inusual	Falta de coincidencia en la impresión digital provocada por una actividad procedente de una ubicación geográfica inusual mientras el usuario no está presente en esa ubicación
Dispositivo final sospechoso	Falta de coincidencia en la impresión digital provocada por una actividad procedente de una ubicación geográfica no típica que utiliza un dispositivo final no típico
Horas de acceso inusuales	Falta de coincidencia en la impresión digital provocada por una actividad realizada en un período de tiempo no típico
Uso anómalo de datos desde un dispositivo final inusual	Falta de coincidencia en la impresión digital provocada por una actividad procedente de un dispositivo final no típico que tiene acceso a datos no típicos
Acceso simultáneo	Inicios de sesión simultáneos desde dos ubicaciones diferentes en un período corto de tiempo
Uso anómalo de datos desde una ubicación y un dispositivo final inusuales	Falta de coincidencia en la impresión digital provocada por una actividad procedente de una ubicación no típica y un dispositivo final no típico que tiene acceso a datos no típicos

Forcepoint CASB también permite la creación de políticas personalizadas en el caso de que su aplicación de producción deba cumplir con requisitos únicos de seguridad y cumplimiento. Con estas políticas personalizadas, puede escoger el "quién, qué, dónde, cuándo y cómo" de su política deseada. Además, puede seleccionar la respuesta apropiada al aplicarse la política. Por ejemplo, puede escoger el mostrar un alerta, bloquear la acción específica que activó el alerta en primer lugar, bloquear la cuenta en el acto o aplicar autenticación de dos factores para verificar la identidad de una persona.

CONSERVACIÓN DE SEGUIMIENTOS DE AUDITORÍA DETALLADOS PARA EVITAR SANCIONES Y MULTAS

La capacidad para realizar un seguimiento de todas las actividades de los usuarios con fines de cumplimiento tiene una importancia tan crucial como la protección de la aplicación misma. Actualmente se aplican regulaciones como la HIPAA, PCI, DSS y muchas otras en diversas industrias. Forcepoint CASB realiza un seguimiento en tiempo real de las actividades de usuarios y administradores en las aplicaciones de producción de su organización, lo que le permite conservar seguimientos de auditoría completos que satisfacen los requisitos de cumplimiento más estrictos.

La tabla siguiente representa una pequeña muestra de las regulaciones que exigen registros detallados de las actividades de los usuarios, incluidos todos los accesos y las modificaciones de datos sensibles:

REGLAMENTACIÓN	SECCIÓN	DETALLES
HIPAA	**164.312(b)**	Controles de auditoría: Implementar hardware, software y/o mecanismos procedimentales que registren y examinen la actividad en los sistemas de información que contienen o utilizan información de salud electrónica protegida.
ISO 27002	**9.4.2 (f)**	Registrar intentos de inicio de sesión exitosos y no exitosos.
PCI DSS	**10.7**	Conservar el historial de seguimiento de auditoría durante al menos un año; al menos tres meses de historiales deben estar disponibles en forma inmediata para análisis.
NIST	**AU-2(1)(1)**	El sistema de información debe ser capaz de auditar con base a una evaluación de riesgos y necesidades de la empresa/misión (p. ej., eventos de inicio de sesión de cuentas, eventos de gestión de cuentas, eventos de inicio de sesión, acceso a objetos, cambio de políticas, uso de privilegios, seguimiento de procesos y eventos del sistema).
FFIEC	**Seguridad de la información - Apéndice A (M)(5)**	Determinar si los registros de eventos relacionados con la seguridad son suficientes para respaldar las actividades de detección de incidentes de seguridad y respuesta a ellos, y que los registros aplicación, huésped y actividad en la red se puedan correlacionar con facilidad.

Forcepoint CASB genera registros de acceso consistentes y normalizados que facilitan el cumplimiento de las exigencias de auditores internos y externos. También brinda una vista consolidada de todas sus aplicaciones, lo que le permite simplificar y agilizar sus procesos de auditoría. Está disponible la integración con las principales soluciones SIEM si desea realizar el seguimiento de alertas y actividades de auditoría como parte de sus procedimientos normales del centro de operaciones de redes. Y finalmente, Forcepoint CASB proporciona estas funcionalidades de auditoría listas para usar, lo que elimina la necesidad de trabajo de desarrollo personalizado.

PROTECCIÓN DE LA WEB	
FUNCIÓN	**DESCRIPCIÓN**
MONITOREO Y ANÁLISIS DE ACTIVIDAD	Monitoreo y análisis de actividad en tiempo real por usuario, grupo, ubicación, dispositivo, acción en una aplicación, objeto de datos, hora del día y departamento.
MONITOREO DE USUARIOS CON PRIVILEGIOS	Monitoreo y elaboración de informes en tiempo real de usuarios con privilegios y administradores, incluido el acceso a datos, cambios de configuración, modificaciones de permisos de usuarios y más.
DETECCIÓN AUTOMÁTICA DE ANOMALÍAS	La función Dynamic User and Device Fingerprinting™ monitorea constantemente el comportamiento y automatiza la detección de conductas anómalas, incluidos empleados de alto riesgo y ataques externos.
PREVENCIÓN DE AMENAZAS EN TIEMPO REAL	Detiene las amenazas centradas en cuentas mediante la aplicación de políticas para monitorear, bloquear, permitir o requerir verificación de identidad para cualquier aplicación o ante acciones específicas dentro de la aplicación.
AUTENTICACIÓN DE MÚLTIPLES FACTORES	Capacidades incorporadas que se pueden aplicar en forma global, basadas en el tipo o la ubicación del dispositivo final, o automatizadas en respuesta a violaciones de políticas.
ALERTAS DINÁMICAS	Reciba notificaciones en tiempo real referente a cualquier violación de política o límite de actividad a través de un mensaje SMS o de correo electrónico.
POLÍTICAS PERSONALIZADAS	El editor visual de políticas permite la fácil configuración de políticas granulares, basada en cualquier combinación de usuario, dispositivo final, ubicación, objeto de datos, acción, hora del día y más.
AUDITORÍA DE LA WEB	
FUNCIÓN	**DESCRIPCIÓN**
REGISTROS DETALLADOS DE ACTIVIDAD	Captura registros de la actividad de usuarios para centros de datos y aplicaciones orientadas a usuarios.
UBICACIÓN DE AUDITORÍA CENTRALIZADA	Una sola vista unificada de todas las aplicaciones para auditorías simplificadas.
INTEGRACIÓN CON SIEM EMPRESARIAL	Adaptadores que proveen registros de actividad directamente a las principales soluciones SIEM, como ArcSight, Splunk y Q1 Labs
ELABORACIÓN DE INFORMES EMPRESARIALES	Opciones flexibles de elaboración de informes, que incluyen informes predefinidos con capacidad para editar y guardar informes personalizados.

CONTACTO
www.forcepoint.com/contact

ACERCA DE FORCEPOINT

[DATASHEET_FORCEPOINT_CASB_WEB_AUDIT_PROTECTION_ES]-100057.022217