BPROT

Más que protección, ofrecemos tranquilidad:
Con nuestras soluciones de ciberseguridad su empresa estará más segura y podrá entender fácilmente lo que ocurre en su red.

SHIELD ARMOR FORTRESS

Tenemos una solución adaptable a su empresa

bprot.com

BPROT

El guardián de su información,
para que su negocio no se detenga.

Elija el nivel de seguridad que su empresa necesita hoy, y crezca con nosotros mañana.

SHIELD

Control de red
Control de navegación

ARMOR

Control de red
Control de navegación
Seguridad proactiva

FORTRESS

Control de red
Control de navegación
Seguridad proactiva
Inventario de red
Control e-mail
Control de personal
Aplicación Web

bprot.com

CONTROL NAVEGACIÓN

BPROT

INCLUIDO EN:

SHIELD ARMOR FORTRESS

Monitoreo de Navegación:
Obtenga visibilidad en tiempo real de la actividad de navegación web de los usuarios, permitiendo la identificación proactiva de patrones de uso no autorizados o riesgosos.

Conozca el tiempo ocupado en cada sitio:
Acceda a métricas detalladas sobre el tiempo de permanencia por sitio web, facilitando la optimización de la productividad y la identificación de posibles fugas de información. Se puede configurar la distribución automatizada de informes de actividad a los usuarios para promover la adhesión a las políticas de uso.

Vigile los accesos seguros (https):
Implemente control de accesos HTTPS para garantizar la seguridad y el control sobre el tráfico cifrado, permitiendo la aplicación de políticas de filtrado y prevención de amenazas en comunicaciones seguras. Este control se logra sin instalar certificados o configurar servidor proxy en cualquiera de los dispositivos de la red.

Optimice la velocidad de su red:
Optimice el rendimiento de la red priorizando el tráfico crítico de negocio y minimizando la latencia causada por contenido no productivo o malicioso, a través de políticas de filtrado y QoS (Quality of Service).

Información a su alcance:
Acceda a inteligencia de amenazas y actividad de usuario mediante reportes exhaustivos en tiempo real e históricos, desagregados por sitio, dirección IP, usuario y eventos de bloqueo, facilitando la auditoría y el cumplimiento normativo.

Protección automática:
Configure políticas de acceso granulares con reportes automatizados de sitios web visitados, permitiendo la gestión proactiva de dominios permitidos y denegados para fortalecer la postura de seguridad y cumplir con las políticas corporativas.

Políticas de uso:
Implemente un framework de políticas de uso personalizables, permitiendo la definición de reglas de navegación basadas en roles, grupos de usuarios, equipos y categorías de sitios web, asegurando el cumplimiento de la política de seguridad de la información. También se puede regularizar el uso de determinadas aplicaciones que generan poco rendimiento a los usuarios

Control detallado: Realice un control granular y en tiempo real de la navegación, incluyendo el monitoreo de URL accedidas y el tiempo de permanencia. La solución permite el bloqueo dinámico de accesos, la generación de informes forenses detallados y la protección automatizada contra sitios de phishing y malware conocidos.

CONTROL DE RED

BPROT

INCLUIDO EN:

SHIELD ARMOR FORTRESS

Control total:
Implemente controles de acceso basados en políticas por equipo o usuario a nivel de aplicación (Layer 7), tales como WhatsApp o TeamViewer, mitigando riesgos de fuga de datos y optimizando la productividad del personal. Todo ello, con una gestión centralizada y simplificada.

Protección en tiempo real:
Proporcione protección perimetral en tiempo real contra amenazas avanzadas como spam, virus, malware y ataques de denegación de servicio (DoS/DDoS) dirigidos a la infraestructura, con capacidad de generar informes de eventos en tiempo real e históricos para análisis forense.

Optimización de la red:
Identifique y aísle proactivamente los cuellos de botella de la red y las fuentes de latencia. Acceda a dashboards en tiempo real e históricos con visibilidad granular de la actividad de los usuarios y el consumo de ancho de banda por destino, facilitando la optimización de recursos.

Monitoreo de equipamiento crítico:
Monitoree proactivamente la disponibilidad y el rendimiento de la infraestructura crítica de red (servidores, switches, routers), con alertas tempranas ante anomalías o fallos que puedan impactar la continuidad del negocio.

Teletrabajo seguro (VPN):
Facilite el acceso seguro y cifrado a la red corporativa desde ubicaciones remotas mediante capacidades de VPN (Virtual Private Network), garantizando la integridad y confidencialidad de los datos en tránsito.

Simple interpretación de datos:
Visualice métricas clave del uso de la red a través de paneles de control intuitivos y gráficos interactivos, que permiten una rápida comprensión de la topología y el flujo de tráfico.

Mapa de Red:
Genere una representación gráfica de la topología de red, proporcionando una vista integral de los dispositivos conectados y sus interconexiones, facilitando la identificación de activos y la planificación de la infraestructura.

Diagnostique las causas de la degradación del rendimiento de la red. Obtenga protección avanzada y alertas en tiempo real ante actividades maliciosas. Implemente la contención de aplicaciones bajo demanda y habilite el teletrabajo seguro a través de VPNs. Acceda a una suite de informes analíticos para auditoría y cumplimiento.

SEGURIDAD PROACTIVA

INCLUIDO EN:

ARMOR FORTRESS

Análisis de vulnerabilidades:

Realice escaneos de vulnerabilidades para identificar activos y servicios expuestos en la red, priorizando las debilidades que podrían ser explotadas por actores maliciosos para obtener acceso no autorizado.

Revisión de credenciales:

Identifique automáticamente servicios con configuraciones por defecto o credenciales débiles, reduciendo la superficie de ataque y fortaleciendo la higiene de seguridad.

Conocimiento para prevenir ataques:

Adquiera una visión consolidada y en tiempo real del posture de seguridad de la red, habilitando la toma de decisiones informadas para la mitigación de riesgos y la planificación de estrategias de defensa.

Alertas ante eventos:

Reciba notificaciones en tiempo real (vía Telegram o correo electrónico) ante la detección de servicios vulnerables o eventos críticos de seguridad, permitiendo una respuesta inmediata.

Simple visualización de los resultados detectados:

Dispositivos	Servicios	Tcp	Udp	Credenciales
318	348	264	84	0

Problemas	Problemas aceptados	Advertencias	Advertencias aceptadas
30	0	54	0

Simple interpretación de la situación en su empresa.
Bajo Demanda: Ejecute análisis de vulnerabilidades bajo demanda o programados, obteniendo un inventario exhaustivo de sus debilidades de seguridad. Esta inteligencia permite una remediación proactiva, adelantándose a posibles vectores de ataque.

INVENTARIO DE RED

INCLUIDO EN:

FORTRESS

Inventario de equipos:

Realice un inventario exhaustivo de hardware y software desplegado en los endpoints (Windows, *Nix), incluyendo la detección de configuraciones y aplicaciones. Se configura la notificación automática a los administradores de sistemas ante cualquier cambio en el baseline del inventario.

Inventario de dispositivos:

Implemente el descubrimiento automatizado de activos de red, identificando y categorizando dispositivos como switches, routers, firewalls y otros componentes de infraestructura, para mantener un CMDB actualizado.

Notificaciones ante cambios:

Reciba alertas proactivas y automatizadas ante cualquier modificación en la configuración de los dispositivos de red, facilitando la detección de desviaciones y la auditoría de cambios.

Organización de Infraestructura:

Automatice la detección y clasificación de la infraestructura de red en función de los roles de los servidores (e.g., servidores de base de datos, servidores de correo electrónico), optimizando la gestión de activos y la aplicación de políticas de seguridad basadas en roles.

Granularidad: Genere un inventario detallado y dinámico del software y hardware de su red. Reciba alertas en tiempo real ante cualquier cambio de configuración, lo que permite mantener la integridad de su infraestructura y cumplir con los requisitos de compliance.

INCLUIDO EN:

FORTRESS

CONTROL E-MAIL

Envío de correo:
Monitoree la actividad de los flujos de correo electrónico entrantes y salientes a nivel corporativo, incluyendo metadatos y contenido.

Información detallada:
Acceda a informes forenses en tiempo real e históricos sobre el volumen y patrón de correos electrónicos, identificando los principales emisores y receptores para análisis de comportamiento y cumplimiento.

Limpieza remota:
Implemente filtros avanzados de spam y phishing, reduciendo la carga de correo no deseado en los buzones de los usuarios y mejorando la eficiencia de la comunicación.

Direcciones autorizadas:
Detecte y alerte sobre el envío de correos desde cuentas externas a través de la infraestructura de correo interna, identificando posibles configuraciones erróneas o actividades maliciosas (e.g., retransmisión de spam).

Protección Local:
Implemente un gateway de correo seguro que realice filtrado de contenido, adjuntos maliciosos, escaneo de virus y aplicación de políticas basadas en listas negras/blancas y remitentes autorizados, antes de la entrega al buzón de usuario.

Identificación de virus:
Detecte y contenga la propagación de malware basado en correo electrónico, incluyendo virus de envío masivo y ransomware, mediante análisis heurístico y basado en firmas.

Implemente un control integral y en tiempo real del flujo de correo electrónico (SMTP). Defina reglas de protección avanzadas, acceda a reportes detallados para auditoría y forense, y obtenga visibilidad sobre la presencia de amenazas persistentes en la red.

CONTROL DE PERSONAL

INCLUIDO EN:

FORTRESS

Uso de Programas:
Monitoree la utilización de aplicaciones por usuario, con métricas detalladas sobre el tiempo de uso productivo vs. no productivo, facilitando la optimización de recursos de software y el análisis de la eficiencia operativa.

Registro de entrada/salida:
Registre con granularidad las actividades del usuario desde el inicio de sesión en la red, proporcionando una traza detallada de eventos, incluso en entornos de estaciones de trabajo compartidas, lo que mejora la atribución y la auditoría.

Capturas de pantalla:
Capture de forma periódica o bajo demanda las pantallas de los usuarios, proporcionando evidencia visual de la actividad en el escritorio, útil para la investigación de incidentes o el cumplimiento de políticas.

Capturas de teclado:
Realice keylogging para registrar las pulsaciones de teclado de los usuarios, una funcionalidad clave para el análisis forense y la prevención de fuga de información sensible.

Actividad de archivos:
Rastree y audite las operaciones de los usuarios sobre archivos (creación, modificación, eliminación, acceso), permitiendo la trazabilidad de la información y la prevención de pérdida de datos.

Controles aún fuera de la empresa:
Extienda las capacidades de monitoreo y control a usuarios que operan fuera del perímetro corporativo (trabajo remoto), garantizando la visibilidad y el cumplimiento de las políticas de seguridad sin importar la ubicación física.

Sistema Integral: Implemente un sistema integral de monitoreo de actividad del personal, capturando métricas detalladas sobre el tiempo de trabajo efectivo, uso de aplicaciones, capturas de pantalla, registros de teclado y operaciones de archivos. Esto permite una supervisión exhaustiva y el cumplimiento de las políticas de uso de recursos

INCLUIDO EN:

FORTRESS

APLICACIÓN WEB

Protección permanente:
Implemente una defensa robusta y continua para sus aplicaciones web contra el Top 10 de OWASP y otras vulnerabilidades de explotación comunes, garantizando la integridad y disponibilidad de sus servicios online.

Monitoreo en tiempo real:
Obtenga visibilidad en tiempo real sobre los intentos de acceso y los eventos de seguridad (permitidos/bloqueados) dirigidos a sus aplicaciones web, lo que permite una respuesta rápida a incidentes.

Alertas ante eventos:
Reciba notificaciones automatizadas en tiempo real ante la detección de ataques o anomalías en el tráfico de sus aplicaciones web, habilitando la contención proactiva.

Fácil configuración:
Implemente políticas de seguridad y configuraciones de alerta de manera ágil e intuitiva, reduciendo el tiempo de despliegue y la curva de aprendizaje.

Reportes simples de actividad:
Simple interpretación de la actividad en tiempo real e histórica.

Blindaje Completo: Blindaje integral para sus aplicaciones web contra los vectores de ataque más prevalentes. Reciba alertas de seguridad en tiempo real y acceda a reportes detallados de actividad, lo que permite un monitoreo proactivo y una auditoría efectiva de la seguridad de sus activos web.

Contáctenos a: info@bprot.com

lo invitamos a visitar nuestra web

https://bprot.com