Censornet MFA

cobranetworks.lat
Tel. +52 55 5599 0691
ventas@cobranetworks.lat

Censornet Multi-Factor Authentication (MFA)

Acceso seguro a una amplia gama de sistemas, servicios y aplicaciones mediante una solución de autenticación de múltiples factores basada en la nube. Proteja las cuentas de usuario con un código de acceso dinámico único para cada sesión adicional a la contraseña y reduzca el impacto de la reutilización de contraseñas, esté preparado para cuando ocurra el próximo ataque de robo de datos a gran escala.

"Censornet MFA" es proporcionado a través de Censornet suite, que también incluye seguridad de correo, seguridad web, seguridad de aplicaciones en la nube y autenticación de múltiples factores, proporciona una única interfaz web para la configuración y gestión central de políticas, así como para la visualización y generación de reportes.

Censornet MFA es un servicio en la nube, lo que simplifica y acelera la implementación ahorrando tiempo para organizaciones de todos los tamaños, no se requiere de una infraestructura compleja, los clientes de autenticación están disponibles para todos los principales proveedores como iOS y Android.

Existen dos versiones disponibles: "el servicio Cloud MFA" y Censornet "on premise MFA", producto que es específicamente para las organizaciones que quieren que los componentes centrales se ejecuten dentro sus propios entornos.

El servicio Censornet MFA proporciona un panel central para analizar y administrar la actividad de autenticación a través de múltiples sistemas, servicios y aplicaciones independientemente de si los usuarios están en la red corporativa o trabajar de forma remota.

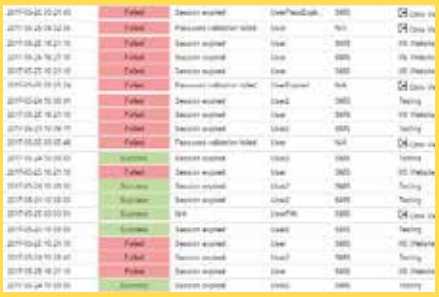
Censornet MFA admite diferentes políticas de envío para la entrega de OTPs, a través de múltiples métodos que incluyen SMS, correo electrónico o aplicaciones móviles de Censornet para Android y Apple iOS.

Conmutación automática por error en caso de una falla en la entrega de OTPs a los usuarios, incluso cuando no tienen señal de móvil, por ejemplo. La conmutación por error se configura en el backend y proporciona continuidad de servicio al usuario, en comparación con otras ofertas donde los usuarios tienen que seleccionar su método de autenticación a mano.

AUTENTICACIÓN MULTIFACTOR

- El backend 100% basado en la nube simplifica implementación y gestión.
- Diseñado para ofrecer al usuario una experiencia de fácil uso y una seguridad superior al acceso local o remoto de las aplicaciones empresariales de uso crítico.
- Multiusuario y multinivel, adecuado para organizaciones de cualquier tamaño, así como para proveedores de servicios.
- Códigos de acceso de un solo uso (OTP), específicos para una sesión de usuario, evitando la suplantación de identidad.
- Los OTPs generados en tiempo real brindan mayor seguridad comparados con aplicaciones que brindan códigos por secuencias por tiempo predeterminado.
- Las políticas de despacho ofrecen una opción de OTP métodos de entrega con conmutación por error automática para la garantía de entrega independientemente del usuario.
- Bloqueo de usuarios con un solo clic, revocando inmediatamente el acceso a todos los servicios protegidos por Censornet MFA.
- Uso de aplicación Censornet para dispositivos Android y Apple para recibir las notificaciones cifrada de extremo a extremo y tomar acción, ya sea para aceptar o bloquear el acceso en tiempo real.
- Servicio Censornet MFA listo para ser usado con una amplia gama de sistemas, servicios y aplicaciones incluidos todos los principales proveedores de VPN (Citrix, Cisco, Barracuda, Fortinet, etc.), Microsoft (incluyendo OWA, SharePoint) y las principales aplicaciones en la nube (Office 365, Salesforce, entre otras).
- Completamente integrado con Microsoft Active Directory.
- Servicio multicapa, escalable, sistemas "backend" con balanceo de carga y alta disponibilidad.

El servicio Censornet MFA mantiene registro detallado de la actividad de autenticación de usuarios, para cumplir con auditoría, regulaciones y legislación, multi-factor proporcionar la evidencia necesaria.



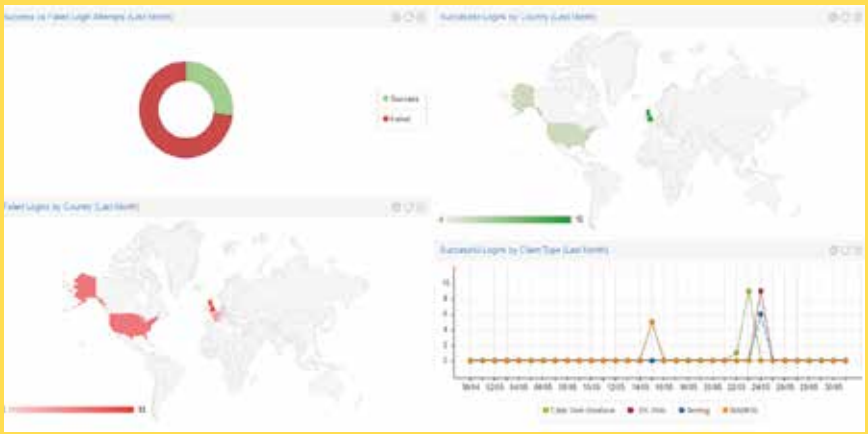
El MFA de Censornet usa memoPasscodes™, una forma única de generar códigos de acceso eso los hace muy fáciles de memorizar y simples para que los usuarios ingresen al iniciar sesión. La aleatoriedad del código de acceso, y por lo tanto la seguridad, no se ve afectada.

MFA utiliza el motor de sincronización AD de la plataforma Censornet, lo que permite una integración total con Microsoft® Active Directory con opciones para usar Local Sync o Cloud Sync. Local Sync utiliza un servicio de conector de AD instalado localmente por medio de un agente, o sincronización de todos los objetos de un árbol a través de Censornet Cloud.

Las actualizaciones diferenciales ocurren cada 15 segundos Cloud Sync utiliza una conexión LDAP o LDAPS para extraer objetos. Local Sync tiene el beneficio adicional de no requerir ningún cambio en las reglas del firewall, ambos métodos requieren una cuenta de servicio de solo lectura en AD. Una vez configurada, la sincronización de AD, está disponible en todas las soluciones de la plataforma Censornet.

Censornet MFA utiliza memoPasscodes™, una forma única de generar contraseñas.

La autenticación multifactor está completamente integrada con la Plataforma Censornet y proporciona visualización de todos los datos e informes a través de un amplio conjunto de atributos y criterios. El análisis y los informes están disponibles por períodos de tiempo, usuario, dirección IP, datos geo-IP, éxito o inicio de sesión fallido y por tipo de cliente



CARACTERÍSTICAS

Clientes de autenticación / Soporte de protocolo	• Soporte para proteger un número ilimitado de clientes de autenticación • RADIUS (protege el acceso VPN, por ejemplo, Citrix Access Gateway o Cisco VPN) • Inicio de sesión de Windows (protege el acceso RDP a los servidores) • ADFS (protege aplicaciones en la nube como Salesforce o Google Apps) • Interfaz web de Citrix (anterior a Citrix Access Gateway con RADIUS) • Sitio web de IIS (protege Outlook Web Access o RD Web Access)
Soporte de proveedores	• Los proveedores admitidos incluyen Barracuda, Check Point, Cisco, Citrix, F5, Google, Juniper Networks, Microsoft, OpenVPN, Palo Alto Networks, Salesforce, Teldat, VMWare.
Políticas de despacho de OTP	• Las políticas de despacho definen el método de entrega OTP con anulación para usuarios individuales. Los métodos de entrega incluyen: • SMS • Correo electrónico • Aplicación Censornet • SMS con conmutación por error a correo electrónico • Aplicación Censornet con conmutación por error a SMS
Generador de código aleatorio OTP	• Basado en un algoritmo aprobado por FIPS 140-2
	• Compatibilidad con SMS estándar y flash

Aplicación móvil censornet MFA	• Disponible para Android e iOS para OTP con cifrado de extremo a extremo.
Transmisión OTP	• Los costos de transmisión OTP están incluidos (sujeto a la política de uso justo).

INFORMES

Visibilidad en tiempo real	• Los gráficos de productividad muestran una visibilidad instantánea del cumplimiento de las políticas definidas. Consulte la actividad de autenticación en tiempo real por usuario, dirección IP, datos de geo-IP, resultado de inicio de sesión, tipo de cliente de autenticación. Vea exactamente qué usuarios se están autenticando en qué sistemas, servicios y aplicaciones.
Generador de informes	• Los administradores pueden definir sus propios informes en función de los nombres y criterios de los campos disponibles. • Los informes se pueden guardar y luego exportar a CSV o PDF. Los informes de auditoría se pueden buscar utilizando criterios que incluyen hora, usuario, dirección IP, datos de geo-IP, inicio de sesión exitoso o fallido y tipo de cliente
Programación y alertas	• Vincule los informes a los horarios y opcionalmente, solo reciba un informe cuando haya contenido (modo de alerta). • Alerta sobre inicios de sesión fallidos, usuarios específicos, etc.
Informes de tendencias principales	• Una selección de informes de tendencias predefinidos con datos de gráficos y tablas. Los informes de tendencias se pueden exportar a PDF y enviar por correo electrónico a los destinatarios.
Múltiples vistas	• Analice e informe por usuario, dirección IP, datos de geo-IP, resultado de inicio de sesión, tipo de cliente de autenticación.
Retención de registros y archivo automático	• Los datos de registro de MFA se archivan automáticamente después de 1 año y están disponibles para descargar desde la Plataforma Censornet por un período de 12 meses más. Están disponibles períodos de retención más largos.

ADMINISTRACIÓN

Sincronización de usuarios	• El servicio de sincronización de Active Directory garantiza que se repliquen los cambios en Active Directory.
Interfaz web	• Totalmente integrado con la Plataforma Censornet.

DESPLIEGUE

Back-end	• Altamente escalable, totalmente redundante y 100% basado en la nube, entregado desde múltiples centros de datos ubicados en EE. UU., Reino Unido y Europa continental.
Clientes de autenticación	• Agentes fáciles de instalar implementados en servicios locales protegidos por MFA para conectarse al backend de la nube.

+52 (55) 5599-0691 ventas@cobranetworks.lat cobranetworks.lat

E. EMAIL

Protección integral contra las amenazas de correo electrónico tradicionales, incluidos spam, virus, ataques de phishing a gran escala y direcciones URL maliciosas.

S. SAT

Defiende tu organización contra los ciberdelincuentes fortaleciendo su participación y estimulación automatizada.

W. WEB

Proteja a los usuarios de la web, malware, contenido ofencivo o inapropiado y mejora la productividad.

C. CASB

Descubra, analice, asegure y administre la interacción del usuario con aplicaciones en la nube, en línea y mediante API.

M. MFA

Reducir el impacto de grandes violaciones de datos, protegiendo cuentas de usuario con algo más que contraseñas.

ID. IDaaS

Controle el acceso de los usuarios con amenaza de identidad. Automáticamente autenticar a los usuarios usando datos contextuales.

Nuestra Plataforma

Nuestra plataforma de seguridad en la nube integra seguridad de correo electrónico, web y aplicaciones en la nube, trabajando a la perfección con una identidad poderosa para activar la Autonomía del Motor de seguridad (ASE).

Esto lo lleva más allá de la seguridad basada en alertas y en ataque automatizado en tiempo real prevención.

Motor de seguridad autónomo

Habilite los productos tradicionalmente para compartir y reaccionar ante eventos de seguridad y estado de datos mientras aprovecha la amenaza de clase mundial. Prevenga los ataques antes de que ocurran.

ASE proporciona seguridad las 24 horas del día, los 7 días de la semana para que usted no tenga que hacerlo.

Acceso completo a inteligencia de amenazas.

Dirección:

Prolongación División del Norte 4318, C.P. 14300 Ciudad de México, México.

Teléfono:

+52 (55) 5599-0691

Correo Electrónico:

ventas@cobranetworks.lat

cobranetworks.lat

COBRA NETWORKS