eScan®
Enterprise Security

eScan Vision Core XDR

(con defensa de inteligencia neuronal lA/ML)

eScan Vision Core XDR (Detección y Respuesta Extendida - XDR) es una solución de seguridad para endpoints más amplia y en capas que ofrece visibilidad en tiempo real, análisis, protección y remediación para los endpoints. Esto proporciona conocimientos más profundos y alerta al administrador sobre actividad maliciosa, lo que facilita una investigación más rápida y restringe los ataques en los endpoints tan pronto como se detectan.

Vision Core XDR consta de los últimos módulos como simulación de phishing y radar de lP. Además, se incluye un marco MlTRE ATT&CK (Tácticas, Técnicas y Conocimientos Comunes de Adversarios) para brindar a su red una cobertura de ciberseguridad ampliada. Como una solución de seguridad de nivel empresarial, admite acciones automatizadas y manuales para restringir las amenazas potenciales en el endpoint. Reduce proactivamente el ataque, previene infecciones de malware y neutraliza amenazas potenciales detectándolas en tiempo real. eScan Vision Core XDR está diseñado utilizando tecnologías demandadas y futuristas disponibles para endpoints basados en Windows, Mac y Linux en toda la empresa.

eScan
Vision Core XDR
(con defensa de inteligencia neuronal IA/ML)

eScan®
Enterprise Security

Why eScan Vision Core XDR?

Gestión Uniforme

• Consola basada en web con panel resumido

La nueva Interfaz Web Segura utiliza tecnología SSL para cifrar todas las comunicaciones. El panel resumido de eScan proporciona a los administradores el estado de los endpoints administrados en formato gráfico, incluyendo estado de despliegue, estado de protección y estadísticas, resumen del Top 10, cambios en activos, estado en vivo y radar de IP.

• Gestión de Activos

El módulo de Gestión de Activos de eScan ayuda a los administradores a rastrear la información del hardware y la lista de software instalado en los endpoints. Además, permite visualizar los cambios en hardware realizados en la configuración de los sistemas de la red. También permite exportar informes detallados para obtener un conocimiento más profundo.

Protección Extendida para Endpoints

• Prevención de Fugas de Datos (DLP)*

Con capacidades adicionales como control de archivos adjuntos, control de contenido, protección de archivos y carpetas sensibles, monitoreo de actividad de archivos, aplicaciones de espacio de trabajo y varias otras funciones, eScan protege a las organizaciones del riesgo asociado con la transferencia no autorizada de contenido sensible. Es una función adicional.

• Autenticación en Dos Factores (2FA)*

eScan proporciona una capa adicional de protección al proceso de inicio de sesión que autentica y evita que cualquier criminal acceda a la computadora y los datos personales. Esto ofrece un paso adicional de seguridad, ya que los ciberdelincuentes requieren más que un nombre de usuario y contraseña para la autenticación. Es una función adicional.

Desarrollado por tecnologías futuristas

• Patrón de Aprendizaje No Intrusivo (NILP)

eScan utiliza el Patrón de Aprendizaje No Intrusivo (NILP), una tecnología revolucionaria que utiliza Filtrado Bayesiano y funciona bajo los principios de Inteligencia Artificial (IA) para analizar cada correo electrónico y evitar que los correos de spam y phishing lleguen a su bandeja de entrada. Tiene capacidades de autoaprendizaje y se actualiza por sí mismo utilizando feeds de investigación regulares desde los servidores de MicroWorld. Utiliza un mecanismo adaptativo para analizar cada correo electrónico y categorizarlo como spam o legítimo en función del patrón de comportamiento del usuario

• Motor de Análisis de Comportamiento Proactivo (PBAE)

PBAE proporciona protección en tiempo real para organizaciones y usuarios contra ataques de Ransomware. Monitorea la actividad de todos los procesos y bloquea aquel cuyo comportamiento coincida con el de un Ransomware.

• Capa MicroWorld Winsock (MWL)

La "MicroWorld-WinSock Layer" (MWL) de eScan es un concepto revolucionario en el escaneo del tráfico de Internet en tiempo real. Ha cambiado la forma en que el mundo enfrenta las amenazas de seguridad de contenido. A diferencia de otros productos y tecnologías, MWL aborda una amenaza antes de que llegue a sus aplicaciones. MWL está técnicamente ubicado por encima de la capa WinSock y actúa como un "Guardián Transparente" en la capa WinSock del sistema operativo.

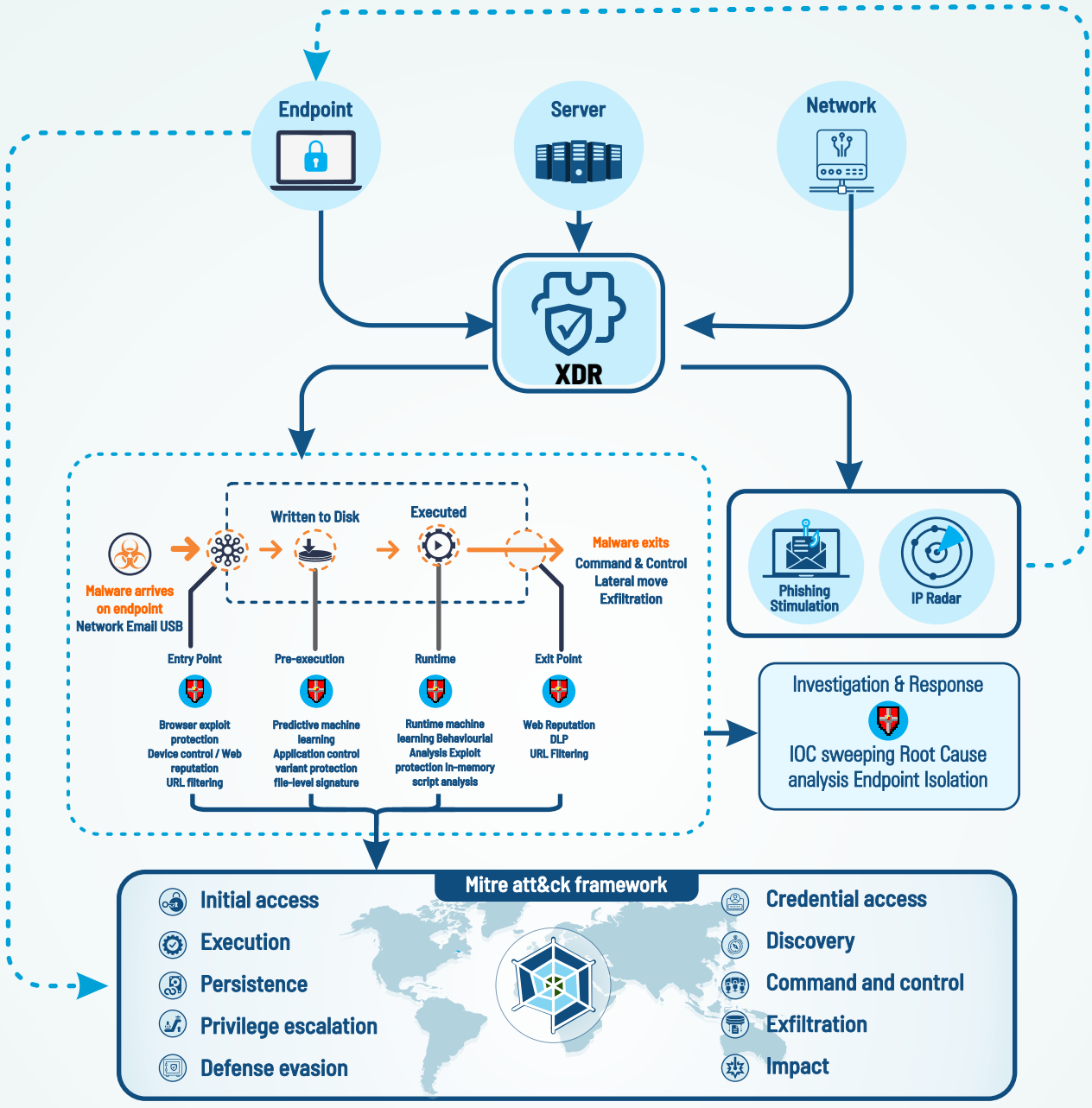
eScan
Vision Core XDR
(con defensa de inteligencia neuronal IA/ML)

eScan Enterprise Security

Powered By Futuristic Technologies

- **Módulo de Protección de Servicios de Terminal (TSPM)**

  eScan está equipado con un TSPM mejorado que no solo detecta y bloquea los intentos de fuerza bruta y las direcciones IP sospechosas, sino que también permite incluir en la lista blanca las direcciones IP para conexiones RDP seguras.



eScan
Vision Core XDR
(con defensa de inteligencia neuronal IA/ML)

eScan®
Enterprise Security

Características Clave - Consola de Administración de eScan

Panel de Control EDR

eScan proporciona el panel resumido de los incidentes, lo que permite a los administradores obtener información más profunda y tomar acciones más rápidas en cuanto se detectan amenazas. Proporciona una visión general de incidentes como eScan, Windows, Endpoints y Red, tanto en formato gráfico como en detalle

Anti-Robo*

eScan te ayuda con el bloqueo del dispositivo, alertas, sonido de alarma, borrado de datos y localización de dispositivos. eScan garantiza una protección completa contra cualquier acceso no autorizado en caso de pérdida o robo del dispositivo. Es una función adicional para endpoints con Windows.

Agrupación Automática

Esta función permite al administrador agregar clientes automáticamente a subgrupos apropiados. Aquí, los administradores deben crear grupos y luego definir criterios para los clientes, basándose en nombre de host, nombre de host con comodín, dirección IP o rango de IP

Configuraciones Mejoradas

eScan proporciona diversas configuraciones avanzadas como clientes en roaming, prevención de brotes, integración con SIEM, creación de informes con logotipo personalizado, plantillas de criterios de políticas, entre muchas otras

Sincronización con Active Directory (ADS)

Con esta función, los administradores pueden sincronizar los grupos de la Consola Centralizada de eScan con los contenedores de Active Directory. Las nuevas computadoras y contenedores descubiertos en Active Directory se copian automáticamente en la Consola Centralizada de eScan y se envía una notificación a los administradores del sistema.

Clientes Excluidos

Esta función permitirá al administrador restringir que endpoints no administrados sean agregados automáticamente a cualquier grupo. El administrador debe agregar las computadoras a la lista usando el nombre de host, nombre de host con comodín, dirección IP o rango de IP. Las computadoras listadas no serán agregadas automáticamente al grupo administrado.

Prevención de Brotes

Si la cantidad de virus excede los límites establecidos por el administrador, se enviará una notificación de brote por correo electrónico al destinatario especificado por el usuario. Esto activará automáticamente el aislamiento de endpoints infectados para restringir la infección en la red

Administración Basada en Roles

La Administración Basada en Roles a través de la Consola de Administración de eScan permite a los administradores crear grupos de administradores basados en niveles con un conjunto de privilegios predefinidos para un acceso más seguro

eScan
Vision Core XDR
(con defensa de inteligencia neuronal IA/ML)

eScan®
Enterprise Security

Características Clave - Consola de Administración de eScan

Simulación de Phishing

La nueva funcionalidad de Simulación de Phishing de eScan permite al equipo de inteligencia de amenazas de la organización evaluar la comprensión de los empleados sobre las amenazas de phishing en correos electrónicos, que son ampliamente utilizados por los atacantes.
En términos simples, la simulación de phishing es una actividad interna donde se envía un correo electrónico de phishing simulado a los empleados para evaluar si hacen clic en los enlaces incrustados o ignoran el correo electrónico.
Estos correos electrónicos de phishing son creados imitando los correos electrónicos de phishing reales. Si los empleados responden al correo electrónico haciendo clic en los enlaces, la acción se almacena para un análisis posterior con el fin de llevar a cabo un programa de concienciación sobre phishing

Radar de IP

eScan ha agregado Radar de IP en su panel de control de la consola web. Es un mapa global donde se pueden ver todas las conexiones IP activas y establecidas que han sido iniciadas y conectadas al servidor de eScan.
Esta función permite rastrear todas las conexiones IP que están actualmente activas a través del servidor de eScan. En términos simples, cuando la comunicación IP es iniciada entre el sensor XDR y los recursos externos a nivel mundial, será capturada y mostrada en el mapa en tiempo real.
Lo mejor de esta función es que Radar de IP no requiere ningún servicio de terceros para su funcionamiento.

Plantillas de Políticas

La plantilla de políticas hace que la implementación de políticas sea sencilla; permite al administrador crear políticas de seguridad y cumplimiento y aplicar estas políticas a los grupos administrados designados.

Actualizador en Vivo del Cliente

Con la ayuda del Actualizador en Vivo del Cliente de eScan, los eventos relacionados con eScan y el estado de seguridad de todos los endpoints son capturados, registrados y pueden ser monitoreados en tiempo real. También puede exportar eventos en un archivo de Excel.

eScan
Vision Core XDR
(con defensa de inteligencia neuronal IA/ML)

eScan®
Enterprise Security

Características Clave - eScan Vision Core XDR

Recolector de Eventos (Eventos de Seguridad) y Correlación

Todos los eventos de seguridad de Windows (intentos de inicio de sesión no autorizados, conexiones RDP y cambios en las políticas) son monitoreados para detectar cambios en el comportamiento, violaciones de políticas y exceder los derechos otorgados. Estos eventos luego se envían al servidor con protocolos seguros para análisis de amenazas y almacenamiento. Además, se recopilan todos los registros del sistema operativo y las aplicaciones, lo que también mejora la visibilidad en tiempo real, la seguridad de la red y la gestión del tiempo

Análisis de Amenazas

Todos los registros de eventos se almacenan en un servidor seguro y se analizan posteriormente en busca de amenazas según el tipo de malware y corrupción. Se verifican en función de políticas y regulaciones basadas en reglas, luego se identifican y categorizan según la naturaleza y el nivel de la amenaza de seguridad.

Eventos de Violación de EDR desde Endpoints

eScan Vision Core XDR está equipado con tecnologías avanzadas que recopilan la información de todos los endpoints que están categorizados como ataques de día cero conocidos y desconocidos. Los endpoints de eScan detectan automáticamente y envían los registros y eventos a la solución. Los ataques incluyen el robo de credenciales, JavaScript malicioso o VBScript, scripts potencialmente ofuscados, archivos ejecutables no confiables o sin firmar desde dispositivos extraíbles, creación de comandos WMI y PsExec, aplicaciones de Office y Adobe creando procesos secundarios, inyección de códigos, creación de contenido ejecutable y llamadas a la API Win32 desde macros. Los endpoints de eScan también evitan que el malware abuse de WMI para lograr persistencia en un dispositivo

Eventos de Violación de EDR desde Ransomware Avanzado

eScan Vision Core XDR recopila los registros y eventos de los endpoints protegiendo y bloqueando la ejecución de archivos ejecutables (.exe, .dll, o .src) y archivos de script (.ps, .vbs, .js) que se ejecutan automáticamente después de abrir un correo electrónico. Utiliza sus tecnologías heurísticas PBAE para monitorear y bloquear todas las aplicaciones que se sospecha son ransomware debido a su actividad o comportamiento. Junto con esto, también termina la sesión de red si algún sistema infectado intenta obtener acceso a un sistema protegido

Investigación Histórica - RCA

Con los eventos de Windows y el Análisis de Amenazas, se lleva a cabo un análisis profundo de la causa raíz (RCA) contra amenazas detectadas y potenciales para identificar su causa raíz. El RCA ayuda a identificar los puntos débiles en la red y tomar las medidas adecuadas para mitigar amenazas antes de que la amenaza tome el control de la red.

Marco MITRE ATT&CK

eScan ofrece el marco MITRE ATT&CK para analizar cada incidente de amenaza detectado por Vision Core XDR. Captura los detalles de las TTPs (tácticas, técnicas y procedimientos) involucrados en el incidente en una computadora servidor. El equipo de inteligencia de amenazas de la organización puede utilizar este marco para detectar comportamientos adversarios y mapear la actividad observada a técnicas específicas de ATT&CK.

Esta información sobre TTPs también se puede utilizar para compartir inteligencia sobre amenazas emergentes, ayudando a las organizaciones a mantenerse actualizadas con los métodos de ataque en constante evolución.

eScan
Vision Core XDR
(con defensa de inteligencia neuronal IA/ML)

eScan®
Enterprise Security

Características Clave - eScan Endpoints (Windows)

eBackup# y Restauración

eScan permite a los administradores realizar copias de seguridad de todos los archivos de forma manual o automática (según una programación) y almacenarlos en un formato cifrado y comprimido. También permite realizar copias de seguridad en un disco local, una unidad de red o en la nube (función adicional). eScan permite a los administradores importar/exportar los datos del servidor, que pueden restaurarse en caso de falla del sistema o desastre.

Monitoreo y Gestión Remota (RMM)*

El monitoreo y gestión remota (RMM) es un tipo de software de gestión de TI a distancia utilizado por Proveedores de Servicios de TI Administrados (MSP), que permite a los administradores rastrear problemas y monitorear activos de TI de forma remota. Ayuda a las organizaciones a obtener información sobre el rendimiento, la salud y el estado de sus endpoints. Es una función adicional.

Informe de Actividad de Sesión

La Consola de Administración de eScan monitorea y registra la actividad de sesión de las computadoras administradas. Mostrará un informe del inicio/apagado del endpoint, inicio/cierre de sesión y conexión/desconexión de sesiones remotas. Los administradores pueden utilizar este informe para rastrear las actividades de inicio y cierre de sesión de los usuarios, así como las sesiones remotas, en todas las computadoras administradas

Monitoreo de Actividad de Impresión

El módulo de Monitoreo de Actividad de Impresión en eScan monitorea y registra de manera eficiente las tareas de impresión realizadas por todos los endpoints administrados. También proporciona un informe detallado en formatos PDF, Excel o HTML de todas las tareas de impresión realizadas por los endpoints administrados a través de cualquier impresora conectada a cualquier computadora en la red o de manera local

Gestión de Parches* e Informes de Parches

eScan consulta la información del sistema operativo y proporciona automáticamente parches de seguridad críticos junto con actualizaciones. El servidor de eScan descarga los parches para diferentes versiones de Windows OS y los distribuye a los diversos endpoints. El Informe de Parches muestra la cantidad de parches de seguridad de Windows instalados y no instalados en las computadoras administradas. Esto ayudará a los administradores a identificar la cantidad de sistemas vulnerables en la red e instalar rápidamente los parches críticos. También es una función adicional.

Actualizaciones sin Conexión

eScan aborda la necesidad de actualizaciones sin conexión para redes aisladas al permitir que el administrador use una computadora conectada a Internet para predescargar todas las actualizaciones requeridas por las computadoras en la red aislada, de modo que luego pueda copiar los archivos de actualización a la red aislada.

eScan
Vision Core XDR
(con defensa de inteligencia neuronal IA/ML)

eScan®
Enterprise Security

Características Clave - eScan Endpoints (Windows)

Anti-Spam

eScan proporciona protección contra correos electrónicos no deseados con su poderosa tecnología Anti-Spam. Verifica el contenido de los correos electrónicos entrantes y salientes y pone en cuarentena los correos comerciales. Además, eScan utiliza motores antivirus duales con tecnología heurística para analizar en tiempo real todos los correos electrónicos en busca de virus, gusanos, troyanos, spyware, adware y contenido malicioso oculto.

Agente de Actualización

Los administradores pueden agregar computadoras como Agentes de Actualización. Como resultado, el tráfico entre el Servidor Corporativo de eScan y el cliente se reduce.
Las actualizaciones de firmas y las políticas se descargarán desde el servidor de eScan y se distribuirán a las demás computadoras administradas en el grupo a través del Agente de Actualización. Esto ahorra todo el ancho de banda y mejora el rendimiento

Control de Privacidad

El Control de Privacidad permite programar el borrado automático de la caché, ActiveX, cookies, complementos e historial. También ayuda a eliminar de forma permanente archivos y carpetas sin riesgo de que sean recuperados por aplicaciones de terceros, evitando así la explotación de datos

Política de Seguridad Avanzada

eScan ha incluido una Política de Seguridad Avanzada que alerta a los administradores sobre actividades maliciosas y ayuda a las organizaciones a identificar y detener brechas de seguridad en tiempo real de manera automática y eficiente, sin sobrecargar al equipo de seguridad con falsas alarmas o afectar las operaciones comerciales

Características clave - eScan Endpoints (Hybrid OS)

Control de dispositivos

eScan está equipado con la función avanzada de Control de Dispositivos que permite/bloquea el acceso a dispositivos USB en los endpoints de la red. El acceso a la cámara web, tarjetas SD, imágenes, Bluetooth y dispositivos compuestos está restringido en los endpoints con Windows. El acceso a memorias USB puede ser restringido en Windows, Mac y Linux. El acceso a CD-ROM puede ser restringido en Windows y Linux.

Escaneo programado

eScan le ofrece una opción para realizar escaneos programados, que se ejecutarán sin problemas en segundo plano sin interrumpir su entorno de trabajo actual. Realiza escaneos programados para archivos/carpetas seleccionados o para todo el sistema durante el período programado, proporcionando así la mejor protección contra amenazas cibernéticas.

eScan
Vision Core XDR
(con defensa de inteligencia neuronal IA/ML)

eScan®
Enterprise Security

Características Clave - eScan Endpoints (Windows)

Protección web avanzada

eScan está equipado con Protección Web Avanzada que protege contra el acceso a páginas peligrosas, de phishing y fraudulentas. Permite al administrador definir la lista de sitios a restringir o incluir en la lista blanca en los endpoints conectados a la red. Como resultado, cuando una URL apunta a un sitio web conocido por phishing o fraude, o a contenido malicioso como spyware o virus, la página web es bloqueada y se muestra una alerta. eScan también proporciona restricciones de acceso basadas en el tiempo en los endpoints con Windows.

Firewall mejorado

El Firewall Bidireccional de eScan filtra todas las solicitudes de red entrantes y salientes, lo que permite monitorear cada conexión entrante y saliente que se está estableciendo. Esto impide que los hackers se conecten al sistema y defiende la conexión de aplicaciones no deseadas a internet. Proporciona la capacidad de definir la configuración del firewall, así como definir el rango de IP, las aplicaciones permitidas, las direcciones MAC de confianza y las direcciones IP locales

Reverse Shell

La función Reverse Shell de eScan para endpoints basados en Linux restringe los ataques de reverse shell desde una máquina remota. De esta manera, se evita que los atacantes exploten una vulnerabilidad de ejecución remota de comandos mediante una sesión de reverse shell.

Monitoreo de Integridad de Archivos

El Monitoreo de Integridad de Archivos de eScan valida la integridad de los valores de archivos y carpetas entre el estado actual y el estado original del archivo para detectar posibles compromisos en endpoints basados en Linux.

Control de aplicaciones

El Control de Aplicaciones de eScan le ayuda a adelantarse a los ciberdelincuentes y mantiene su negocio seguro y productivo. Previene ataques de día cero y ATP bloqueando la ejecución de aplicaciones no autorizadas. Mediante la lista blanca, los administradores pueden prevenir ataques de malware desconocido permitiendo solo aplicaciones conocidas en la lista blanca.

* Esta función requiere una licencia adicional.

Esta función requiere una licencia adicional para permitir el uso del almacenamiento en la nube

eScan®

Enterprise Security

An ISO 27001 Certified Company

www.latam.escanav.com

MicroWorld Technologies Inc.
Tel.: (+1) 248 374 5020, 248 522 7960
Email: sales@escanav.com

Awards

Partnerships

Comprehensive Protection for

SOHO • BUSINESS • CORPORATE • ENTERPRISE