ManageEngine

Guía del educador para una gestión de TI más inteligente

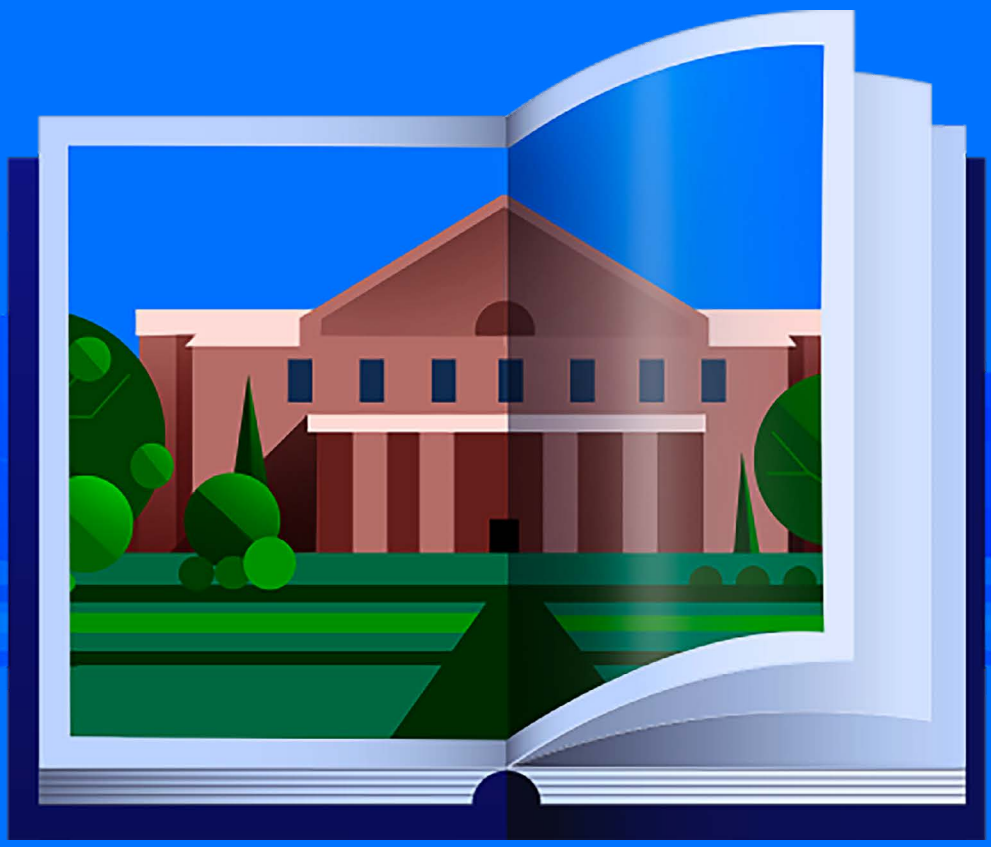


Tabla de contenido

Detrás de cada gran campus hay una fuerte columna vertebral de TI

Las instituciones educativas se enfrentan hoy a un complejo conjunto de desafíos de TI. La mayoría opera con presupuestos limitados, pequeños equipos de TI y expectativas crecientes de estudiantes, profesores y personal. Con más de miles de usuarios que dependen de sistemas digitales todos los días, incluso un simple problema de red, error de inicio de sesión o dispositivo lento puede interrumpir rápidamente los procesos de enseñanza y aprendizaje.

La seguridad es otra preocupación apremiante. Las escuelas y universidades almacenan información altamente sensible, como registros de estudiantes, preguntas y resultados de exámenes, datos de nómina e identificaciones personales. Sin controles de acceso, monitoreo y medidas de protección de datos adecuados, estos sistemas son vulnerables a las infracciones y el mal uso. El riesgo aumenta cuando los equipos de TI carecen de visibilidad o se ven obligados a administrar todo manualmente.

Al mismo tiempo, los requisitos de cumplimiento en torno a la privacidad de datos y la ciberseguridad se están volviendo más estrictos. Las instituciones educativas deben demostrar responsabilidad, garantizar la integridad de los datos y responder rápidamente a incidentes. Confiar en herramientas obsoletas o procesos fragmentados hace que esto sea casi imposible.

Estos puntos de dolor son reales y persistentes. Las sólidas herramientas de TI pueden ayudar a resolverlas mediante la automatización de tareas rutinarias, proporcionando información en tiempo real y mejorando el control en infraestructura, dispositivos y usuarios. Más que conveniencia, son cruciales para mantener operaciones fluidas, proteger los datos y crear un entorno confiable para que la educación prospere.

6 grandes obstáculos de TI para las instituciones educativas

#1
Operaciones fragmentadas y poca visibilidad

#2
Expansión de activos y gestión de TI manual

#3
Escritorios de ayuda tensos y recursos limitados

#4
Tiempo de inactividad de la infraestructura y fallos de aplicaciones

#5
Aumento de ciberataques y robo de datos

#6
Requisitos de cumplimiento complejos y en evolución

#1: Operaciones fragmentadas y poca visibilidad

Gestionar las operaciones cotidianas a través de funciones académicas, administrativas y de apoyo es un desafío importante. Las instituciones a menudo dependen de sistemas en silos que no hablan entre sí, lo que lleva a la duplicación de esfuerzos, retrasos en la toma de decisiones y una mala experiencia del usuario. Tareas como incorporar a nuevos estudiantes, administrar dispositivos en laboratorios o asignar licencias de software consumen mucho tiempo sin visibilidad centralizada. A medida que crecen los sistemas digitales, la falta de integración conduce a ineficiencias que presionan tanto a los equipos de TI como a la facultad.

#2: Expansión de activos y gestión de TI manual

La mayoría de los campus tienen miles de activos físicos y digitales: computadoras portátiles, escritorios, máquinas de laboratorio, proyectores, herramientas de software, aplicaciones en la nube y más. Sin un sistema unificado de gestión de activos, el seguimiento de estos recursos es extremadamente difícil. Los dispositivos no parches, el software permanece infrautilizado y el hardware a menudo no se contabiliza. Esto no solo desperdicia los presupuestos de TI, sino que también aumenta la superficie de riesgo de la institución.

#3: Escritorios de ayuda tensos y recursos limitados

Los escritorios de ayuda de TI en entornos educativos a menudo se ven abrumados por grandes volúmenes de solicitudes repetitivas, restablecimiento de contraseñas, problemas de acceso Wi-Fi, instalaciones de software y fallas del proyector. El personal limitado y los presupuestos ajustados significan tiempos de espera más largos y problemas no resueltos. La falta de integración entre el help desk y los sistemas de TI principales impide que los técnicos vean el contexto completo, ralentiza aún más la resolución y frustrar a los usuarios.

#4: Tiempo de inactividad de la infraestructura y fallos de aplicaciones

Los campus modernos prosperan en la conectividad. Ya sea que un estudiante inicie sesión desde casa, un profesor subiendo cursos o un administrador que apruebe ayuda financiera, todo depende de que los sistemas de TI trabajen en sincronía. Cuando se produce el tiempo de inactividad, ya sea debido a fallas de infraestructura, interrupciones de la red o el mal funcionamiento de las aplicaciones, el impacto es inmediato y generalizado. El aprendizaje se detiene, la comunicación se detiene y los servicios esenciales se detienen. En entornos de aprendizaje híbridos, donde el acceso digital es tan importante como la presencia física, incluso cortes cortos pueden causar interrupciones duraderas. Una columna vertebral de TI confiable y bien monitoreada garantiza la continuidad y mantiene funcionando el ecosistema del campus, sin importar dónde se lleven a cabo la enseñanza y el aprendizaje.

#5: Aumento de ciberataques y robo de datos

Las instituciones educativas tienen una gran cantidad de información sensible, registros de estudiantes y ex alumnos, transcripciones académicas, detalles básicos de salud, datos de nómina de empleados e investigación patentada. Sin embargo, a menudo operan con presupuestos limitados de ciberseguridad, lo que los convierte en un objetivo atractivo para los atacantes. Los actores de amenazas utilizan phishing, malware y tácticas de ingeniería social para robar datos, extorsionar fondos o simplemente interrumpir sistemas. El daño a la reputación y financiero de una infracción puede ser grave, con consecuencias duraderas.

#6: Requisitos de cumplimiento complejos y en evolución

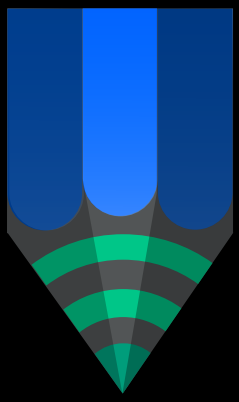
Con los datos que fluyen de plataformas de inscripción, servicios en la nube y herramientas de terceros, mantener el cumplimiento de regulaciones como la Ley de Derechos Educativos Familiares y Privacidad (FERPA), el GDPR o las leyes nacionales de protección de datos se vuelve cada vez más difícil. Las instituciones deben asegurarse de que los datos de los estudiantes se recopilan, procesan y almacenan de manera que cumplan con los estándares legales y éticos. El incumplimiento puede conducir a sanciones legales, pérdida de fondos y pérdida de confianza pública.

Cómo las soluciones avanzadas de TI pueden ayudarle a superar estos obstáculos

Con la creciente demanda digital y los recursos de TI limitados, las instituciones educativas necesitan formas más inteligentes y escalables de administrar operaciones, infraestructura y seguridad. Aquí es donde las soluciones de gestión de TI impulsadas por IA pueden ayudar como sistemas inteligentes que brindan visibilidad, velocidad y control en todo el entorno de TI del campus.

Así es como las herramientas de TI sólidas abordan directamente los desafíos principales que enfrentan las instituciones educativas:

Simplifique la gestión de dispositivos y redes



Administrar miles de dispositivos en las aulas, laboratorios, bibliotecas y oficinas administrativas puede volverse caótico fácilmente. Con herramientas centralizadas de gestión de TI, las instituciones pueden monitorear la salud del dispositivo, los patrones de uso y el cumplimiento del software en tiempo real. Por ejemplo, si se detecta software obsoleto en un laboratorio justo antes de los exámenes, TI puede empujar actualizaciones de forma remota instantáneamente, evitando interrupciones de último minuto que podrán afectar la capacidad de los estudiantes para completar los cursos.

Cómo IT lo ayuda:

- Monitoree la salud, disponibilidad y uso de todos los dispositivos conectados al campus desde una sola consola.
- Detectar software no conforme o anticuado y empuje actualizaciones remotamente para minimizar la intervención manual.
- Gestionar licencias de software y realizar un seguimiento de las instalaciones para garantizar el cumplimiento de las políticas institucionales.
- Identifique dispositivos subutilizados o utilizados en exceso para apoyar la reasignación de recursos y reducir gastos innecesarios.
- Reciba alertas sobre fallos de hardware de rendimiento para tomar medidas correctivas rápidas y evitar el tiempo de inactividad.

Automatice las operaciones de Help Desk

Los equipos de apoyo de la institución a menudo están inundados de grandes volúmenes de problemas repetitivos. Las herramientas de TI modernas permiten a los escritorios de ayuda con el enrutamiento inteligente de tickets, portales de autoservicio y acceso a soluciones pasadas. En la practica, esto significa que un estudiante que lucha por conectarse a la VPN del campus puede escribir su problema en un portal, ser guiado a través de una resolución instantáneamente y evitar esperar en una cola, ahorrando tiempo valioso tanto al estudiante como al equipo de soporte.

Las herramientas avanzadas de TI también simplifican los procesos cotidianos mediante la automatización de tareas que una vez consumieron horas de esfuerzo manual. Cuando un nuevo estudiante se inscribe, el sistema puede generar automáticamente sus credenciales de inicio de sesión, asignar acceso a Wi-Fi, configurar permisos de dispositivo y notificarle instrucciones de incorporación. Esto reduce los retrasos en la incorporación, minimiza los errores y garantiza que los estudiantes puedan acceder a los recursos de aprendizaje desde el primer día.

Cómo ayuda IT:

- Asigne automáticamente tickets al técnico adecuado en función del tipo de problema, prioridad o departamento.
- Proporcionar portales de autoservicio y bases de conocimiento para que los usuarios puedan resolver problemas comunes por su cuenta.

- Mantenga informados a los usuarios con actualizaciones en tiempo real sobre el estado del ticket y los plazos de resolución.
- Reduzca el esfuerzo manual a través de la integración con los servicios de gestión de identidades y directorio durante la incorporación.
- Utilice el análisis de causa raíz impulsado por IA para identificar problemas recurrentes, como cortes de VPN, errores de sistemas de gestión de aprendizaje e(LMS) o fallos de Wi-Fi, y abordarlos de manera efectiva, evitando una futura recurrencia.
- Empoderar a los equipos de soporte con análisis avanzados de autoservicio e inteligencia de decisiones para identificar brechas en los procesos, el rendimiento de referencia y tomar medidas correctivas, sin depender de la intervención técnica.

Monitoree su infraestructura y red en tiempo real

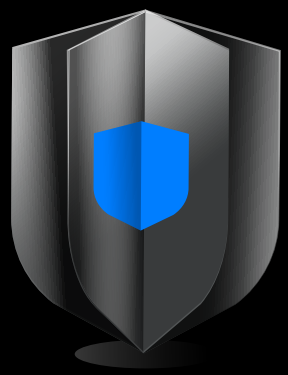
Los cortes no planificados pueden detener el acceso a sistemas de gestión de aprendizaje, portales o pasarelas de pago. Para evitar tales interrupciones, las herramientas avanzadas de monitoreo proporcionan visibilidad en tiempo real del tráfico de red, el rendimiento del servidor y el estado general del sistema. Por ejemplo, antes de un examen importante, TI recibe alertas sobre el alto uso del servidor y escala los recursos con anticipación, asegurando que la plataforma se mantenga estable cuando más se necesita. Del mismo modo, en configuraciones de aprendizaje híbrido o plataformas de tecnología, el monitoreo en tiempo real garantiza que las clases en vivo, evaluaciones en línea y seminarios web interactivos se ejecuten sin interrupciones, manteniendo una experiencia de aprendizaje fluida tanto para estudiantes remotos como en el campus.

Cómo lo ayuda TI:

- Monitoree continuamente el rendimiento de la red para detectar desaceleraciones, congestión o problemas de conectividad.
- Analizar los patrones de tráfico de red para identificar el acaparamiento de ancho de banda, los aumentos de tráfico recurrentes, los picos sospechosos o la actividad DDoS potencial.
- Realice un seguimiento de la disponibilidad de aplicaciones, los tiempos de respuesta, las tasas de error y las dependencias para mantener un servicio consistente.

- Utilice mapas de organización para visualizar las relaciones entre los componentes de infraestructura y las aplicaciones, ayudando a los equipos a identificar las causas raíz y resolver problemas más rápidamente.
- Simule los viajes de los usuarios para garantizar un acceso sin problemas a las aulas virtuales, portales y evaluaciones en línea.
- Establezca alertas basadas en umbrales y anomalías para marcar el comportamiento inusual de CPU, memoria o tráfico.
- Aproveche las previsiones multivariante para predecir aumentos de demanda durante la actividad pico, como inscripciones de estudiantes, horarios de exámenes o sesiones de clase concurrentes, para que los recursos se puedan escalar de manera proactiva.

Fortalecer la seguridad y los controles de acceso



Con datos confidenciales como registros académicos, documentos de investigación e información de nómina en juego, las instituciones educativas deben gestionar estrechamente quien tiene acceso a qué. Los sistemas avanzados de control de acceso permiten permisos basados en roles y monitorio continuo de inicio de sesión. Imagine un escenario en el que un miembro temporal del personal intenta accidentalmente acceder a los datos de nómina; el sistema automáticamente marca y bloquea el intento, manteniendo la privacidad de los datos sin intervención humana.

Cómo lo ayuda IT:

- Definir y hacer cumplir políticas de acceso basadas en roles entre usuarios, departamentos y sistemas.
- Monitoree la actividad de inicio de sesión en tiempo real para detectar comportamientos inusuales o intentos de acceso sospechosos.
- Bloquee el acceso no autorizado y desencadena alertas para una investigación inmediata.
- Aproveche las herramientas de administración de endpoints para proteger los dispositivos de profesores y estudiantes con parches oportunos y aplicación de políticas.
- Mantenga registros de auditora de todos los cambios de acceso y permisos para admitir revisiones de cumplimiento y seguridad.
- Detectar comportamientos anormales y marque amenazas potenciales para garantizar una respuesta más rápida a las amenazas y la mitigación de riesgos.

Garantizar la disponibilidad 24/7 de la infraestructura de TI del campus

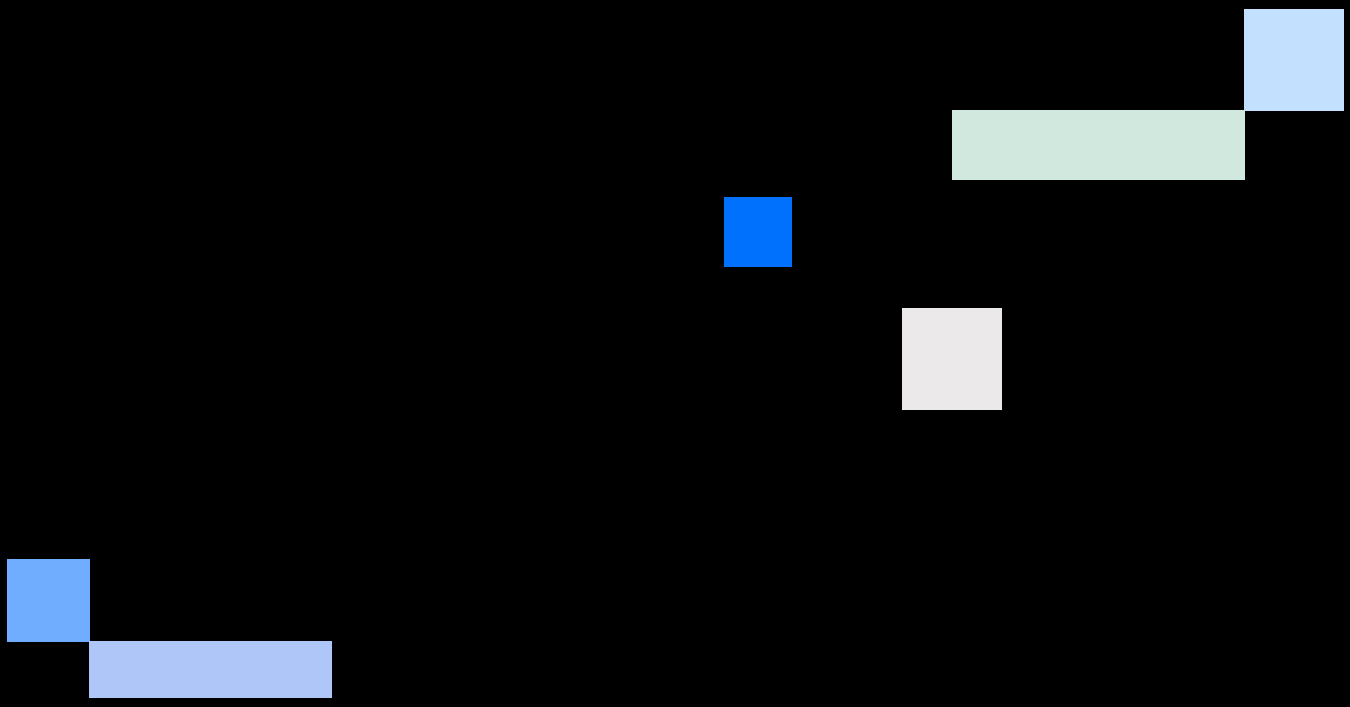
Los sistemas de TI del campus deben funcionar de manera confiable en todo momento, especialmente durante periodos de inscripción, clases virtuales, presentaciones de tareas y exámenes en linea. Para manejar los picos de tráfico y mantener el tiempo de actividad, las instituciones pueden equilibrar la carga utilizando servidores internos o basados en la nube.

Al analizar los datos históricos de rendimiento de redes, servidores y aplicaciones, los equipos de TI pueden detectar signos tempranos de problemas y abordar las causas raíz antes de que afecten a los usuarios. interrupciones. El mantenimiento de rutina se puede programar para minimizar las sobreutilización, los presupuestos de TI se pueden optimizar de manera efectiva.

Cómo ayuda IT:

- Asegure una conectividad estable de red identificando y resolviendo problemas con routers, puntos de acceso Wi-Fi, switches y pilas de switches.
- Monitoree la disponibilidad y el rendimiento de servidores y servidores de aplicaciones para evitar interrupciones para los estudiantes y el personal.

- Mantenga el uso del almacenamiento bajo control estableciendo umbrales y recibiendo alertas antes de quedarse sin espacio.
- Mantener un acceso consistente a las aplicaciones web mediante el seguimiento del rendimiento de los servidores web.
- Utilice datos históricos para identificar patrones de uso y predecir necesidades futuras de infraestructura.
- Manténgase actualizado con las alertas de pronóstico que le ayudan a monitorear la utilización de recursos de sus dispositivos de red al predecir aproximadamente cuánto tiempo tardará en agotar cada uno de sus recursos.



Agilice el cumplimiento y la preparación para la auditoría

Cumplir con las regulaciones de protección de datos requiere una supervisión constante. Las herramientas avanzadas de TI ayudan generando informes automatizados, registrando la actividad del usuario y destacando acciones que no cumplen. Por ejemplo, durante una revisión de cumplimiento, el equipo de TI de la institución puede producir instantáneamente un informe que muestre todo el acceso a la información personal identificable (PII) del estudiante durante los últimos 90 días sin necesidad de extraer datos manuales y manipular.

Cómo lo ayuda IT:

- Haga un seguimiento automático y registre el acceso del usuario a datos confidenciales, incluyendo PII y registros académicos.
- Generar informes listos para auditorías para revisiones internas o inspecciones externas con el mínimo esfuerzo.
- Reciba alertas por infracciones de políticas, accesos no autorizados o cambios de configuración.
- Mantener un rastro detallado de actividades para apoyar las investigaciones y demostrar el cumplimiento de las regulaciones del sector educativo.

Aplicando ManageEngine: soluciones prácticas para las necesidades de TI del campus

Caso de uso 1:

Automatización de las operaciones de help desk y ticketing

Imagina que es el comienzo de un nuevo semestre. Los estudiantes están iniciando sesión en sus portales; algunos han olvidado sus contraseñas. Los profesores están preparando material del curso, algunos necesitan ayuda con las herramientas de LMS. El personal está tratando de conectarse al Wi-Fi del campus, mientras que otros están aumentando solicitudes de actualizaciones de software o accediendo a dispositivos emitidos por el instituto. Incluso la biblioteca se está inundando con consultas de servicio. Desde restablecimiento de contraseñas hasta problemas de Wi-Fi y fallos del dispositivo, el equipo de soporte de TI está lleno de boletos de todos los rincones del campus. Sin un sistema adecuado en su lugar, las cosas pueden girar rápidamente en espiral. Las solicitudes se pierden, los seguimiento caen y la satisfacción del usuario recibe un golpe.

Para reducir la carga sobre el personal de TI y proporcionar una experiencia de campus más fluida, problemas comunes como el restablecimiento de contraseñas o la orientación de software pueden manejarse a través de un portal de autoservicio respaldado por una base de conocimientos bien mantenida.

Para todo lo que los usuarios necesitan resolver problemas menores por su cuenta, piense en preguntas frecuentes, guías prácticas y videos. Estos liberan al equipo de apoyo para centrarse en cuestiones más estratégicas o urgentes, como aquellos que realmente requieren su experiencia, asegurando al mismo tiempo que todos en el campus todavía reciban la ayuda que necesitan, rápidamente. Porque cuando la tecnología funciona sin problemas, el aprendizaje y la enseñanza también pueden hacerlo.

Cómo los productos de ManageEngine benefician a su institución

Producto de ManageEngine	Cómo ayuda
ServiceDesk Plus	Automatiza funciones rutinarias y repetitivas con flujos de trabajo personalizados para satisfacer las solicitudes de servicio, administrar cambios y lanzar lanzamientos sin problemas. Permite a los técnicos cerrar un problema y activar un cierre automático de todos los incidentes vinculados. Crea un portal de autoservicio unificado en todo el campus que ayuda a los usuarios finales a acceder a diferentes departamentos para solicitar servicios o registrar quejas. Construye una amplia base de conocimientos que es accesible desde el portal integrado de autoservicio. Anfitrión de guías del campus, soluciones a problemas comunes de TI y artículos de guía. Libera a los técnicos de realizar tareas mundanas y permite a los usuarios finales recibir ayuda para crear tickets y encontrar soluciones más rápido con Ask Zia, el agente de soporte virtual conversacional impulsado por GenAI.
Endpoint Central	Preaprueba la solicitud requerida en función de calificaciones, optativas y clases, quitando la carga del departamento de TI y reduciendo el número de tickets.
SupportCenter Plus	Gestiona tickets en varias escuelas y colegios desde una única plataforma de atención al cliente. Lanza portales de autoservicio personalizados y configura flujos de trabajo únicos para cada organización que administre.

Analytics Plus	Identifica tendencias recurrentes en los tickets, como restablecimientos de contraseña, problemas de Pronóstico de volúmenes de tickets durante los ciclos académicos, como nuevas inscripciones o presentaciones de exámenes para permitir la dotación de personal proactiva y la asignación de recursos. Proporciona paneles de SLA para rastrear los tiempos de resolución para reducir la frustración de estudiantes y profesores durante períodos de alta demanda. Aprovecha los conocimientos impulsados por IA para interpretar los picos, por ejemplo, problemas repentinos de Wi-Fi en un bloque de campus, y recibe recomendaciones personalizadas para resolver los cuellos de botella antes de que necesiten ser escalados. Ofrece paneles unificados que miden la eficiencia de la mesa de ayuda, la satisfacción de los estudiantes y los resultados de prestación de servicios en todos los departamentos.
AppCreator	Crea aplicaciones de autoservicio personalizadas adaptadas a las necesidades del campus, como una aplicación nativa móvil para consultas de bibliotecas, solicitudes de TI relacionadas con exámenes o formularios específicos de departamento. Estas aplicaciones pueden integrarse con ServiceDesk Plus, asegurando que los tickets de soporte fluyan sin problemas en la cola del help central.

Caso de uso 2:

Fortalecimiento de la seguridad de endpoint en toda la institución

Supongamos que es la semana de presentación de proyectos. Los estudiantes están subiendo informes finales al portal del campus, la facultad está accediendo a los sistemas de calificación y los equipos de administración están procesando la nómina. Miles de endpoints como computadoras portátiles, computadoras de escritorio, sistemas de laboratorio y dispositivos móviles están activos a través de las redes del campus. Algunos dispositivos son personales, otros son emitidos por instituciones. Simultáneamente, los datos confidenciales como resultados de exámenes, números de identificación, registros financieros y certificados de salud fluyen a través del sistema.

Ahora imagina que el USB infectado de un estudiante desencadena un brote de malware. O un clic en un enlace de phishing en un correo electrónico del personal conduce al robo de credenciales. O peor aún, una computadora portátil robada termina exponiendo datos confidenciales de investigación. Todo lo que se necesita es un eslabón débil.

Con los estudiantes y el personal que se conectan constantemente desde diferentes ubicaciones y dispositivos, la seguridad tradicional basada en el perímetro simplemente ya no lo corta. Lo que los campus necesitan es una protección en capas que siga al usuario, desde donde inicie sesión, sea cual sea el dispositivo que utilicen.

Para minimizar estos riesgos, es crucial implementar parches continuos, hacer cumplir políticas de acceso estrictas, monitorear el comportamiento del usuario y detectar anomalías antes de que aumenten. Piense en alertas en tiempo real para iniciar sesión sospechosos, restricciones en USB no confiables, limpieza remota de dispositivos perdidos y respuesta automatizada a amenazas para endpoints comprometidos.

IŦsuruy vxuj{izuy SgtgmkKtmotk hktklοiogt g y{ otyzοz{ ioŦt

Producto de ManageEngine	IŦsug {jg
Log360	Vxuvuxiouτg |oyohoro jgj iu s vrkzg j k rgy gizο|ojgjky j k kt j vuοtzy {y{gxouy kt zu j u kr igs v{y4 Gr xk i uvorgx xkmoyzxuy j k kt j vuοtzy2 G izο|k Joxk izux 2 yoyzk s gy j k g{zk tzοig i oşt nkxxg s οk tzgy j k ykm{xο j g j 2 Rum9<6 j kzk i zg g s k tg¡gy iu s u οtlk i iou tky j k s gr } gxk2 {yu tu g{zuxο¡g j u j k [YH k οtzk tzuy j k xuhu j k ixk j k t iogrky4 Gvxu|k i ng y{ s uzux j k g tŏroyoy j k iu s vuxzg s οk tzu j k {y{gxou k tzο j g j . [KHG/ w{k kyzghrk i k rg g izο|οj g j tux s gr vgxg i g j g {y{gxou j οyvuyozο|u2 mk t kxg t j u grkxzgy ο tyzg tzŏ t kgy i {gt j u yk vxu j { i k t g tu s gŚgy iu s u ο t ο i ouy j k ykyoşt οt {y{grky2 ky i grg j gy j k vxο|orkmouy u g i i kyu s gyο|u g gxin ο|uy4 [zoro¡g t j u y{y xkmrgy j k iuxxkrg i oşt kt zok s vu xkgr grkxzgy vxk j klοt ο j gy2 ruy kw{οvuy j k ZΟ v{k j k t xkyvu t j kx xŏvο j g s k t zk g ο t zk t zuy j k vnoyn ο t m2 g s k tg¡gy ο tzkx tgy u j οyvuyοzο|uy iu s vxu s kzο j uy4 G { j g g ng i kx i { s vrox kyzxο izuy iu t zxurky j k g i i kyu g{ j οzg t j u k|k tzuy j k ο t ο i ou j k ykyoşt2 ig s houy j k vxο|orkmouy |ourg i ou t ky j k vurŚzο i gy4 Ruy xοkymuy j k j οyvuyοzο|uy vkx j ο j uy u xuhg j uy v{k j k t s οzomgxyk g zxg|Ŗy j k xkmoyzxuy j kzgrrg j uy Ir{ρuy j k zxghgρu g{zu s gzο¡g j uy j k xkyv{kyzg2 gykm{xg t j u w{k ruy j gzuy g i g j Ŗ s ο i uy j k ο t |kyzomg i oş t yk t yοhrk vkx s g t k¡ i g t vxuzkmο j uy4

Endpoint Central	Refuerza las defensas de endpoint y asegúrate de que todos los sistemas se mantengan actualizados con Endpoint Central. Esta plataforma unificada de gestión y seguridad de endpoints permite a los equipos de TI automatizar el sistema operativo y los parches de terceros en todos los dispositivos, ya sean dispositivos personales de propiedad de una institución o registrados. Un solo estudiante que conecte un dispositivo o descargue malware durante un examen puede comprometer toda la red de TI. Endpoint Central bloquea estas amenazas instantáneamente con control de dispositivos, seguridad del navegador, control de aplicaciones, antivirus de próxima generación y protección contra malware, todo gestionado desde una consola para mantener segura la infraestructura. Si un enlace de phishing infecta un dispositivo, Endpoint Central lo detecta y pone en cuarentena rápidamente, alerta a los administradores y luego elimina el malware. También ejecuta análisis forense para prevenir ataques repetidos, asegurando una protección continua.

Patch Manager Plus	Automatiza parches y reduce las vulnerabilidades de endpoints. Esta solución de administración de parches ayuda a los equipos de TI a mantener todos los puntos finales de Windows, macOS y Linux actualizados con las últimas correcciones de seguridad. Admite parches para más de 1.100 aplicaciones de terceros comúnmente utilizadas por los estudiantes y el personal, como navegadores, herramientas de productividad y software de desarrollo. Durante tiempos críticos como la semana de presentación de proyectos, Patch Manager Plus garantiza que los endpoints no estén expuestos a vulnerabilidades conocidas que el malware o el ransomware puedan explotar. Con características como implementación automática, pruebas de parches y programación flexible, las instituciones pueden mantener un entorno seguro y compatible sin interrumpir los flujos de trabajo académicos.

Vulnerability Manager Plus	Detecta vulnerabilidades y configuraciones erróneas en dispositivos registrados en instituciones. Escanea todos los sistemas operativos, servidores web y dispositivos de red para detectar debilidades explotables, software no autorizado, configuraciones erróneas del firewall y certificados SSL vencidos. Prioriza las amenazas mediante análisis basados en atacantes y los puntos de referencia de cumplimiento CIS, automatiza la remediación a través de la implementación de parches, el despliegue de configuración segura o la eliminación de aplicaciones inseguras. Con informes centralizados y visibilidad en tiempo real, esta solución permite a los equipos de TI sellar las brechas de seguridad de manera proactiva, reduciendo la probabilidad de brotes de malware y robos de credenciales.
AD360	Autentica a los usuarios de forma segura y aplica controles de acceso contextuales. Esta solución de administración de contraseñas de autoservicio y autenticación multifactor (MFA) ayuda a proteger los inicios de sesión para las aplicaciones de instituir. AD360 admite MFA adaptativo basado en el dispositivo, la ubicación y el tiempo, lo que garantiza que incluso si se roban credenciales, se puede bloquear el acceso no autorizado. restablecer contraseñas por su cuenta.También reduce la carga de help desk durante las semanas.

Access Manager Plus	Protege contra el compromiso de credenciales y hace cumplir el acceso de confianza cero. Esta solución ayuda a asegurar los inicios de sesión remotos y acceso privilegiado a través de la red del campus. Access Manager Plus permite a los equipos de TI administrar, supervisar y auditar sesiones privilegiadas, ya sea un administrador del sistema que se conecta a servidores de nómina o un investigador accediendo a conjuntos de datos confidenciales. Su grabación de sesiones y acceso justo a tiempo reducen el riesgo de abuso o exposición a datos de dispositivos robados.

Caso de uso 3:

Monitoreo de la salud de la red y reducción del tiempo de inactividad

Hay varios tipos de interrupciones que descarrilan el ritmo de las operaciones académicas diarias. Por ejemplo, una interrupción de la red de cinco minutos puede afectar significativamente el progreso en un examen en línea. La demora en el LMS al igual que los estudiantes están tratando de enviar tareas es frustrante tanto para los estudiantes como para los educadores. Un aumento repentino en la carga del servidor durante las horas pico de registro puede detener las operaciones vitales.

Muchos equipos de TI se encuentran atrapados reaccionando a los problemas después de que ya han afectado a cientos de usuarios. Sin visibilidad en tiempo real, identificar la causa del tiempo de inactividad se convierte en un juego de adivinación, y se pierde tiempo valioso. Aquí es donde el monitoreo full stack marca la diferencia.

Mediante el uso de una plataforma unificada de monitoreo del rendimiento, las instituciones educativas pueden obtener una visión en vivo de redes, servidores y aplicaciones. Pueden rastrear el uso del ancho de banda, detectar anomalías, recibir alertas instantáneas y identificar la causa raíz, antes de que los tickets comiencen a inundarse.

Cómo los productos ManageEngine benefician a su institución

Producto de ManageEngine	Cómo ayuda
OpManager Plus (on-premises) / Site24x7 (cloud)	Garantiza operaciones académicas ininterrumpidas supervisando continuamente el estado de salud de redes, servidores y aplicaciones desde una única plataforma unificada. Detecta proactivamente los problemas antes de que afecten a los estudiantes, profesores o personal, y minimiza el tiempo de inactividad durante momentos críticos como exámenes, presentaciones o registros. Monitorea el uso del ancho de banda, los patrones de tráfico y el rendimiento del dispositivo en toda la red del campus para detectar anomalías temprano. Genera alertas en tiempo real sobre el momento en que ocurren latencia, pérdida de paquetes o interrupciones, lo que permite una respuesta a incidentes más rápida. Indica la causa raíz del tiempo de inactividad en aplicaciones, servidores o dispositivos de red a través de correlación y diagnósticos impulsados por IA. Permite a los equipos de TI para pasar de la solución reactiva de problemas a la prevención proactiva, reduce el tiempo de inactividad y ofrece experiencias de aprendizaje digital ininterrumpidas.

Endpoint Central	Asegura que el equipo de TI reciba métricas en vivo de todos los endpoints de los estudiantes, máquinas de profesores y servidores. Las alertas automatizadas marcan instantáneamente picos anormales en el uso del ancho de banda o el consumo de recursos antes de que afecten el examen. Los análisis de Endpoint Central pueden identificar rápidamente si la desaceleración se debe a una aplicación específica, un servidor sobrecargado o nodo Wi-Fi. Esto permite al departamento de TI iniciar scripts automatizados desde la consola, como reiniciar servicios o reasignar recursos, resolviendo el problema antes de que las quejas de los estudiantes aumenten.
NetFlow Analyzer	Analiza el uso del ancho de banda e identifica patrones de tráfico de red. Esta herramienta proporciona visibilidad detallada de qué usuarios, aplicaciones o sitios web consumen la mayor cantidad de ancho de banda en el campus. Al detectar picos repentinos de tráfico o flujo de datos inusual, los equipos de TI pueden evitar desaceleraciones durante períodos cruciales como evaluaciones en línea o registros de cursos. Esta solución ayuda a establecer políticas de ancho de banda y optimizar el rendimiento de la red, asegurando que las plataformas académicas permanezcan en línea, rápidas y accesibles.

Applications Manager	Diagnostica problemas de aplicación hasta el nivel de código. Esta solución supervisa el rendimiento y la disponibilidad de aplicaciones críticas, como un LMS, portales de estudiantes y herramientas ERP del campus. Applications Manager ayuda a detectar consultas lentas de bases de datos, fugas de memoria o errores de aplicación que de otro modo podrían pasar desapercibidos hasta que los usuarios comiencen a subir tickets. Al proporcionar una visibilidad profunda del stack de aplicaciones, permite a los equipos de TI para solucionar problemas de rendimiento antes de que afecten a estudiantes o profesores.

Analytics Plus	Consolida los datos de monitoreo de servidores, aplicaciones, redes y sistemas Wi-Fi en paneles unificados que convierten los datos brutos en información estratégica y proporciona visibilidad completa en tiempo real en toda la infraestructura del campus. Detecta anomalías como picos de ancho de banda, ralentizaciones de LMS o sobrecargas de servidores utilizando modelos ML sin código y activa alertas solo cuando se rompen los umbrales. Correlaciona eventos entre herramientas para identificar problemas subyacentes utilizando análisis de causa raíz automatizado impulsado por IA que permite a los equipos de TI resolver problemas antes de que resulten en tiempos de inactividad. Aprovecha el análisis de cluster para agrupar eventos similares, como errores recurrentes de LMS, cortes de VPN o patrones de inicio de sesión de estudiantes. Esto permite a los equipos de TI identificar patrones, priorizar problemas de alto impacto y asignar recursos de manera eficiente. Utiliza análisis predictivo para anticipar los picos en el uso de redes o aplicaciones durante exámenes, registro de cursos o eventos en línea, lo que permite la dotación proactiva y el mantenimiento preventivo.

AppCreator	Sirve como complemento a las herramientas de monitoreo al funcionar como front end profundamente personalizable para los equipos de TI de las instituciones educativas. Usando la plataforma, los administradores de TI pueden crear paneles personalizados que consolidan métricas de herramientas de monitoreo de redes, servidores y aplicaciones a través de API. Los flujos de trabajo automatizados e integrados se pueden utilizar para registrar alertas como tickets, escalar tickets en función de la gravedad y los SLA, y notificar a las partes interesadas instantáneamente. Los datos crudos de las herramientas de monitoreo pueden transformarse en insights accionables que impulsan flujos de trabajo de respuesta orquestados. Esto reduce el impacto del tiempo de inactividad en el personal y los estudiantes.

Caso de uso 4:

Mantener seguros los datos personales y la información de investigación

Una institución educativa que ofrece una amplia gama de cursos y oportunidades de investigación quiere asegurar la información personal sensible de sus estudiantes, profesores y personal y garantizar que sus valiosos datos de investigación no se vean comprometidos. La institución debe descubrir los datos sensibles del sistema e implementar medidas de seguridad más estrictas para protegerlos.

Con los estudiantes que traen sus dispositivos personales con fines de aprendizaje, la superficie de ataque aumenta exponencialmente. Se deben implementar políticas y procedimientos para gestionar los riesgos de seguridad asociados con los dispositivos personales, especialmente cuando se accede a datos desde la red del campus. Los datos de los estudiantes a menudo se comparten con varios proveedores externos para otorgar acceso a plataformas de aprendizaje, software especializado y servicios administrativos. Las instituciones deben garantizar que estos proveedores cumplan con los mandatos regulatorios pertinentes para minimizar los riesgos.

Cómo los productos de ManageEngine benefician a su institución

Producto de ManageEngine	Cómo ayuda
Data Security Plus	Descubre datos confidenciales en sus archivos y los clasifica en función de vulnerabilidades. Monitorea continuamente el acceso y las modificaciones realizadas a estos archivos, y automatiza las respuestas inmediatas a ataques de ransomware, intentos de exfiltración de datos, anomalías de transferencia de archivos y más.
Log360	Detecta cualquier IP, URL o dominio en la lista negra que intente entrometerse en la red del campus. Eleva alertas cuando se detecta una IP sospechosa en sus registros de red, basándose en feed de amenazas actualizadas dinámicamente. Monitorea cambios en privilegios de usuario para identificar posibles ataques internos basados en desviaciones en patrones establecidos. Alerta a sus administradores de TI sobre anomalías de identidad y patrones de ataque con UEBA en tiempo real. Mitiga el riesgo de ransomware con alertas oportunas cuando ocurren cambios críticos en su red, como nuevas instalaciones de servicio, modificaciones de claves de registro, creaciones de archivos no autorizadas o creaciones de procesos maliciosos. Activa flujos de trabajo de remediación para evitar la propagación. Monitorea la base de datos de estudiantes para identificar posibles violaciones de datos. ransomware. Proporciona informes listos para usar información completa sobre las actividades de los usuarios, cambios de privilegios, cambios de configuración y mucho más.

ADAudit Plus	Encuentra acciones maliciosas de archivos instantáneamente con análisis de comportamiento del usuario (UBA), genera notificaciones instantáneas y permite una rápida remediación de amenazas. Audita y rastrea a los usuarios añadidos a grupos de seguridad de alto privilegios y reduce proactivamente el riesgo de que actores maliciosos obtengan acceso a los datos de sus estudiantes.
Endpoint Central	Asegura datos sensibles de estudiantes, profesores e investigación mediante el descubrimiento y clasificación de información confidencial. Fortalece políticas granulares de protección de datos en dispositivos personales e institucionales. Monitorea las actividades de datos de riesgo en tiempo real. Garantiza el cumplimiento de los estándares regulatorios, todos gestionados centralmente para reducir los riesgos de violación de datos y protege información valiosa con la ayuda del módulo de prevención de fugas de datos de Endpoint Central. Este módulo gestiona los riesgos de seguridad asociados con dispositivos personales a través de la administración de dispositivos móviles, permitiendo políticas BYOD que separan datos personales e institucionales, hace cumplir las normas y controlan el acceso a la red del campus de manera segura. Detecta y responde a amenazas avanzadas como ransomware y malware dirigido que intentan moverse lateralmente a través de las redes del campus. Fortalece las políticas de cifrado para garantizar que los datos permanezcan seguros, incluso si los dispositivos se pierden o son robados.

DataSecurity Plus	Descubre datos confidenciales y aplica políticas estrictas, incluido el control de dispositivos, para proteger los datos en dispositivos personales y garantizar el cumplimiento de las regulaciones educativas como FERPA. Con los datos de los estudiantes compartidos con proveedores externos, el módulo DLP Plus de DataSecurity Plus restringe las transferencias de datos no autorizadas y supervisa el cumplimiento de los proveedores. Proporciona alertas e informes en tiempo real para evitar fugas de datos rápidamente y proteger la integridad de los datos institucionales.
Firewall Analyzer	Monitorea sus políticas de firewall en busca de anomalías y administra los controles de firewall para fortalecer la seguridad de la red de TI. Asegura que solo los administradores de firewall autorizados puedan implementar cambios de política.

Caso de uso 5:

Agilización de la experiencia del estudiante

Una institución educativa quiere optimizar la experiencia que proporciona a sus alumnos. Los estudiantes deben tener acceso a un portal en línea fácil de usar para presentar sus solicitudes con documentos relevantes. La información sensible en la aplicación debe protegerse a través de procesos de autenticación. El portal en línea cuenta con chatbots integrados para ayudar a los estudiantes con cualquier consulta en cualquier momento del día.

Nuevos lotes de estudiantes se inscriben en una institución educativa cada año, y los estudiantes también se gradúan y se van. Los estudiantes incorporados deben tener acceso a los recursos relevantes del curso y otros servicios académicos basados en sus identidades digitales, que deben garantizarse con MFA.

Las instituciones educativas deben apoyar a los estudiantes y sus variadas necesidades de servicios anticipando las solicitudes de servicio estudiantil y automatizando los flujos de trabajo digitales. Los estudiantes deben ser capaces de resolver los problemas relacionados con contraseñas por su cuenta y reducir sus dependencias de los administradores de TI.

Cómo los productos de ManageEngine benefician a su institución

Producto de ManageEngine	Cómo ayuda
AD360	Automatiza la creación de cuentas en un solo paso para nuevos estudiantes en Active Directory, Microsoft 365, Exchange, Google Workspace y Skype Empresarial. Automatiza y agiliza el proceso de aprovisionamiento de usuarios con archivos CSV. desprovisionamiento masivo de cuentas de estudiantes. Simplifica el aprovisionamiento y Establece reglas para automatizar el proceso de aprovisionamiento basado en condiciones específicas. Aprovecha el inicio de sesión único para proporcionar a los estudiantes acceso a múltiples aplicaciones académicas después de iniciar sesión una vez. Permite restablecer contraseñas masivas para estudiantes que han olvidado sus contraseñas o cuyas contraseñas han expirado. Permite a los estudiantes restablecer contraseñas de Active Directory y desbloquear sus cuentas, al tiempo que mejora la seguridad mediante la aplicación de estrictas políticas de contraseñas estrictas.
Identity360	Proporciona varios MFA, incluido Google Authenticator, y autenticadores personalizados de contraseñas de una sola vez basados en el tiempo para verificar las identidades de los usuarios cuando inician sesión en aplicaciones académicas y para la verificación de correo electrónico.

PAM360	Crea y asigna usuarios roles específicos y niveles de acceso definidos. Asegura que solo los usuarios autorizados tengan acceso a ver, editar o administrar los recursos permitidos en función de su rol. Evita el acceso de los estudiantes a los recursos destinados a los maestros.
ServiceDesk Plus	Ofrece mejores experiencias a los estudiantes con Ask Zia, el agente virtual impulsado por una interfaz estilo LLM y soporte multimodal. Esta solución sirve como el punto de contacto principal para varias interacciones de Service Desk: proporcionar respuestas instantáneamente, buscar en el Service Desk, extraer y resumir artículos de KB y realizar acciones de ticketing.

OpManager Plus (on-premises) / Site24x7 (cloud)	Garantiza un rendimiento óptimo y disponibilidad de sistemas cruciales orientados a los estudiantes, como portales en línea, chatbots y servicios de backend. Monitorea servidores, máquinas virtuales, dispositivos de red y aplicaciones en tiempo real para evitar ralentizaciones que podrían afectar la experiencia del estudiante. Ofrece una experiencia digital perfecta a los estudiantes al garantizar la disponibilidad, el rendimiento y la seguridad de portales y aplicaciones académicas. Monitorea proactivamente los servicios orientados a los estudiantes para simplificar la incorporación, proteger la información sensible y proporcionar acceso ininterrumpido a los recursos a lo largo de su viaje académico. • Monitorea el tiempo de actividad de las aplicaciones, los tiempos de respuesta y los flujos de autenticación para garantizar que los portales y los servicios estudiantiles sean siempre accesibles. • Asegura las identidades de los estudiantes con monitoreo de MFA y rastrea fallas de autenticación para proteger los datos confidenciales de aplicaciones. • Proporciona visibilidad continua de chatbots, plataformas LMS y servicios académicos para garantizar interacciones fluidas. • Anticipa picos en la actividad estudiantil durante la inscripción, exámenes o graduaciones con pronósticos impulsados por IA para evitar desaceleraciones

OpManager Plus (on-premises) / Site24x7 (cloud)	• Permite a los administradores de TI agilizar la resolución de problemas y minimizar el tiempo de inactividad, asegurando que los estudiantes obtengan un acceso más rápido a los recursos que necesitan. • Aprovecha la monitorización sintética y de los usuarios reales para garantizar experiencias fluidas durante eventos de carga máxima, como exámenes en línea o períodos de inscripción. • Mejora cada etapa del viaje estudiantil con monitoreo proactivo, asegurando que los estudiantes reciban una experiencia digital confiable, segura y sin fricciones.
Endpoint Central	Permite a los estudiantes instalar aplicaciones académicas por su cuenta y automatizar actualizaciones y parches. Endpoint Central simplifica la incorporación y el offboard a través de tipos de inscripción personalizados, asegurando que sea fácil administrar el acceso para estudiantes nuevos y graduados, y facilitando limpiar el dispositivo si un estudiante sale sin previo aviso o cuando el dispositivo se pierde. Esta solución mejora la participación de los estudiantes y la eficiencia de TI al asegurar el acceso con autenticación multifactor, automatiza tareas rutinarias como el restablecimiento de contraseñas a través del autoservicio y proporciona a los equipos de TI información en tiempo real para la resolución proactiva de problemas que garantizan una solución fluida, segura y personalizada. entorno de aprendizaje digital.

Analytics Plus	Analiza los datos de servicio estudiantil de solicitudes de TI, portales de admisión y sistemas académicos para identificar cuellos de botella y retrasos en el viaje estudiantil. Implementa estrategias respaldadas por datos para resolver los cuellos de botella descubiertos de manera efectiva. Proporciona paneles interdepartamentales que combinan datos de servicios de TI, académicos y administrativos para una visión única de las interacciones y requisitos de los estudiantes. Utiliza recomendaciones basadas en IA para optimizar los servicios para reducir los fallos de inicio de sesión del portal, acortar el tiempo de procesamiento de admisiones y mejorar los tiempos de respuesta a consultas. Hace un seguimiento de las métricas de satisfacción de los estudiantes de encuestas y comentarios vinculados al cierre de boletos, ayudando a las instituciones a mejorar continuamente la experiencia del campus.
AppCreator	Agiliza la experiencia estudiantil facilitando a las instituciones diseñar un portal estudiantil seguro y de autoservicio adaptado a cada etapa del viaje académico. Permite a los estudiantes enviar solicitudes y cargar documentos a través de formularios personalizados que requieren autenticación MFA que garantice la protección de datos. Crea flujos de trabajo que notifican instant y automáticamente a las partes interesadas sobre los cambios de curso y, en general, agilizan las operaciones de estudiantes y profesores. Construye sistemas integrales de gestión del aprendizaje (LMS), que sirven como una ventanilla única para todos los requisitos del curso de los estudiantes.

Caso de uso 6:

Gestión del ciclo de vida de estudiantes y profesores

Cada ciclo académico atrae a nuevos estudiantes y personal mientras que otros se gradúan o avanzan, lo que hace que sea esencial a bordo, apoyen y fuera de borda de manera eficiente y segura. Cuando un nuevo estudiante o miembro de la facultad se une, los sistemas de TI aprovisionan automáticamente sus identidades digitales, configuran el acceso basado en roles a las aplicaciones del campus y les asignan recursos relevantes. Ya sea que un estudiante accede a plataformas de aprendizaje y horarios o un miembro de la facultad estableciendo clases virtuales y sistemas de calificación, la experiencia debe ser perfecta.

Los eventos del ciclo de vida, como las inscripciones de cursos, las hojas de ausencia o las transferencias de profesores, deben desencadenar actualizaciones automatizadas en los permisos de acceso, asegurando que las personas solo usen las herramientas y datos que necesitan en cada etapa. A medida que los profesores asumen proyectos de investigación o roles de asesoría, su acceso se expande en consecuencia, mientras que TI continúa aplicando la seguridad a través de políticas como MFA y acceso condicional.

Eventualmente, cuando los estudiantes se gradúen o el personal sale, TI debe desprovisionar automáticamente su acceso, archivar datos importantes y cerrar el bucle para reducir errores manuales, proteger la información confidencial y agilizar las transiciones. Con la gestión unificada del ciclo de vida, las instituciones pueden proporcionar una experiencia digital segura, consistente y sin fricciones para todos desde el día en que se unen hasta el día que se van.

Cómo los productos ManageEngine benefician a su institución

Producto de ManageEngine	Cómo ayuda
PAM360	Asegura el acceso privilegiado para profesores, investigadores y administradores de TI mediante la abovedación de credenciales, imponiendo el acceso justo a tiempo y grabando sesiones privilegiadas. PAM360 impone controles de acceso basados en roles para que los estudiantes, profesores y administradores reciban solo los recursos que necesitan, mientras que revoca automáticamente el acceso cuando se gradúan o abandonan la institución.
ServiceDesk Plus	Construye plantillas personalizadas con formularios dinámicos y aprobaciones y SLA asociados para manejar las solicitudes de incorporación, offboarding y transferencia para estudiantes y profesores. Aprovecha la automatización del flujo de trabajo de un solo toque dentro de ServiceDesk Plus para organizar una amplia gama de actividades en múltiples aplicaciones y herramientas.

AD360	Agiliza la incorporación y el offboard de estudiantes y profesores mediante la automatización de la creación de cuentas, la asignación de roles y el desprovisionamiento en Active Directory, Microsoft 365 y Google Workspace. Permite a los estudiantes y profesores administrar sus propias cuentas de forma segura al habilitar restablecimiento de contraseñas, desbloqueos de cuentas y actualizaciones de perfil sin intervención de TI. Esta solución fortalece la seguridad a través de MFA y el acceso condicional, al tiempo que reduce la carga de trabajo del help desk durante períodos de alta demanda, como el inicio de semestres.
Identity360	Unifica la gestión del ciclo de vida de la identidad en entornos locales y en la nube mediante la automatización del aprovisionamiento y el gobierno de acceso para aplicaciones como plataformas LMS, herramientas de colaboración y servicios de correo electrónico. Identity360 garantiza un acceso consistente y basado en políticas para estudiantes y profesores, independientemente de si los recursos están alojados en Active Directory, Azure AD o aplicaciones en la nube.

Endpoint Central	Cuando los nuevos estudiantes se inscriben, Endpoint Central aprovecha automáticamente sus computadoras portátiles con el software académico requerido, configura el acceso Wi-Fi y VPN, aplica políticas de seguridad y aprovecha su función de administración de contenido para distribuir de manera eficiente los materiales educativos. Con esta solución, esto puede suceder antes del primer día de clase para garantizar que los estudiantes estén completamente preparados y equipados desde el primer día. Los estudiantes traen dispositivos personales al campus para acceder a los recursos de aprendizaje. Endpoint Central segrega los datos personales y académicos en estos dispositivos. Importantes anuncios en todo el campus, como horarios de exámenes o alertas de mantenimiento de TI, se envían automáticamente a grupos relevantes a través de las herramientas de comunicación de Endpoint Central, lo que garantiza la entrega de información oportuna y reduce las brechas de comunicación. Cuando los estudiantes se gradúan o el personal se va, Endpoint Central revoca instantáneamente el acceso, archiva registros académicos de forma segura y borra los datos institucionales de los dispositivos, minimizando los riesgos de fugas de datos y garantizando transiciones sin gastos manuales.

AppCreator	Construye flujos de trabajo automatizados que manejan la incorporación de estudiantes y partes interesadas, aprovisionamiento de acceso basado en roles granular y offboarding. Cuando los nuevos estudiantes se incorporen a la institución, integrarlos con sistemas de gestión de identidades para asignar automáticamente derechos de acceso y recursos de provisión. Activa flujos de trabajo dinámicos para eventos del ciclo de vida de los estudiantes, tales como cambios en la inscripción de cursos, tareas de proyectos de investigación o transferencias de profesores que notifican a las partes interesadas en tiempo real.

Acerca de ManageEngine

ManageEngine crea el conjunto más amplio de software de gestión de TI de la industria. Tenemos todo lo que necesita, más de 60 productos, para administrar sus operaciones de TI, incluyendo redes y servidores a aplicaciones, Service Desk, Active Directory, seguridad, escritorios y dispositivos móviles.

Desde 2002, equipos de TI como el suyo han recurrido a nosotros en busca de software asequible y rico en funciones que sea fácil de usar.

A medida que se prepara para los desafíos de gestión de TI por delante, continuaremos liderando el camino con nuevas soluciones, integraciones contextuales y otros avances que solo pueden provenir de una empresa singularmente dedicada a sus clientes. Y como división de Zoho Corporation, continuaremos presionando por la estrecha alineación entre TI y negocios que necesitará para aprovechar las oportunidades en el futuro.

Empresas que confían en nosotros

UNIVERSITY OF CAMBRIDGE

UNIVERSITY OF PLYMOUTH

UNIVERSITY OF TORONTO

THE UNIVERSITY OF SYDNEY

SUNY The State University of New York

ManageEngine
a division of Zoho Corp.

Para más información:
www.manageengine.com | sales@manageengine.com