

**INDUSTRIA**

Finanzas

**ENTORNO**

300 empleados y 400 dispositivos en un entorno altamente regulado

**DESAFÍO**

- Garantizar que todas las computadoras portátiles y estaciones de trabajo conectadas a una red sean utilizadas por usuarios corporativos legítimos
- Automatizar los controles de seguridad para mitigar riesgos y acelerar la respuesta ante incidentes
- Evitar la interrupción de la productividad del negocio

**RESÚMENES**

- Solución sin agente, simple de usar, que requiere mínima sobrecarga manual
- Instalación no intrusiva y rápida que se integra fácilmente con la red combinada de KKB de puntos de acceso inalámbricos Aruba y switches Cisco®
- Integración de los complementos FireEye® y ArcSight™ con la plataforma ForeScout CounterACT, lo que habilita la inteligencia de seguridad compartida y las acciones correctivas en extremos automatizados
- Solución de seguridad de redes altamente confiable; el tráfico en espejo se dirige a CounterACT

**RESULTADOS**

- Visibilidad en tiempo real y supervisión continua de extremos en la red, lo que reduce la posibilidad de ciberataques mediante las vulnerabilidades conocidas
- Automatización de la gestión de contraseñas mediante administrador local para dispositivos de trabajadores remotos, lo que ahorra una cantidad de semanas-empleado por año
- Control preventivo de "ataques de tipo pass-to-hash"
- Mejora en el cumplimiento de las normas bancarias sobre seguridad de la información

# KKB

## KKB (organismo de información crediticia de Turquía) califica a ForeScout CounterACT® como el primero en seguridad de la información

### Información general

Kredi Kayit Burosu (KKB), el primer y único organismo de información crediticia de Turquía, fue fundado por nueve importantes bancos turcos en 1995. KKB contribuye a reducir riesgos financieros para numerosos sectores, entre los que se incluyen bancos, empresas de alquiler de automóviles, empresas de alquiler de casas y particulares, y tiene un millón de miembros que usan su portal de Internet habitualmente. La organización procesó 500 millones de consultas en 2014.

### Desafío de negocio

El cumplimiento y la ciberseguridad de la información financiera y personal confidencial son fundamentales para la reputación de KKB como proveedor de un servicio de confianza. En línea con estos valores, KKB solicitó una solución para obtener visibilidad y control más integrales de red para sus 300 empleados y 400 extremos.

### ¿Por qué ForeScout?

Cuando comenzó la búsqueda de una solución para aumentar la visibilidad y controles de seguridad de sus redes, KKB se puso en contacto con Symturk, su socio consultor en seguridad de la información. Symturk recomendó ForeScout CounterACT y ofreció una prueba de concepto (PoC) in situ al Jefe de seguridad de la información y administración de riesgos, Ali Kutluhan Aktaş. También se consideró Cisco ISE.

Los criterios utilizados para la evaluación incluyeron: instalación rápida, compatibilidad con una infraestructura de TI mixta (puntos de acceso inalámbricos Aruba y switches Cisco), solución sin interrupciones para garantizar la continuidad del negocio, y la provisión de más acciones automatizadas y controles de cumplimiento. KKB tomó su decisión después de comparar hojas informativas de producto y referencias de ambos productos.

Aktaş comentó: "Elegimos ForeScout en lugar de Cisco NAC en parte debido a que tenemos una infraestructura de TI mixta (no solo Cisco), pero necesitábamos una solución rápida y fácil de instalar. ForeScout nos lo ofrecía. Además, CounterACT es una plataforma única con sólidas propiedades de integración. El hecho de que pudiéramos integrarnos fácilmente con otros productos de seguridad, como FireEye, ArcSight y CyberArk®, ha permitido mejor visibilidad y protección de ciberseguridad dentro de KKB, ya que podemos acceder a la inteligencia de seguridad combinada de los productos y beneficiarnos con ello".

### Impacto en el negocio

#### Visibilidad en tiempo real de los dispositivos y vulnerabilidades

Desde que implementó ForeScout CounterACT, KKB ha obtenido mucha más visibilidad de los extremos de su red y puede controlar continuamente la infraestructura de seguridad de cada dispositivo. Aktaş sostiene: "Anteriormente, si un escaneo de puertos tenía lugar en la red, ante la posibilidad de actividad malintencionada, solo podíamos lograr la identificación después del hecho. Con ForeScout podemos detectar, ver y bloquear al mismo tiempo. Además, CounterACT nos alerta sobre las vulnerabilidades de seguridad a medida que se producen, mientras que también nos posibilita la corrección automática de los extremos. De esta forma disminuye la probabilidad de error humano".



Necesitábamos una solución NAC que fuera de rápida implementación sin correr el riesgo de interrupciones del negocio. Además, era preciso que fuera compatible con nuestra infraestructura de TI mixta con Aruba y Cisco. ForeScout CounterACT nos ofreció todo esto y mucho más, incluso magníficas capacidades de integración con nuestras herramientas de seguridad existentes FireEye y ArcSight. Es por este motivo que a CounterACT la llamamos el cuchillo del ejército suizo de nuestro departamento de seguridad de la información, ya que facilita varios controles de seguridad y controles de cumplimiento automáticos de la manera más eficiente”.

**Ali Kutluhan Aktaş, jefe de seguridad de la información y administración de riesgos de KKB**

## La diferencia de ForeScout

Los factores de diferenciación clave que contribuyeron al éxito general de KKB:

- Integración de productos de seguridad mediante la arquitectura ControlFabric
- Facilidad de implementación/ interoperabilidad en entornos de varios proveedores
- Supervisión y mitigación continuas de las brechas de seguridad y los ciberataques
- Visibilidad en tiempo real de los dispositivos en la red
- Controles automáticos de seguridad y cumplimiento, lo que reduce la sobrecarga manual

Obtenga más información en [www.ForeScout.com](http://www.ForeScout.com)



ForeScout Technologies, Inc.  
900 E. Hamilton Avenue #300  
Campbell, CA 95008, Estados Unidos

**Número gratuito para llamadas en los EE. UU.**

1-866-377-8771

**Tel. (internacional)** +1-408-213-3191

**Asistencia técnica** 1-708-237-6591

**Fax** 1-408-371-2284

## Creación y aplicación de políticas

Aktaş explicó algunas de las políticas de seguridad personalizadas que su organización ha creado con CounterACT:

- “Hemos integrado ForeScout-ArcSight-CyberArk de manera que cuando una computadora de escritorio o portátil se conecta con nuestra red, ForeScout controla la antigüedad del administrador local y si es mayor de 45 días, ForeScout envía un mensaje CEF que contiene el nombre del dispositivo a ArcSight. ArcSight correlaciona este mensaje dentro de nuestra regla personalizada y ejecuta un script en un agente instalado en el servidor CyberArk. Dentro de este script, CyberArk inicia el proceso de cambio de contraseña y, como resultado, se cambia satisfactoriamente la contraseña. Esta es una medida de seguridad esencial, especialmente para aquellos empleados que suelen trabajar fuera, lejos de las instalaciones de la empresa”.
- “Con ForeScout CounterACT, controlamos los hash de credenciales de administrador de dominio en las máquinas cliente y si encontramos un hash de inicio de sesión/credencial de administrador de dominio en una estación de trabajo, aislamos la máquina de la red. De esta forma se garantiza el control preventivo de ataques de tipo pass-to-hash. También controlamos los privilegios de administrador local en las estaciones de trabajo: Si el departamento de soporte técnico otorga un privilegio de administrador local no aprobado a un miembro del personal, lo detectamos y aislamos ese extremo”.
- “Mediante CounterACT controlamos los servicios de prevención de pérdida de datos y, sino se están ejecutando, enviamos un comando para que los ejecute tres veces. Si siguen sin ejecutarse o están completamente desinstalados, aislamos el dispositivo. También controlamos elementos, incluido el cifrado de disco, programas p2p, comportamiento sospechoso y frecuencia de escaneo de antivirus”.

## Reducción de sobrecarga manual

Uno de los criterios de selección de KKB fue la optimización de los controles automáticos de seguridad para reducir la sobrecarga manual y los riesgos. Aktaş comentó: “Antes de ForeScout, teníamos que cambiar manualmente las contraseñas en las computadoras portátiles y estaciones de trabajo, por ejemplo: si un empleado se iba de la empresa, lo que insumía mucho tiempo. Con CounterACT creamos una política personalizada que vincula ForeScout-ArcSight-CyberArk, lo que significa que el proceso ahora es automático. De esta forma podemos ahorrar dinero y garantizar una mejor seguridad de la información. Al ser proactivos y automatizar este proceso, estimo que ahorramos muchas semanas-empleado por año”.

## Integración de productos de seguridad

La tecnología ControlFabric® de ForeScout permite que CounterACT y otros sistemas de TI intercambien información y mitiguen una amplia variedad de problemas. KKB capitaliza estas oportunidades al integrar CounterACT con sus soluciones FireEye y ArcSight.

La integración ForeScout-FireEye permite la supervisión en tiempo real y la mitigación del riesgo empresarial asociado con extremos que no cumplen o se encuentran en riesgo. Las amenazas avanzadas persistentes, las redes de bots y el software malintencionado en entornos distribuidos y BYOD se pueden identificar, verificar y poner en cuarentena rápidamente.

La interoperabilidad de ForeScout con ArcSight SIEM (Security Information and Event Management) proporciona información detallada sobre la infraestructura de seguridad de los extremos, lo que permite tomar decisiones mejores, más rápidas y más informadas acerca de los riesgos de seguridad y violaciones de cumplimiento relacionados con extremos.