Case Study

FORESCOUT

KKB

KKB (Credit Bureau of Turkey) Rates the Forescout Platform First for Information Security

WEEKS SAVED
each year by automating local admin password

DETECT
look and block automatically

EASY
integration with other security products

KREDİ KAYIT BÜROSU

Industry
Financial

Environment
300 employees and 400 devices in a highly regulated environment

Challenge

- Ensure that all network-connected notebooks and workstations are used by legitimate corporate users
- Automate security controls to mitigate risks and accelerate security incident response
- Avoid business productivity disruption

Overview

Kredi Kayit Burosu (KKB), the first and only credit bureau in Turkey, was founded by nine major Turkish banks in 1995. Reducing financial risks for numerous sectors—including banks, car rentals, house rentals and households—KKB has one million members regularly using its Internet portal; the organisation dealt with 500 million enquiries in 2014.

Business Challenge

Compliance and cybersecurity of sensitive financial and personal information are fundamental to KKB's reputation as a trusted service provider. In line with this ethos, KKB required a solution to gain more comprehensive network visibility and control for its 300 employees and 400 endpoints.

Why Forescout?

When it began the search for a solution to increase network visibility and security controls, KKB approached Symturk, its information security consulting partner. Symturk recommended the Forescout platform and offered an on-site Proof of Concept (PoC) to KKB's Head of Information Security/Risk Management, Ali Kutluhan Aktaş. Cisco ISE was also considered.

The criteria used for evaluation included: fast installation, being able to support a mixed IT infrastructure (Aruba wireless access points and Cisco switches), an interruption-free solution to ensure business continuity: and the provision of more automated actions and compliance controls. KKB made its decision after comparing product sheets and references for both products.

Aktaş commented, "We chose Forescout instead of Cisco NAC partly because we have a mixed IT infrastructure (not just Cisco), but needed a fast and easy-to-install

Security Solution

- Forescout platform
- Forescout eyeExtend for FireEye NX
- Forescout eyeExtend for HP ArcSight

Use Cases

- Device visibility
- Device compliance
- Network access control
- Incident response

Results

- Real-time visibility and continuous monitoring of endpoints on the network, reducing the potential for cyberattacks via known vulnerabilities
- Automation of local admin password management for remote worker devices—saving a number of employee-weeks per year
- Preventative control of "pass-tohash attacks"
- Improved compliance with information security banking regulations

solution. Forescout delivered on this. In addition, the Forescout platform is a unique platform with strong integration properties. The fact we could easily integrate it with other security products, such as FireEye, ArcSight and CyberArk®, has enabled better visibility and cybersecurity protection within KKB, as we are able to access—and benefit from—the products' combined security intelligence."

Business Impact

Real-Time Visibility of Devices and Vulnerabilities

Since deploying the Forescout platform, KKB has gained much greater visibility of the endpoints on its network, and is able to continuously check the security posture of each device. Aktaş said, "Previously, if a port scan was taking place on the network—with the possibility of malicious activity—we could only identify that after the fact. With Forescout, we can detect, look and block at the same time. In addition, the Forescout platform alerts us to security vulnerabilities as they happen, while also enabling automated endpoint remediation. This reduces the chance of human error."

> "We needed an access visibility and control solution that was fast to deploy, without any risk of business interruption. In addition, it needed to support our mixed Aruba and Cisco IT infrastructure. The Forescout platform offered us all of this and much more—including impressive integration capabilities with our existing FireEye and ArcSight security tools.
>
> — Ali Kutluhan Aktaş, Head of Information Security/Risk Management at KKB

Policy Creation and Enforcement

Aktaş explained some of the custom security policies his organisation has created using the Forescout platform:

- "We have integrated Forescout-ArcSight-CyberArk so that whenever a computer or laptop connects to our network, Forescout checks its local admin age and, if it's older than 45 days, Forescout sends a CEF message containing the device's name to ArcSight. ArcSight correlates this message within our custom rule and runs a script on an agent installed in the CyberArk server. With this script, CyberArk starts the password change process and, as a result, the password is successfully changed. This is an essential security measure, especially for those employees who regularly work off-site, away from the company premises."
- "Using the Forescout platform, we check domain admin credential hashes on client machines and if we find a domain admin login/credential hash on a workstation, we isolate the machine from the network. This ensures preventative control of passto- hash attacks. We also check local admin privileges on workstations: If the helpdesk gives unapproved local admin privilege to a staff member, we detect and isolate that endpoint."
- "Via the Forescout platform, we check data loss prevention services and, if they are not running, send a command to run them three times. If they still don't run, or are totally uninstalled, we isolate the device. We also check items, including disk encryption, p2p programs, suspicious behaviour and antivirus scan frequencies."

Manual Overhead Reduction

One of KKB's selection criteria was optimizing automated security controls to reduce manual overhead and risk. Aktaş commented, "Before Forescout, we had to change passwords on notebooks and workstations manually— for instance if an employee left the company, which took a lot of time. Via the Forescout platform, we have created a custom policy linking Forescout-ArcSight- CyberArk, meaning that the process is now automated. This allows us to save money, as well as ensuring better information security. By being proactive and automating this process, I estimate that we save multiple employee-weeks per year."

Security Product Integration

Forescout's orchestration capabilities technology enables the Forescout platform and other IT systems to exchange information and mitigate a wide variety of issues. KKB capitalises on these opportunities by integrating the Forescout platform with its FireEye and ArcSight solutions. The Forescout-FireEye integration enables real-time monitoring and mitigation of enterprise risk associated with non-compliant or compromised endpoints. Advanced Persistent Threats, botnets and propagating malware in distributed and BYOD environments can be rapidly identified, verified and quarantined. Forescout's interoperability with ArcSight SIEM (Security Information and Event Management) provides detailed information about endpoint security posture, allowing it to make better, faster and more informed decisions around endpoint-related security risks and compliance violations.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com