Turkcell Selected SECURRENT for Its User Segmentation Project

Identity-Based Security Policy Enforcement Strengthens its Security Infrastructure

An IDC Buyer Case Study
Sponsored by SECURRENT
March 2018

Author: Yeşim Öztürk

IDC ANALYZE THE FUTURE

Executive Summary

The results of IDC's 2015 Turkey CIO survey showed that only 22% of surveyed CIOs considered advanced security solutions to be a priority. However, during IDC's 2017 survey of Turkish CIOs, that number had increased to 35% of respondents prioritizing advanced security investments. The increasing number of cyberattacks in the last three years on Turkey's most critical sectors — including banking, telecommunications, and public sectors — has increased security awareness among CIOs and CISOs (Chief Information Security Officers). Furthermore, security has started to be discussed at the board level.

Considering the exponentially growing threat landscape in Turkey, all organizations in the country should be proactively taking relevant IT security measures and providing clear guidance to business users, particularly as such users have relatively lower awareness of what they should do to avoid exposure to security threats. Minimizing employee-led errors is one of the key elements of maintaining IT security; as such, one of the ways to reduce risk of getting exposed to external threats is to eliminate employee-led security incidents. To avoid costly employee errors and improve endpoint security, companies are taking action that includes company-wide security awareness training exercises in identifying and handling phishing emails. However, these activities will not be sufficient to secure organizations amid the dynamic threat landscape. Furthermore, cybercriminals continue to find new ways for penetrating into networks.

Under traditional methods of network access management, static IP addresses were used for connecting to a corporate network. However, this method is considered a burden, given the increasing number of devices in disparate office locations, and creates management complexity. Other traditional challenges are an increasing number of mobile users, the spread of geographically distributed office locations, the growing number of on-premise and mobile applications, the diversification of products and services, and more fragmented user roles which require a detailed access definition. Furthermore, the lack of an identity-based access management protocol that is based on employee credentials can put an entire IT system at risk, as a breach at one point of the network can be used to impact an entire corporate system as a whole. That said, implementing an identity-based control mechanism for access management become a necessity.

In order to overcome all these challenges and respond to existing cyberthreats, Turkcell, the leading mobile phone operator in Turkey, selected SECURRENT to evaluate and implement a complete redesign of their network access management architecture and radically change their current approach to security. The solution implemented by SECURRENT (namely, Checkpoint Firewall Appliance) required high level of customization, and used Active Directory credentials, rather than IP addresses to identify users on the Turkcell network. The access level of each user was defined by referring their network logs and capturing their most frequent activities. User segmentation which enables enterprises to isolate workloads and define security policies for each business unit or user group, to ensure containment of threats outside the server environment was used in this case.

The solution was implemented in 35 Turkcell locations across Turkey and impacted more than 5,000 users. At the time of implementation of this solution, in late 2013, identity-based access management was a relatively new concept in Turkey. This solution, which has now been in use at Turkcell for more than four years, has exceeded the company's expectations, and as a result, other entities that are interested in a similar approach can proceed with such security investments. Engaging with the right solution provider stands out as the key success factor of the delivery of such a complex project.

The user segmentation project has created a basis for upcoming projects such as server segmentation and virtual desktop infrastructure. Furthermore, the logs generated by this new intermediate security layer are fed into the company's security operation center (SOC) which Turkcell uses to monitor anomalies and investigate the incidents. In 2018, the company plans to implement behavioral analytics, a project that will make these logs much more valuable. Turkcell aim to look at behavior patterns of its users for identifying lateral movements and advanced persistent threats by leveraging these log data.

Table of Contents

In This Buyer Case Study

This IDC Buyer Case Study looks at the issues that Turkcell was facing with their security process and systems and why they decided to engage SECURRENT in their user segmentation project. It also examines how Turkcell has benefitted from using an identity-based enforcement model (rather than an IP address-based model).

Situation Overview

Organization Overview

Turkcell is a digital operator headquartered in Turkey, serving its customers with its unique portfolio of digital services along with voice, messaging, data and IPTV services on its mobile and fixed networks. Turkcell Group companies operate in 9 countries – Turkey, Ukraine, Belarus, Northern Cyprus, Germany, Azerbaijan, Kazakhstan, Georgia, Moldova. Turkcell launched LTE services in its home country on April 1st, 2016, employing LTE-Advanced and 3 carrier aggregation technologies in 81 cities. In 2G and 3G, Turkcell's population coverage in Turkey is at 99.61% and 97.94%, respectively, as of December 2017. Turkcell offers up to 1 Gbps fiber internet speed with its FTTH services. Turkcell Group reported TRY17.6 billion revenues in FY17 with total assets of TRY34.0 billion as of December 31, 2017. It has been listed on the NYSE and the BIST since July 2000 and is the only NYSE-listed company in Turkey.

Project Overview

Turkcell's objective was to implement a solution that would allow it to have more granular control and improved visibility over the communications between servers and users. Turkcell required multiple proof-of-concept (POC) stages during this time, to ensure it found the most suitable solution and the strongest provider. Following a thorough evaluation process, Turkcell decided to engage SECURRENT for the design of its new identity-based access policy architecture and the implementation of Checkpoint firewall solutions. Checkpoint was preferred by Turkcell for various reasons, one of the reasons being that its firewall appliances were able to handle high volumes of network traffic. Generally, firewalls are perceived by organizations as bottlenecks to network traffic; however, Turkcell did not bring this bias up as a challenge, due to the capability of Checkpoint solutions. In addition, Checkpoint's "Software Defined Protection" architecture enabled Turkcell to use simpler and more modular security policies while segmenting its network. The protection features provided by Checkpoint's architecture automatically adapt to the threat landscape of the client, freeing up security administrators from manually changing or configuring thousands of user profiles/requests. Moreover, this architecture could be integrated into Turkcell's IT environment and lay the foundation for new technologies (such as software-defined networks).

The solution implemented in 35 Turkcell locations across Turkey and impacted more than 5,000 users. The project started in late 2013, and — despite its scale — was completed in less than one year (a fairly short time span for such a project):

> **As this project was of critical importance to our company, we tried to select the most suitable solution provider. SECURRENT is among the most competent and experienced Checkpoint partners in Turkey, which was one of the reasons we chose to work with them.**
>
> *Hakan Tokay, Turkcell Cyber Security Operation Manager*

Customer Objectives

According to Turkcell, a fundamental change to its previous access management model was needed to meet the challenges brought about by new business requirements, the increasing complexity of IT systems, and a growing user base. Some of the key challenges Turkcell outlined are presented below:

- Turkcell wanted to change its approach for access management by using an identity-based user segmentation model for authenticating employees on the network. However, the use of such a model was going to require a radical change to its existing architecture.
- Any ordinary user of the previous architecture could access a server to use a specific application or service. However, tracing the logs of such users was a time-consuming process for IT, because of the static, IP-based management approach in place.
- Turkcell recognized that malicious software could spread across an entire system if only one internal service or application being used by a specific user was infected. While Turkcell used a holistic IT security approach, in which different security measures applied to different levels of IT infrastructure, it nevertheless needed to further improve its security processes to minimize this risk.
- Business users' lack of awareness with regard to threats and employee-led errors could expose the company to security incidents.
- Ensuring IT employee productivity was a key identified challenge. As a part of its continuous improvement process, Turkcell wanted to improve its operational

efficiency by embracing a new approach to user segmentation and access management that would allow its IT employees to be more productive.

The new approach adopted by Turkcell and SECURRENT made use of Active Directory employee credentials to identify any attempts to connect to the corporate network, authenticate users based on rules defined on the firewall, and authorize access to certain parts of the network. However, a few concerns were highlighted by both Turkcell and SECURRENT with regard to this approach:

- The use of firewalls to control overall access management is considered risky by some enterprises. For example, no Turkcell user would be able to access the network in the case of any failure in the firewall.
- Putting firewalls between the user and the datacenter in large enterprises can be considered as a risk factor due to large and constantly growing traffic volumes on corporate networks. In this specific use case, Turkcell firewalls would also have to act smarter to identify users trying to connect to the network based on their access levels, which would increase the amount of work undertaken by these devices. This situation raised questions with regard to potential performance issues.
- It was recognized during implementation of the project that user access profiles (i.e., profiles determining who will access what service or application) needed to be analyzed, and access rights granted accordingly, in a smooth manner that prevented any business disruption.

In order to ensure the success of the project and guarantee a smooth implementation process, Turkcell and SECURRENT worked very closely to come up with a highly robust and customized architecture.

Solution Implementation

Turkcell and SECURRENT embraced a "one-step-at-a-time" approach and implemented the highly customized solution in a phased manner. The first phase of the project began in November 2013, and in the following year more than 5,000 Turkcell employees were migrated to the identity-based access management system in phases.

Turkcell and SECURRENT ran a number of tests on Checkpoint solutions and tried to identify the areas that needed customization. Turkcell subsequently created approximately 70 cases (specific parts/features of the solution that required customization or fixes) that SECURRENT needed to examine in this respect. SECURRENT was able to handle most of these cases in combination with Checkpoint engineers. In a few cases, there were major customization requests that required some development effort at Checkpoint's end. Checkpoint, however, provided all the support needed throughout the project, and played a key role in the successful delivery of the solution.

SECURRENT has played an important role in the successful management of project components by providing new approaches to the most challenging processes and ensuring business continuity.

Hakan Tokay, Turkcell Cyber Security Operation Manager

Determining the access levels of different users was one of the most challenging parts of the project. SECURRENT and Turkcell addressed this challenge with a innovative solution that saved significant time and effort. SECURRENT first monitored employee activities on the network by capturing user logs. Based on employee behavior on the network, the most frequently used applications and services were identified. Thereafter, SECURRENT configured specific rules on the firewall and access rights of users were assigned automatically. As this process did not require any updates to user devices (such as installation of agents on user PCs), most users did not notice any changes to Turkcell systems. The implemented solution also integrated with the relevant parts of Turkcell's IT infrastructure, as different individual users had varied access requirements to the internal systems.

Another important challenge was ensuring that the redesigned infrastructure was highly reliable and robust. To lower the risk of downtime to an acceptable level, avoid even a single point of failure, and ensure business continuity, Turkcell and SECURRENT designed and implemented a distributed and redundant architecture. In addition, the new architecture was made highly scalable, and designed in a way to enable business growth (e.g., to support the growing employee base and the opening of new office locations). Turkcell still uses these appliances and has not experienced any capacity problems since 2013. The company plans to use these devices until support is discontinued. SECURRENT offered quality support services to Turkcell during the implementation of the project and has maintained the service quality.

SECURRENT has maintained quality service and has continue to offer same service level since the project was completed.

Hakan Tokay, Turkcell Cyber Security Operation Manager

Solution Benefits

Turkcell gained several key benefits from using an identity-based access management approach:

- Employees are now guaranteed secure "anytime, anywhere" access to Turkcell systems.
- Turkcell derived increased control over user activities on the network by recognizing employees from their Active Directory credentials.
- There were significant decreases in the number of security incidents.
- Stronger security governance was put in place through predefined, identity-based access policies.
- There was centralized management of firewalls and access policies through a software-defined system; resulting in reduced operational burdens on IT and improved agility.
- The scalable architecture was able to support business growth.
- Agentless access management and smooth, automated migration of new users to the system was achieved.
- The highly redundant architecture guaranteed continued uptime.

There were other benefits as well to Turkcell that emerged over time:

- The time and scope of regulatory audit process got reduced.
- The ability to feed SOC with logs generated by these firewalls was created, strengthening security infrastructure.
- Limited lateral movement of cybercriminals from clients to servers.
- Formed a basis for virtual desktop infrastructure project, which expedited the implementation of this project due to defined access policies.

Present and Future Outlook

The Turkcell team is now able to replicate this authentication model to servers which are deployed in their new datacenter —thus allowing the company to enhance the protection of its infrastructure and builds its software-defined datacenter SDDC model on a strong foundation. With this approach, mission-critical applications have separate IT security policies to non-mission-critical applications. Turkcell will be able to have isolated server pools within a broader virtual server pool, with each pool having a customized security policy. This approach would further provide improved protection for virtual servers (if an isolated server environment is exposed to a security attack, other server pools will remain intact).

A further ongoing project — virtual desktop infrastructure — benefited from having varying user access levels as determined by the user segmentation project. The aim of this project is to eliminate the security risks that can result if, for example, an end-user client contains

ransomware. This brings one more layer of security on the network and increases the level of security. Users will be required to use a second authentication to connect critical applications and services.

The logs generated by the implemented solution are sowing the seeds of a new project in Turkcell. The team has plans to leverage these logs to implement user-behavioral analytics in 2018. Behavioral analytics holds great potential to improve the visibility of threats and help identify lateral movements by analyzing user behaviors across the organization. The logs collated by the existing solutions will become much more valuable with this project.

Essential Guidance

Ensuring the Availability of Network Inventory

Before starting implementation of any IT security project, organizations should ensure the availability of network inventory — a highly accurate inventory will increase the likelihood of a successful project and shorten the project timeframe. Otherwise, adding one more layer to the network may lead to a service outage due to the wrong inventory data. As a result, it is crucial to maintain accurate inventory to ensure the system's 24x7 availability.

Performing Risk Analysis and Understanding the Vulnerabilities in the IT Environment

Before proceeding with security related project, it will be useful for an organization to first understand the current vulnerabilities in its IT systems, and design RFPs accordingly. Based on the results of this assessment, organizations can identify areas of improvement within their IT systems and provide detailed specifications to prospective solution providers.

Working with Solution Providers with Proven Track Records

Complex projects require competent solution providers. Turkcell had a unique requirement for its access management system and wanted to try a new approach. This led to a lot of customization to the firewall appliance, as segmenting employees based on their behavior could only be done by successfully correlating their logs on the network. Customers are thus advised to run proof-of-concept (POC) tests and seek solution providers with solid reputations and expertise in specific domains. Additionally, providers should understand the overall IT architecture of the client, and possess strong integration capabilities, particularly if a proposed solution needs to interface with various IT systems.

Investing in a Solution Based on Long-term Business and IT Plans

Business growth in terms of increased numbers of employees, geographical expansion, and the launch of new products and services will have implications on IT strategies (and IT security as well). Enterprises should thus factor in the future state of their business operations while embarking on an access management project. The plans of IT departments

should also be considered at this stage; for example, IT may have plans to transform itself via the utilization of new technologies. Any planned solution should be scalable (i.e., be able to accommodate new users and office locations) and integrated with next-generation technologies such as private clouds and software-defined networks.

Creating a Strong Project Plan and Ensuring Successful Project Execution

Enterprises, especially large organizations such as Turkcell, need strong implementation plans to complete projects within agreed timelines. Such plans should be developed and executed jointly with the solution provider. Due to the large number of dependencies in any given project (e.g., number of business units, employees, and locations), contingency plans should also be in place as the risk of delays is high. The amount of customization might also have an impact on the project timelines; as such, this aspect should be thoroughly discussed between the partner and vendor before a project starts (preferably during the PoC stage in the tender process).

Running Pilot Projects before Going Live

A phased approach is one of the most important elements to the successful implementation of a project. In order to ensure the success of an identity-based access management solution, a small group of employees should be included in a pilot project. any improvements to a proposed system can be handled with relative ease at the pilot stage, as only a small group of employees would be affected. Based on the outcome of this pilot, a company may decide to roll out the system available to all employees and office locations.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Middle East, Africa, and Turkey

Level 15, Thuraya Tower 1
Dubai Media City
P.O. Box 500615
Dubai, United Arab Emirates
+971.4.3912741

Twitter: @IDC
https://idc-community.com/
www.idc.com