How Turkcell Ensures Its Privileged Accounts Are Under Control

Kron's Solution Meets Turkcell's Evolving Business Needs

An IDC Buyer Case Study
Sponsored by Kron
June 2018

Author: Eren ESER

IDC ANALYZE THE FUTURE

IDC Opinion

Cyberattacks are becoming more advanced, better planned, and increasingly sophisticated. According to IDC Turkey's 2018 CIO Summit Survey, maintaining security is once again the biggest technology-related challenge facing Turkish CIOs. CIOs are dealing with the real challenge of delivering strong security postures while maintaining agility and data accessibility. In recent years, many high-profile cyberattacks have been made possible by lax management of end-user permissions. An analysis of these security breaches revealed that detailed management of privileged authorizations is often overlooked by most companies.

Companies need to avoid such attacks by:

- Securing and centralizing the management of passwords and enforcing password policies.
- Controlling access to shared accounts.
- Monitoring and managing privileged sessions in real-time.
- Comprehensively logging and recording all activities for auditing purposes.
- Keeping a detailed view of privileged accounts.
- Maintaining individual accountability.
- Responding rapidly and properly in cases of misuse.

To gain further insights into how leading companies are ensuring their privileged accounts are under control, IDC recently conversed with Turkcell's security operations manager. The conversation revealed how Turkcell effectively used Kron's Single Connect solution to meet its evolving business needs. Turkcell also shared the key reasons why it chose Kron as its valuable security solutions provider.

In This Buyer Case Study

This IDC Buyer Case Study looks at how Kron's privileged access management solution is effectively used to support Turkcell's stringent business requirements. Turkcell identified scalability and efficiency as the foremost benefits offered by Kron, the engaged security solutions provider. This document looks at the challenges Turkcell faced prior to implementation of a privileged account management solution and highlights the benefits realized from its completion. At the end of the study, IDC provides practical guidance to companies aiming to mitigate the risks posed by insider threats.

Situation Overview

Organization Overview

Turkcell is a converged telecommunications and technology services provider founded and headquartered in Turkey. It serves its customers with voice, data, television (TV), and value-added consumer and enterprise services on mobile and fixed networks. Since 1994, Turkcell has continuously enlarged the variety of its services based on mobile voice and data communications, and also steadily improved the quality of its services. As a result, the company has been able to routinely increase its number of subscribers. As of April 2018, Turkcell served more than 34.6 million mobile subscribers, 2.2 million fixed subscribers, and 2.4 million TV subscribers (including over-the-top [OTT] TV subscribers). The company aims to become an integrated communication and technology services player in Southeastern Europe, operating a converged mobile and fixed network platform and offering a wide range of innovative products and services.

Turkcell has numerous investments abroad. Turkcell Group companies operate in eight countries – Ukraine, Belarus, Northern Cyprus, Germany, Azerbaijan, Kazakhstan, Georgia, and Moldova. The company was also one of the first global operators to implement HSPA+ technology (the company runs two HSPA+ technologies on its 3G network to address the high rates of data use in Turkey). Turkcell launched Long-Term Evolution (LTE) services in Turkey in April 2016, and now employs LTE-Advanced and three carrier aggregation technologies in 81 cities across the country. The company also offers fiber-to-the-home (FTTH) services with internets speeds of up to 1 Gbps. Turkcell's shares have been traded on the Borsa Istanbul (BIST) and New York Stock Exchanges (NYSE) since July 2000, and Turkcell is the only Turkish company to be listed on the latter exchange.

Challenges and Solution

Since 1994, Turkcell has witnessed the enormous growth of the Turkish telecommunications market. The company's IT operations have thus become more complex, with hundreds of users and thousands of devices that need to be managed. Before the deployment of Kron's solution, Turkcell's network consisted of disparate systems operated by independent teams. The distributed structure of the existing legacy systems created a significant cost and manpower burden on Turkcell's security management functions.

Turkcell's IT infrastructure also consisted of devices manufactured by different vendors. Each vendor's devices had distinct capabilities that needed be managed separately. In this multi-vendor environment, granting access to users was a cumbersome process. In some cases, access management was not even possible with legacy solutions in place. Moreover, as the IT infrastructure grew and became more diverse with different suppliers and device types, the management of distinct devices became ever more complicated.

In Turkcell's IT environment, there were many privileged users ranging from desktop administrators to select business users, system administrators, and third-party service providers (including outsourced workers and vendors' customer service and support engineers). The number of users from third-party service providers had also significantly increased. As such, enabling control of outsourcing teams' elevated privileges was extremely critical. Credentials needed to be granted from a central unit based on certain rules. Unfortunately, Turkcell's legacy systems were not scalable and flexible enough to address the growing requirements of outsourced teams.

As the Turkish telecommunications market continued to grow, the regulatory and compliance requirements associated with the market evolved in tandem. The comprehensive logging and recording of all activities became critical for auditing and compliance purposes. Due its growing customer base, Turkcell was required to manage vast quantities of sensitive customer data and responsibly safeguard this information. However, one shortcoming of Turkcell's legacy systems was the readability of the logs created; previous logs were difficult to read and understand, making the auditing process cumbersome. This also hindered the organization's ability to respond swiftly and properly to cases of misuse.

Overall, it was extremely costly for Turkcell to maintain its existing legacy systems. Furthermore, the legacy systems were not capable of deploying context-aware access policies and they lacked advanced device, user, and policy interaction mechanisms, which made policy creation unmanageable. With a growing number of users and managed devices, Turkcell needed a better solution that could handle the

management and storage of user credentials and system passwords in a way that would support context-aware policy creation.

Given that Turkcell offers managed security solutions to organizations, it not only abides by sector-specific regulations but also enforces strict security procedures and policies on its internal operations. After performing an internal assessment of its systems, Turkcell realized that there was a significant opportunity to improve its operational efficiency by replacing its legacy systems.

To address the challenges of regulatory compliance, insider threats, and inadequate audit trails and on-demand reporting, Turkcell decided to enhance its existing IT architecture and improve its access management systems. The company's main goal was to establish a platform that would unify and simplify the management of user access rights.

As its legacy systems were not scalable enough to handle the increasing numbers of devices and endpoints, Turkcell focused on finding a solution that could support the growing IT infrastructure needs of the company. While there were several solutions in the market, none could capably address all of Turkcell's challenges. In particular, the imperative to comply with both global and local country-specific regulations made the Turkish telecommunications industry a challenging and unique sector for most providers. Following a comprehensive evaluation process, Turkcell decided to engage Kron to efficiently secure access to its network infrastructure and applications. Kron provided the most comprehensive solution on the market — its offering had the ability to manage dozens of vendors and hundreds of network elements within a single, universal system. In addition, its offering had important impulsive response (i.e., customization) and regulatory compliance features.

Turkcell had around 15,000 devices at the start of the Kron project in 2013 (this number has since increased to 100,000). During execution of the project, the Kron project team was in close collaboration with key Turkcell stakeholders. As such, changing requirements and additional requests were addressed with agility. The project was also completed smoothly and on time.

Results

After the implementation of Kron's solution, productivity at Turkcell improved significantly in two dimensions. Due to Kron's comprehensive solution, there was a dramatic reduction in the time spent by system administrators on policy enforcement, discovery, and password retrieval and regeneration. The deployed solution also reduced the time required to set up privileged access control and support for tens of thousands of users and accounts, millions of devices and endpoints, and billions of authentication combinations. Through automation,

Turkcell also reduced the time required to change passwords for its IT environments from hours to seconds.

In addition to the reduction in labor costs associated with IT system administration, the costs related to implementing and operating applications fell dramatically. Kron's solution not only significantly improved operational efficiency but also provided IT teams with more time to implement innovative solutions that will help move the business forward.

From a licensing perspective, Turkcell also achieved significant gains. Previously, separate licenses were needed for different access control and logging systems; with the present Kron solution, only a single license is required. Additionally, three separate legacy systems — logging, monitoring, and auditing — were unified under Kron's solution.

Turkcell is now able to create policies based on groups or sub-groups that are configured in identity databases. Turkcell can also enforce policies based on user, source address, device type, and date and time.

Previously, security auditing was a grueling process as the logs created by legacy systems were difficult to understand. Justification of security alerts took a significant amount of time before implementation of Kron's solution. However, Kron was instrumental in helping maintain and sustain compliance. The solution's built-in integration with network management systems and security information and event management systems provided advanced auditing capabilities. With Kron's Single Connect solution, Turkcell auditors can now ensure that appropriate controls are in place and guarantee that user credentials are managed effectively.

> "Kron delivered a comprehensive and robust solution that addressed all of our stringent business requirements."
>
> *– Hakan Tokay, Turkcell Security Operations Manager*

The results of this project were not limited to gains in auditing, logging, and end-user authorization. Turkcell also minimized the number and duration of service losses arising from operational faults. Furthermore, Kron's solution cemented the company's capability to cope with fraud attempts. Overall, Turkcell has reached an important milestone and achieved new momentum in protecting its confidential information while simultaneously speeding up its IT operations.

Essential Guidance

Given that the volume and sophistication of cyberattacks has been increasing at an alarming rate, IDC believes that the unified management of privileged access accounts now plays an essential role. To get the best results from such management, IDC offers the following guidance:

Treat Security Management as a Vital Part of Digital Transformation

As digital transformation steadily gains momentum over time, traditional security approaches will be inadequate in addressing the evolving requirements of the new era of digital business. Security should therefore be a fundamental component of any organization's digital transformation strategy.

Look for Solutions Not Products

The IT security realm comprises a wide range of products. Each company is also unique; accordingly, end-user requirements differ based on industry and market landscape. Organizations should outline their requirements (keeping future needs in mind) and focus on deploying long-term solutions rather than procuring different security products that complicate their IT security environments.

Adopt a Unified Platform Approach

With the ever-expanding IT architectures of organizations, unified platforms will become necessary if security personnel are to gain consolidated views of user actions. Unified platforms will enable organizations to respond rapidly to cases of misuse and highlight activities that require further investigation.

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 Turkey

Zincirlikuyu Akademiler Sitesi, D Blok Daire: 74
34340 Beşiktaş – İstanbul, Turkey
+90 212 356-0282
Twitter: @IDC
https://idc-community.com/
www.idc.com