Forcepoint

Customer Story

Eczacıbaşı Holding Extends Security to the Cloud to Protect Remote Staff

Deploying CASB and extending DLP and SWG to the cloud enabled Eczacıbaşı to securely power productivity on Office 365 and other cloud applications.

As Eczacıbaşı Holding began to move its software, data, and employees to the cloud, its security strategy needed to shift with it. By deploying Cloud Access Security Broker (CASB) and extending Data Loss Prevention (DLP) and Secure Web Gateway (SWG) to the cloud, Eczacıbaşı was able to provide the same level of security it has on its enterprise network anywhere in the world. With its security policies firmly enforced everywhere, the company now has exceptional visibility into data usage and the assurance that its staff is always protected.

CUSTOMER PROFILE:
Eczacıbaşı Holding is a Turkish industrial group comprised of 44 companies across four sectors: building products, consumer products, healthcare, and other products and services. The company has over 11,000 employees and has been operating for over 80 years, though some of its brands are over 250 years old.

INDUSTRY:
Manufacturing

HQ COUNTRY:
Turkey

PRODUCT(S):
- Data Loss Prevention (DLP)
- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)

Unlocking Innovation and Productivity in the Cloud

Innovation fuels success for Eczacıbaşı Holding, a Turkish conglomerate whose brands garner international notoriety. Since being founded in 1942, the company's forward-looking mindset has helped its more than 40 businesses become leaders in their respective industries.

However, innovation at Eczacıbaşı isn't exclusively reserved for consumers. It plays an important role in defining how the business operates and collaborates. As it continuously pushes to find new ways to enable its workforce to be more productive, it has begun to migrate more applications to the cloud.

"Many of our investments over the past two years have been on the cloud side," Gürkan Papila, CIO at Eczacıbaşı, said. "While moving to the cloud isn't our main focus, it enables us to accelerate the business value of these applications."

To avoid the significant investments in hardware and talent required of on-premises solutions, the company moved to Office 365 and began migrating other systems like its Microsoft Exchange to the cloud too.

It was a tall order, but Eczacıbaşı successfully completed the migration for 5,500 people to Office 365, across 35 corporate networks, in just three months.

Shifting Security from On-Premises to the Cloud

Data privacy laws such as KVKK and GDPR pose strict requirements for Turkish companies. Eczacıbaşı has used Forcepoint's DLP and SWG in the past to meet compliance and protect its employees, but shifting to the cloud posed a new challenge: maintaining visibility of and securing data in the cloud.

Eczacıbaşı's swift migration to Office 365 led to a healthy adoption rate of the new solutions, partly due to business information being more easily accessible. However, the new infrastructure still needed the same level of security that its older applications were afforded.

One of the benefits of migrating to cloud-based applications is the accessibility of data it offers to employees. However, the popularity and ease of access that platforms like Office 365 provide means visibility into data at rest and in transit is all the more important.

In fact, just three months after migrating to Office 365, Eczacıbaşı learned from Microsoft that it had surged to the top percentile for usage of its entire platform – Teams, SharePoint, OneDrive, and others – within the EMEA region.

"This is why CASB became a 'must' for our organization," Nurdan Demirci, Digital Security and Risk Manager at Eczacıbaşı, said. "The cloud enables everyone to move quickly, and because everything is accessible from one application, we need visibility of where it goes and who accesses it. CASB gives us this functionality."

In addition to deploying the CASB, Eczacıbaşı also ran another security-driven project in parallel with the migration to Office 365: extending its DLP and SWG to the cloud in a hybrid deployment.

Challenges

- Protect sensitive data in a hybrid infrastructure.
- Balance productivity with security for remote workers.
- Gain insight on cloud application activity.
- Comply with data protection laws like KVKK and GDPR.

Approach

- Extend on-premises deployment of DLP and SWG to the cloud.
- Implement a CASB.

Driving Business Value by Mitigating Risk

By deploying a hybrid CASB solution and extending its DLP and SWG deployment to the cloud, Eczacıbaşı was able to provide the same level of security at the endpoint to all its users – whether they were on the enterprise network or sitting in a local coffee shop.

The granular visibility of data usage, scalable policy setting, and protection for web traffic all helped Eczacıbaşı mitigate risk to its business brought on by evolving workforce habits and the introduction of the cloud.

The security coverage afforded by these solutions gives Eczacıbaşı the reassurance that its employees are protected from threats that might pose a greater risk to those working outside of the traditional perimeter, like malicious URLs.

"The lack of incidents we've seen lets us know that our security policies are working as intended," Ömer Erdem, Senior Information Security Specialist at Eczacıbaşı, said. "We expect people to click malicious links while they're working at home or on the road and so ensuring they receive the same level of protection as if they were on the enterprise network is very valuable to us."

Eczacıbaşı continues to migrate more of its solutions to the cloud and extend the coverage of its DLP, SWG, and CASB. The two initiatives run in parallel to ensure the company can foster innovation and improve user productivity as securely as possible.

With more projects in the pipeline, the company is continuously evaluating its security architecture to ensure it has the right solutions to protect its employees and sensitive data, wherever they may be.

Results

- Hybrid security deployment successfully run in parallel with migration to the cloud.
- Secure traffic and data in the cloud, wherever employees are located.
- Protect users from malicious URLs and other threats.
- Generate visibility into cloud applications.