successstory

brandefense.io · info@brandefense.io

BRANDEFENSE X Doğuş Teknoloji

Interview with EMRAH KOCABUGA,
Information Security Manager

CUSTOMER	COMPANY SIZE	INDUSTRY	REGION
Doğuş Teknoloji	650+	Technology	Türkiye

> *Doğuş Teknoloji is using Brandefense to protect against cyber attacks and build the future.*

1. OVERVIEW

A leading technology company named Doğuş Teknoloji, based in Türkiye, has a workforce of over 500 individuals. As technology evolves, so do the cybersecurity threats that companies face. To protect its technological infrastructure, Doğuş Teknoloji recognized the importance of strengthening its defenses, reducing attack surfaces, and improving its response capabilities.

2. SOLUTION HIGHLIGHTS

Brandefense partnered with Doğuş Teknoloji to implement a robust cybersecurity strategy centered around continuous attack surface discovery. The solution focused on decreasing response times from days to minutes, minimizing false positives, and adopting a proactive prevention approach. The human-centric cybersecurity methodology ensured a comprehensive defense against emerging threats.

Brandefense not only provided cutting-edge cybersecurity features but also demonstrated a genuine commitment to its clients. The emphasis on customer support and responsiveness to feature requests ensured that Doğuş Teknoloji had a cybersecurity partner willing to evolve in tandem with its needs.

This customer-centric approach, marked by attentive customer support and a commitment to accommodating feature requests, positions Brandefense as not just a cybersecurity vendor but a trusted partner invested in the success of Doğuş Teknoloji's cybersecurity journey.

3. CHALLENGES

Doğuş Teknoloji, the digital security arm of the expansive Doğuş Group, faced multifaceted challenges in fortifying the cybersecurity defenses of an organization with more than 300 companies and 21,000 employees, each contributing to seven major industries: automotive, construction, media, hospitality, real estate, energy, and technology. The complexities of securing a conglomerate with diverse dynamics demanded a strategic approach to reduce the attack surface, elevate the efficacy of controls, and prioritize critical risks for prompt remediation.

Doğuş Teknoloji's security team encountered challenges in streamlining security controls, reducing the attack surface, and efficiently prioritizing critical risks for timely remediation. The company sought a solution that would not only address these challenges but also enhance overall cybersecurity posture and vision.

SUCCESS HIGHLIGHTS

- Discover attack surface continuously.
- Decreased response times from days to minutes.
- Minimize false-positives.
- Effective risk reduction with proactive prevention.
- Human-centric cybersecurity approach

CHALLENGES

- Doğuş Technology's security team aimed to reduce attack surface, elevate efficacy of controls, and focus on critical risks for remediation.

The security team at Doğuş Technology had set out some primary objectives to enhance the security of the organization.

The first among them was to reduce the attack surface of the company, which meant identifying and eliminating any vulnerabilities or weaknesses that could be exploited by malicious actors. This was to be achieved by undertaking regular security audits and assessments, implementing strong access control measures, and keeping software and systems up-to-date with the latest security patches.

The second objective was to elevate the efficacy of security controls. This involved implementing best practices and standards for security controls, such as intrusion detection and prevention systems. It also meant ensuring that these controls were regularly scanned the online world including dark, deep and surface web, to discover unknown events, automatically prioritize risks and deliver actionable intelligence.

The third and final objective was to focus remediation efforts on critical risks. This meant prioritizing the vulnerabilities that posed the greatest risk to the organization and addressing them first. The security team was responsible for conducting risk assessments and developing a remediation plan that addressed these risks in a timely and effective manner. By focusing on critical risks, the security team aimed to minimize the impact of potential security incidents and ensure the continuity of business operations.

4.RESULTS AND BENEFITS

Doğuş Teknoloji experienced a significant improvement in their security landscape after implementing Brandefense's cybersecurity solution. The solution provided real-time visibility into their attack surface, enabling proactive threat detection and response. The response time to potential threats was reduced from days to minutes, ensuring swift and effective action against cyber incidents. With the help of Brandefense's solution, the company was able to fine-tune their threat detection mechanisms, minimizing false positives and allowing the security team to focus on genuine threats. Furthermore, the proactive prevention approach resulted in effective risk reduction, enhancing the resilience of Doğuş Teknoloji's digital infrastructure.

Emrah Kocabuga

Information Security Manager, Doğuş Teknoloji

"Brandefense strengthens our company's journey in the digital world by identifying risks in advance. That's why Doğuş Teknoloji is using Brandefense to protect against cyber attacks and build the future."

5. CONCLUSION

The collaboration between Doğuş Teknoloji and Brandefense resulted in concrete outcomes, enabling the company to confidently navigate the complex cybersecurity landscape. The results include a fortified security posture, improved incident response capabilities, and a human-centric cybersecurity approach that aligns seamlessly with Doğuş Teknoloji's commitment to technological excellence and innovation.

This case study exemplifies how a strategic partnership with Brandefense can empower technology companies to proactively tackle cybersecurity challenges and secure the future.

ABOUT BRANDEFENSE

Brandefense is a proactive digital risk protection solution for organizations. Our AI-driven technology constantly scans the online world, including the dark, deep and surface web, to discover unknown events, automatically prioritize risks and deliver actionable intelligence you can use instantly to improve security.

Follow Us on @brandefense