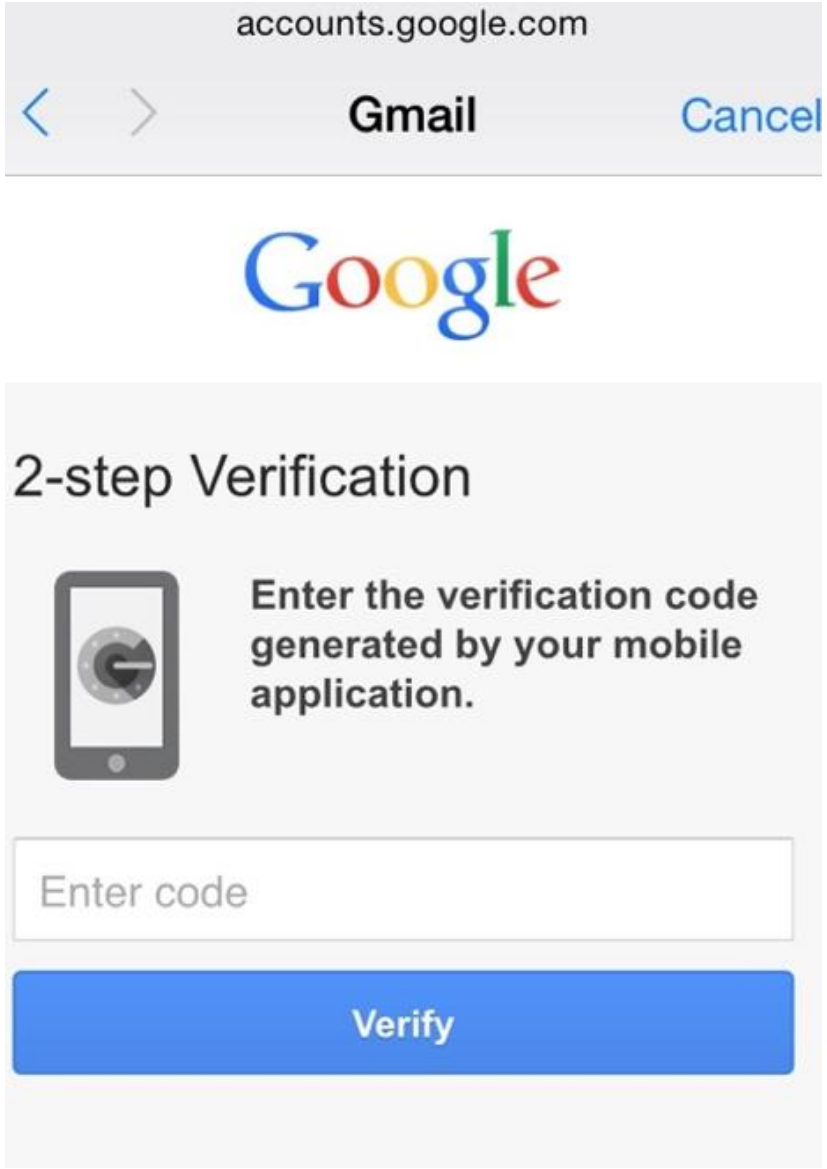
5 EASY WAYS TO ELEVATE YOUR STATE OF PROTECTION*

*Otherwise known as A Simple Guide to Vulnerability Protection

gigit®
Elevate your Cybersecurity
State of Protection

1. Implement Two-Factor Authentication



Two-Factor Authentication

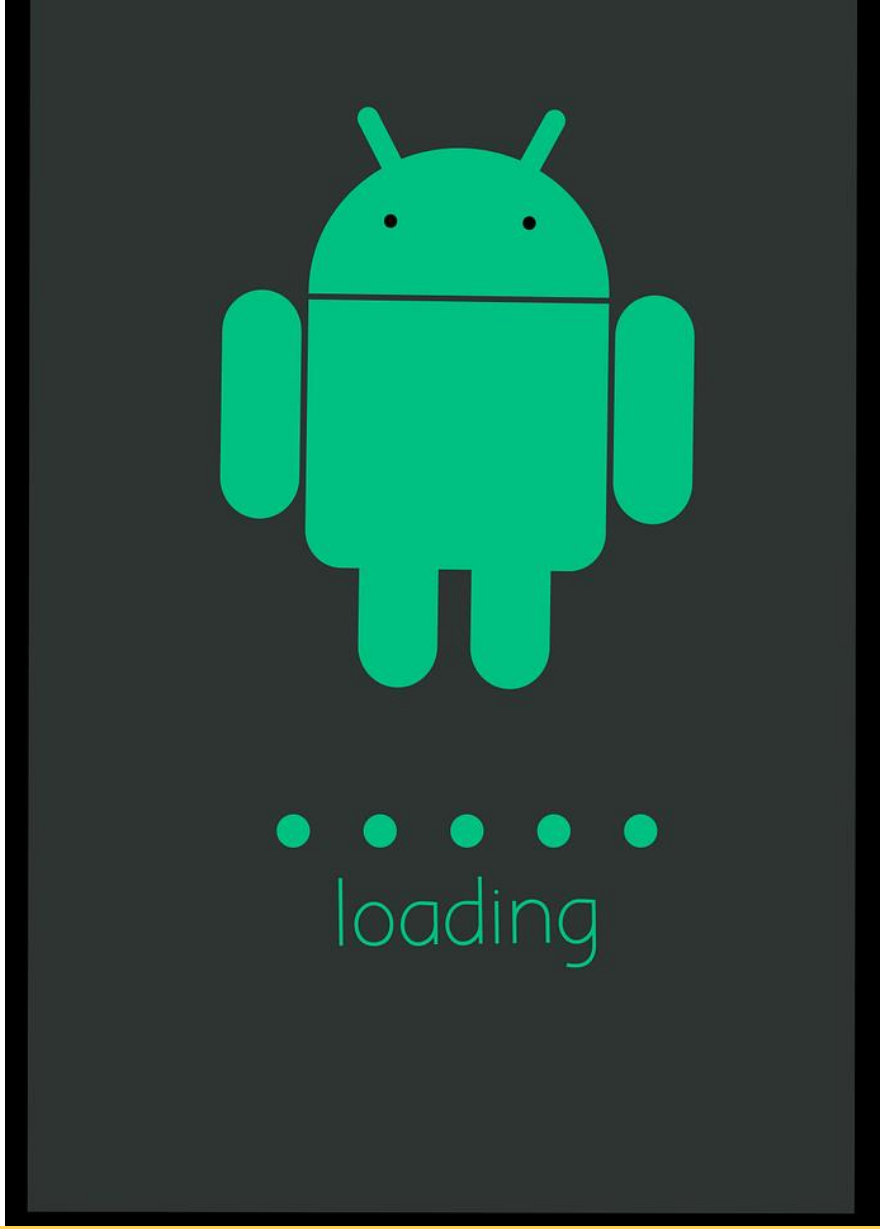
Two-Factor Authentication (2FA), also known as Multi-Factor Authentication (MFA), is a method to increase the protection of an individual's access to a resource by requiring two or more pieces of evidence:

1. Something you have
2. Something you know
3. Something you are

Why use 2FA?

1. **Passwords alone are weak** and prone to duplication and misuse. They are the weakest point guarding access to your data. Humans are predictable and will use easy to guess passwords whenever possible. ***Protect against human error.***
2. **Save resource time.** Password resets take up valuable IT resources. Let your staff work on more important projects.
3. **Thwart cybercriminals.** Without BOTH pieces of authentication information, an attacker using a person's credentials cannot move around in your environment

2. Patch Management



Patch Management

Patch Management ensures your environment is protected from vulnerabilities and Day One attacks. A patch management plan should include scheduled updates of the entire data eco-system: Hardware, Software, and the Internet of Things (all connected devices) and the implementation and testing of zero-day vulnerabilities.

Why use Patch Management?

Most of attacks are executed upon the newest vulnerabilities.

3. SIEM/Log Aggregation Review

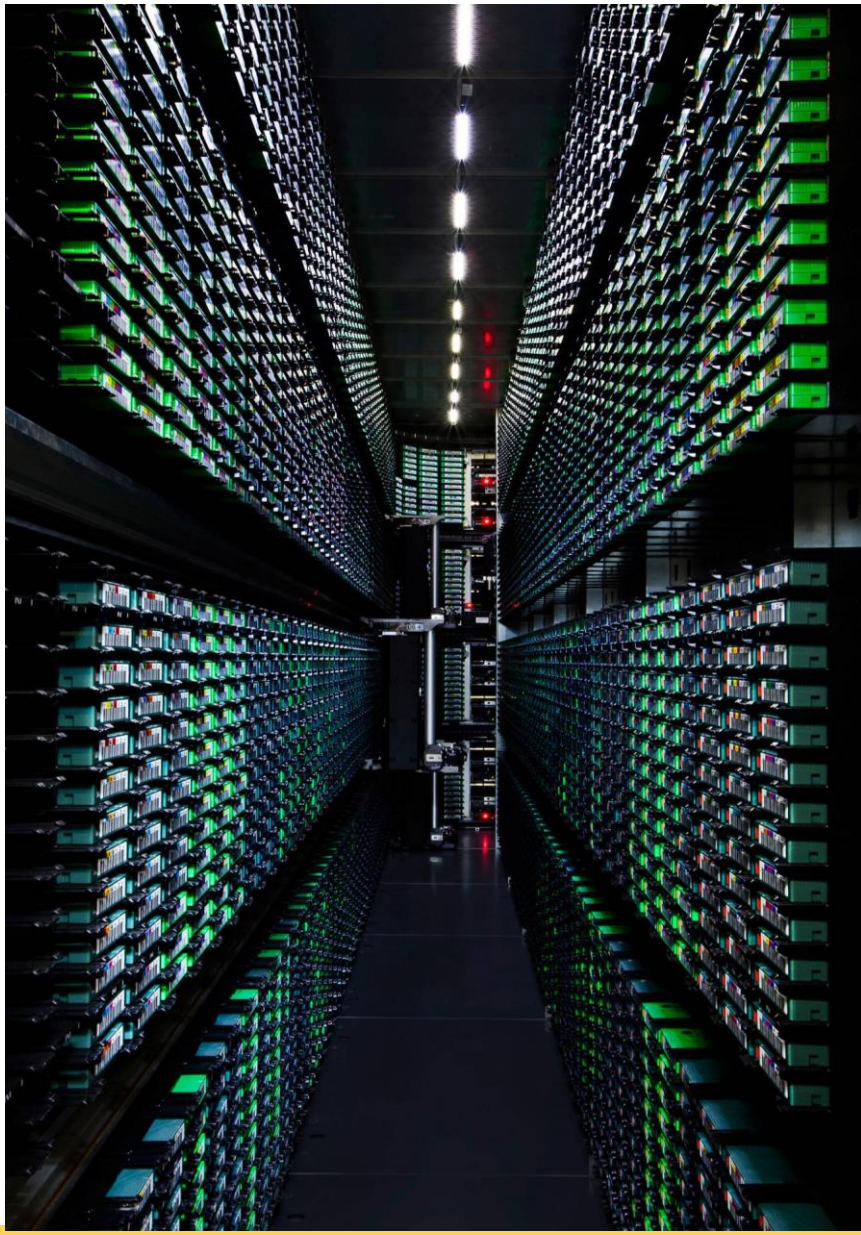
SIEM/Log Aggregation Review

A SIEM is a log aggregation system. It aggregates logs from multiple types of systems (OS, SQL, Hardware, Endpoint, and more) and analyzes those logs for anomalies, intrusions, and suspicious behavior. Newer versions of SIEM will actively mitigate and connect to other security devices to help block active attacks.

Why use a SIEM/Log Aggregation Review?

If you don't know what's going on in your environment, you can't protect it.

4. Back-Up & Disaster Planning



Back-Up/Disaster Planning

Create Separate Backups that are offsite and disconnected is key to protecting and recovering from a cyberattack.

The Disaster Recovery Plan (DR) is the key to getting the systems back up and running.

Both these combined make for a solid defense in case of an attack.

Why use a Back-Up & Disaster Planning?

Ransomware attacks are getting better at finding and deleting archived data. Having multiple, separate backups is the key to protecting and recovering from an attack…and possibly avoid paying out any ransom money.

5. Endpoint Protection

Endpoint Protection

Endpoint Protection is how corporations protect their data while employees work remotely. It's more than just using an anti-virus. It also includes:

- Network Access Control
- Application Control
- URL Filtering
- Encryption
- Logging

Why use Endpoint Protection?

1. Companies have more people working remotely.
2. Endpoints are easy targets for ransomware attacks since endpoints are often used on uncontrolled and unsecured networks.
3. Endpoint protection adds ability to lock down infected machines to prevent the spread of ransomware

Foiling cybercriminals starts with the basics, but that's not enough.

Not feeling secure about your ongoing cybersecurity?

Ask about Gigit's Cyberthreat Vulnerability Protection services.

ELEVATE YOUR STATE OF PROTECTION

Contact us today!

gigit®
Elevate your Cybersecurity State of Protection