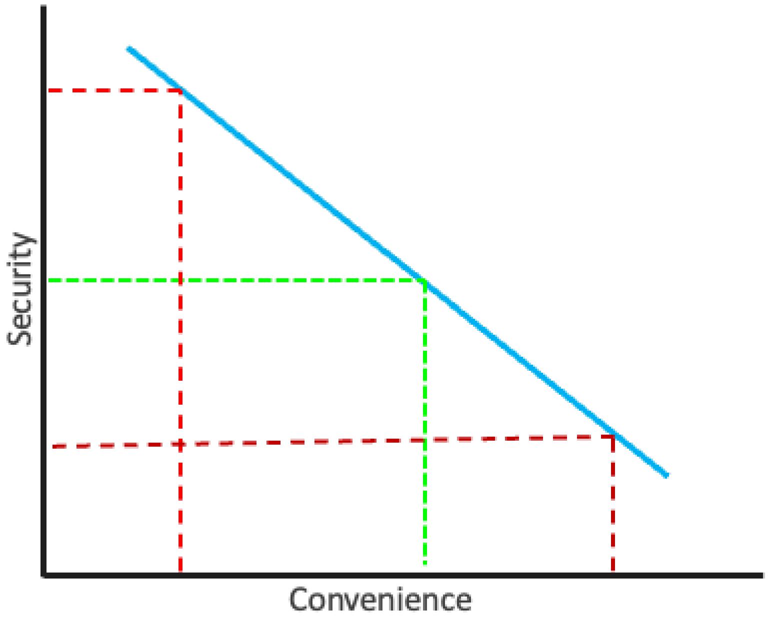
Considerations

By hosting a service, we must act as designers, developers and systems administrators. Whether it is on the open internet, available to a select few, or only for your personal use – we must make sure we consider how we can safely approach it.

Hosting your own personal cloud server can provide a great deal of digital utility, but maintaining one can come with a great deal of responsibility. We must be proactive in maintaining privacy and security – for ourselves and any community whose trust we are seeking to maintain.

We will be exploring these important considerations and what we can do to address them. Depending on how you'll be using your services, you may not need to take the same measures as someone else. Making these decisions requires we consider our needs, our audience and how we'll balance the security with convenience for our server.



Learning to balance security and privacy while creating an intuitive and approachable experience can be a difficult task, but it is perhaps the most important. While building a digital ecosystem, you'll quickly find that every decision is a trade-off between security and convenience.

Along one end, security allows us to prevent unauthorized access so we can protect private and sensitive information. We can take proactive measures by using strong randomly generated passwords, enforcing data encryption and enabling two-factor authentication.

However, as we add more steps to the process, the user experience can become more difficult to use. Remembering multiple unique passwords and entering a constantly changing authentication code every time we log in can be annoying.

The more secure we create a system, the more restricting it will generally become. It is not uncommon for the hardest part of secure tools being that they're simply hard to learn to use. If we were to use the most secure enterprise tools available, we'd have to sacrifice usability and convenience – both for setup and continued usage.

In practice, there cannot be a system that is fully secure because then we would never be able to access it. To that end, convenience is important to consider because it can affect and inform how people will use that system.

When a user is frustrated by the inconvenience of remembering multiple random passwords, they may seek to remove a step in the process by writing down the password and attaching them to the monitor. People may hunt down insecure ways to access a system – decreasing security for everyone.

We need to find an ideal medium between our control over a system and our ability to use it. Threat modeling is a necessity to understand that balance point for our purposes. Through four targeted questions, we will explore how these apply to us.

Threat Models

Security is not a checklist of steps to be completed, but an active and ongoing discussion's. When stopping to consider the largest and most likely threats to our security, we have begun to create a threat model. They are a vitally important step to building a relationship with security.

In cyber security, a threat is any event undermines your ability to keep your data private and system secure. This can be the intentional actions of a malicious actor, an accidentally unsecured website offering a backdoor, or people intentionally getting around confusing security measures.

It's impossible to plan for every potential edge case, which is why a threat model focuses on the most probable and critical threats. Once we have a better understanding of these weaknesses, we can create safeguards and prioritize countermeasures.

The threat model outlines a defensive gameplan that provides a systematic overview. This covers what the system will be, who will have access, who might attack and why, as well as what they're hoping to acquire and how they might do it.

Bomb

Attack Vector

When a malicious actor has made the decision to attack to get their desired target, they will need to figure out how. Depending on what they're after, there are various strategies they can employ – each informed by what they're hoping to achieve.

While considering these facets of security, you might start to see the ways it can be broken. By creating a threat model, we can identify key weaknesses and implement safeguards throughout its lifetime. This is not checklist, but instead an ongoing discussion to surface any potential (and emergent) flaws.

Through a series of questions, we will explore the potential weaknesses within the systems outlined within these guides. Alongside exploring how to proactively protect against these potential attack vectors, you will need to explore whether they're the right option for you.

How Large is Your Community?

This is important to identify because it can help us draw boundaries around potential malicious actors. When hosting a small server for your own personal use, there are far fewer people you need to worry about overall. Meanwhile, orchestrating several websites each catering to a hundred people has much more risk involved.

The cloud server systems provided by this guide are similar techniques to large companies – but they have a magnitude of scale more computing power. Realistically, a refurbished workstation and the tools provided herein will work decently well for supporting up to twenty-five people. The quality of their service depends on several factors:

Diversity_3

Community Dynamics

When offering services to a community, you must keep in mind the support you will need to provide. This will manifest differently depending on the services you are hosting.

- ***Code of Conduct:*** When creating a public space where people interact, it is necessary to state norms, rules and responsibilities.
- ***Moderation:*** Enabling communication within a community necessitates the enforcement of the rules to ensure a safe space for all.
- ***Tech Support:*** In the event that something goes wrong, you'll need to offer the time to help get it working again.
- ***Outreach:*** Growing a platform requires an investment in community relationships.

What is Your Attack Surface?

When dealing with a software environment powered by physical hardware – such as hosting a server – you need to consider your level of exposure. There are often many vectors that malicious actors can exploit to attack software systems. An attack surface is the sum total of all possible vulnerabilities within the system being examined.

The goal of cybersecurity is an attack surface that is as small as possible with proactive protection against known weaknesses. The digital landscape continues to change rapidly, only increasing the necessity of systematic threat analysis.

Measuring your attack surface is an ongoing process that can expand over time – often unevenly. As you add more hardware, the more potential you have for encountering vulnerability within the system.

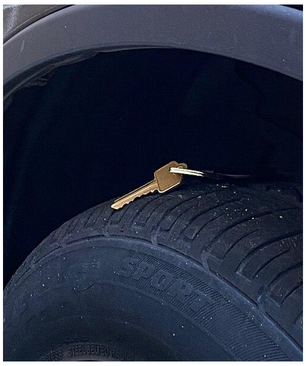
As you provide community services and offer access to broader audiences, your threats deepen. While you may be able to exert control over a private cloud server, members have their own autonomy – to enforce or eschew best security practices. More moving parts invites more risk: can you ensure that your friend will use a strong password?

When approaching security in software development, there are two important philosophies that inform the choices made:

Lens_blur

Security By Obscurity

This paradigm relies on concealing how the software works as a proactive security measure. While security traditionally constitutes physical locks or safeguards, this approach relies on sleight of hand – such as a key obscured by shadows as it rests on a car tire.



This philosophy assumes that secrets with remain secret – but this is often not the case. This is heavily employed by proprietary software by obscuring source code. While this can complement an already robust system, it is deeply discouraged as the sole security.

Confidentiality, integrity and availability are the core underlying of security. Ensuring there is no unauthorized access or modification while keeping systems always available requires careful planning.

Step 1: Visualize Systems

Before we can correct any potential vulnerabilities, we need to take stock of our hardware and software systems. This will include making a list of internet-connection electronic devices, such as:

Smartphone

Mobile Devices

These devices generally focus on a "cloud-first" approach and wireless connection methods for improved portability.

- Cellphones
- Tablets
- Smart Watches

Terminal

Software

User applications add more variability to the defined standards of operating systems.

- Servers
- Drivers

Router

Communication

Computers process information independently and often transmit their data over a network – either local or regional in scale.

- Wired Networks
- Wireless Networks
- Personal Area Networks
- Networking Devices

Home_iot_device

Internet-of-Things Smart Devices

These devices often contain system-on-a-chip computers that enable updates over the Internet.

- Appliances
- Climate Control
- Lighting
- Sensors
- Speakers
- Microphones
- Security Devices

[[Basic diagram of some devices and the ways they connect]]

Your digital attack surface will change shape from day-to-day and continue to morph over time. While computers may shut off at night or disconnect from the Internet, a server will always be a beacon visible over the network.

As the number of vulnerable points grow and opens potential for attacks, defenses become even more important. In the worst case clscenario, malicious actors only need one exploit to gain unauthorized access. These are some common elements:

Domino_mask	**Privacy** WHOIS registration You will be sharing your public IP address with the world. Domain registration Credit card payments Things that are tied back to you by address, name and money.
Deployed_code	**Dependencies** Web Frameworks (PHP, Apache, Java, etc.) Web Server Services (email, database, applications)
Psychology	**Social Engineering** Phishing

Step 2. Define Boundaries

Step 2: Find indicators of exposures. The second step is to correspond each indicator of a vulnerability being potentially exposed to the visualized map in the previous step. IOEs include "missing security controls in systems and software".[4]

Define your boundaries

Who do I want to protect it from?

What do you consider an attack?

Pest_control

Web Crawler

bots and web crawlers

https://en.m.wikipedia.org/wiki/Web_crawler

Web crawler, sometimes called a **spider** or **spiderbot** and often shortened to **crawler**, is an Internet bot that systematically browses the World Wide Web and that is typically operated by search engines for the purpose of Web indexing (*web spidering*).[1]

Crawlers consume resources on visited systems and often visit sites unprompted. Issues of schedule, load, and "politeness" come into play when large collections of pages are accessed. Mechanisms exist for public sites not wishing to be crawled to make this known to the crawling agent. For example, including a `robots.txt` file can request bots to index only parts of a website, or nothing at all.

Claude ai bots

https://en.m.wikipedia.org/wiki/Claude_(language_model)

Step 3. Create Safeguards

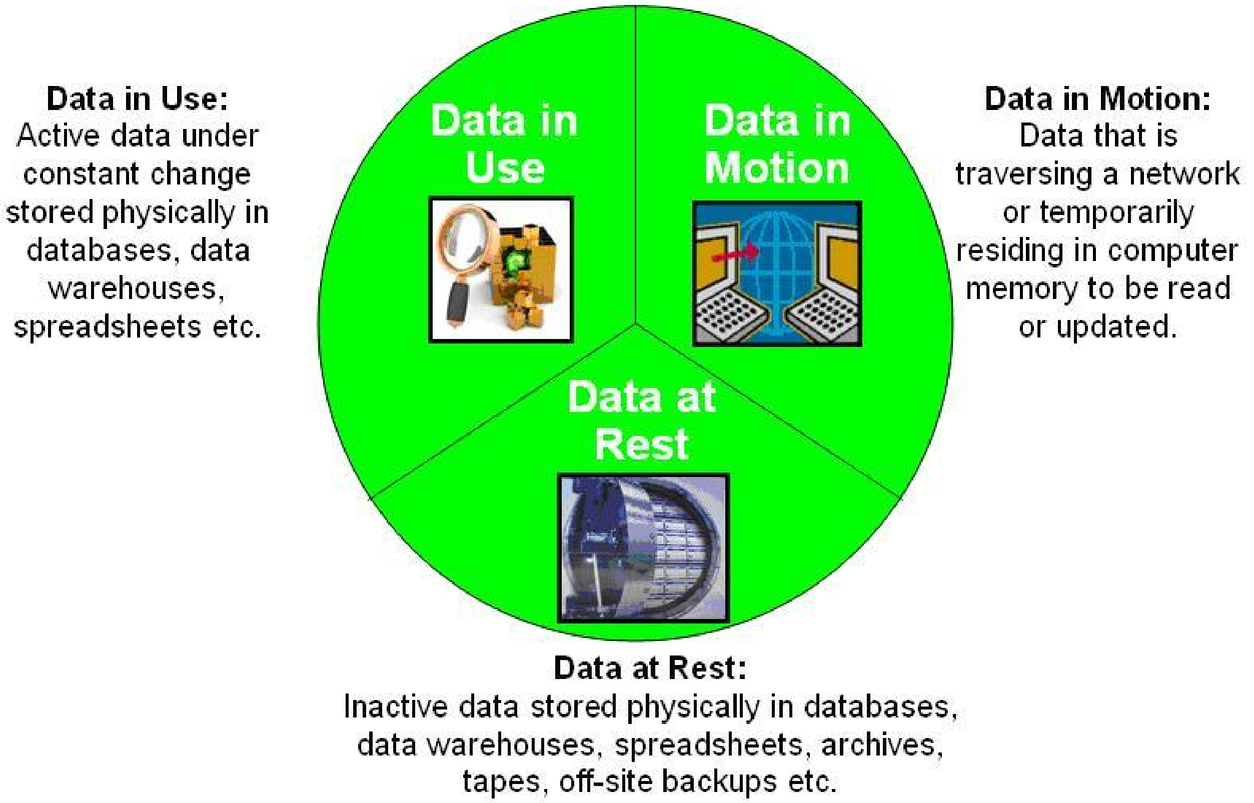
Step 3: Find indicators of compromise. This is an indicator that an attack has already succeeded.[4]

Add safeguards

One of the most simple and important ways to protect data and security is through encryption.

Encryption

https://en.wikipedia.org/wiki/Encryption



In cryptography, **encryption** (more specifically, encoding) is the process of transforming information in a way that, ideally, only authorized parties can decode. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Despite its goal, encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.

Animation

Data in Transit

Https enceyption

encryption in transit

https://en.wikipedia.org/wiki/Data_in_transit

Data in transit, also referred to as **data in motion**[1] and **data in flight**,[2] is data en route between source and destination, typically on a computer network.

Data in transit can be separated into two categories: information that flows over the public or untrusted network such as the Internet and data that flows in the confines of a private network such as a corporate or enterprise local area network (LAN).[3]

Data in transit is used as a complement to the terms *data in use*, and *data at rest* which together define the three states of digital data.[4]

end to end encryption

using all three to ensure data is always encrypted.

On top of this foundation, we can add targeted defenses to help shore up security from specific angles

Encrypted	**Physical Security** Lock case Restrict access to server Remove keyblard and mouse unless needed
Policy	**Monitoring** intrusion protection services Monitoring services Swag dashboard Fail2ban
Security	**Isolation** LAN access vs server only access (127.0.0.1:80:80) vs 80:80 Within docker, containers can be configured to be accessible over the local network to all computers, as well as restricted to access from only the local machine. This means you can open it while using a browser on the server computer, but your other computers cannot access it over the network.

kill switch

https://en.m.wikipedia.org/wiki/Kill_switch

A **kill switch**, also known more formally as an **emergency brake**, **emergency stop** (**E-stop**), **emergency off** (**EMO**), or **emergency power off** (**EPO**), is a safety mechanism used to shut off machinery in an emergency, when it cannot be shut down in the usual manner. Unlike a normal shut-down switch or shut-down procedure, which shuts down all systems in order and turns off the machine without damage, a kill switch is designed and configured to abort the operation as quickly as possible (even if it damages the equipment) and to be operated simply and quickly (so that even a panicked operator with impaired executive functions or a bystander can activate it). Kill switches are usually designed to be noticeable, even to an untrained operator or a bystander.

What is The Value of Your Data?

- What do I want to protect?
- How likely is it that I will need to protect it?
- How bad are the consequences if I fail?
- What is the value of the data? Does a hacker care about Joe Schmo? Probably not. But do you have confidential company data, or are you an important stakeholder? Well, now you've suddenly become a bigger target.
- How important is it to someone else, and how important is it to you, your security, identity and privacy?
- Privacy ensures that unauthorized parties do not have access to your information and that you continue to control your personally identifiable information (PII). Therefore, Data privacy primarily deals with procedures and policies governing the collection, storage, and use of PII and proprietary company information such as trade secrets, personnel, and internal processes. PII is highly confidential because of the civil and criminal liability companies and individuals face if improper disclosure is allowed overtly or due to unintended data security breaches.

  To ensure privacy, you need more than a specific technology or set of technologies. This includes training all employees who have access to sensitive data about approved data protection processes. Just as airline pilots use checklists to ensure that essential items are checked before a flight and monitored during flight, IT professionals must also be willing to use privacy policies and other resources to protect PII and other sensitive information. In particular, to ensure privacy, IT professionals must have a set of policies, and processes detailing how organizations and their employees collect, store, and use sensitive data on all systems. This privacy policy aims for all employees to recognize the importance of privacy, understand how to prevent inappropriate disclosure of information, and deal with privacy issues and policy violations.

  Data breaches are no longer just embarrassing or inconvenient for businesses. Currently, privacy laws such as GDPR impose penalties for failing to protect the privacy of PII and other sensitive personal information. These compliance standards may impose financial penalties and criminal charges for PII's intentional and, in some cases, unintentional disclosures. GDPR imposes privacy standards and legal requirements on all companies that store or process the personal information of EU residents.

- What Is Data Security?
  Data security uses physical and logical strategies to protect information from data breaches, cyber-attacks, and accidental or intentional data loss. Specifically, technologies and techniques used to prevent:

    - Unauthorized access
    - The deliberate loss of sensitive data
    - Accidental loss or corruption of sensitive data

  Examples of measures to ensure data security include data encryption, both at rest and in transit, and physical and logical access control to prevent unauthorized access. Specific techniques include multi-factor authentication, multiple layers of network and application-level access control, and detection and isolation of rogue devices after connecting to the network. Regular backups and a proven disaster recovery plan are essential parts of data security.

  In short, data security is based on a technically sophisticated and comprehensive approach to protecting all networks, applications, devices, and data stores within an enterprise IT infrastructure.
- The best way to understand the difference between data security and privacy is to look at the mechanisms used in your data security and privacy policies. Privacy policies control how data is collected, processed, and stored. While your organization's data security is more robust, detailing physical and logical controls to secure data. The way you collect, store, or distribute that data can violate your privacy policy. For example, enterprises can ensure that sensitive information is encrypted, masked, and restricted adequately to authorized parties. However, improper collection of this data, such as not obtaining informed consent from the data owner before collecting the data, does not change the security of the data but violates data privacy rules.
- Is this a vulnerable community?
- Vulnerable communities are groups within a population that face a higher risk of negative health, social, or economic outcomes due to various factors. These factors can include social, economic, political, and environmental components, as well as limitations due to illness or disability. Examples include people with disabilities, low-income individuals, racial and ethnic minorities, and those experiencing homelessness.
- Social:
  Poverty, lack of access to healthcare, discrimination, limited English proficiency, and social isolation can all increase vulnerability.
  Economic:
  Low income, unemployment, and lack of access to financial resources can make individuals more susceptible to hardship.
  Political:
  Marginalization, lack of political representation, and policies that disproportionately affect certain groups can contribute to vulnerability.
  Environmental:
  Living in areas prone to natural disasters, pollution, or lack of access to clean water can create vulnerability.
  Health-related:
  Disabilities, chronic illnesses, and mental health conditions can limit an individual's ability to cope with challenges.
-

  Examples of Vulnerable Communities:

People with disabilities:
May face physical and social barriers, limiting their access to employment, healthcare, and other essential services.

Racial and ethnic minorities:
May experience discrimination, systemic barriers, and disparities in health and socioeconomic outcomes.
Low-income individuals and families:
May struggle to afford basic necessities, access healthcare, and live in safe environments.
Individuals experiencing homelessness:
Face high risks of health problems, violence, and social exclusion.
Elderly individuals:
May be more susceptible to illness, social isolation, and financial hardship.
Children:
May be particularly vulnerable to neglect, abuse, and the effects of poverty and environmental hazards.
LGBTQIA+ individuals:
May face discrimination and social stigma, leading to increased risks of mental health issues and violence.
Migrant workers:
May be vulnerable to exploitation, low wages, and lack of access to legal protections.

- Prisoners
- Should this data be accessible to the outside world, should it even be digitized?
- Is this information about your personal media collection or is it access to all of your financial data?
- Physical and digital security
- Physically locking down a computer

How Much Effort Are You Willing to Spend?

- How much trouble am I willing to go through to try to prevent potential consequences?
- How much time, money and effort are you willing to put into your security? Remember, there are entire companies dedicated to security, and entire SOC's whose sole job is monitoring for security incidents and even they don't catch everything. These organizations have multiple experts, layers of defense and constant monitoring, but the data they protect is worth it (see #2 above). How much effot you're willing to put in determines how many steps you need to take.
- Documentation
- Resources
- Updates & Upgrades
- Hardware and software
- Integration
- what you can handle yourself vs what you need a dedicated professi me

- onal for.

Revision #42
Created 17 April 2025 03:52:39 by metaphorraccoon
Updated 10 July 2025 09:19:50 by metaphorraccoon