Building and operating a secure online service

Guidance for organisations that use, own, or operate an online service who are looking to start securing it.

Introduction

Organisations rely on online services to communicate and exchange information with their customers and partners. By definition, these services are exposed to the internet and all the cyber security risks that this brings.

This guidance aims to provide organisations with a place to start in securing their online service by highlighting key cyber security considerations for those that use, own, or operate an online service. Where applicable, this is supported by more detailed NCSC guidance.

The following diagram provides a high-level view of how modern online services are delivered. This diagram will be used throughout this guidance to illustrate the area covered in each section.

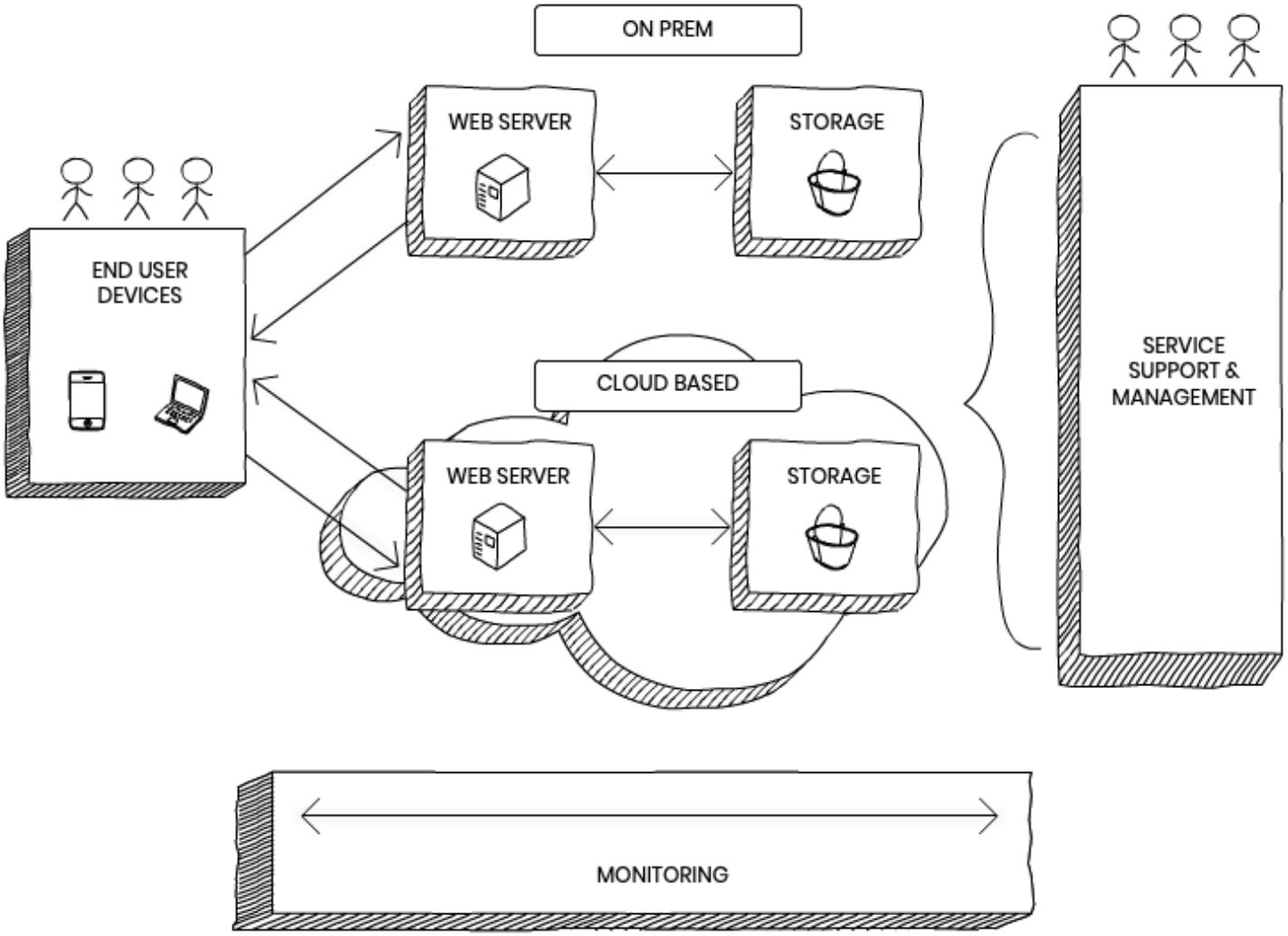

Figure 1: Overview of an online service

Managing your risk

Online services are attractive targets for all kinds of attackers with varying levels of competence, resources, and motivation. It is therefore important that the cyber security risks facing any online service, that you are building or operating, are understood and that steps are taken to manage them effectively.

Attackers may target your online service for many reason, which could include:

- to commit fraud or gain unauthorised access to sensitive information (for example your IPR, or employee or customer data)
- to prevent your service from functioning

- to damage your reputation, or for political reasons

Irrespective of whether your online service is delivered by a cloud-based or on-premise-based solution, it is important that you understand the cyber security risks associated with its delivery, management and maintenance including any risk that is associated with the supply chain for your service. Where a shared responsibility model exists between you and your cloud or service provider, you must ensure you are always aware of what you are accountable for. While security responsibilities will vary depending on the type of cloud service you are consuming, you will always be responsible for the effective management of the data that you store and process within your online service.

Risk analysis techniques such as attack tree analysis and threat modelling can provide meaningful insights to inform the design and development of your online service. These approaches become even more useful when used in conjunction with knowledge bases of known threat tactics, techniques and processes (TTPs) for example those provided by Mitre Att&ck® framework.

Assurance

Online services are sociotechnical systems, meaning that they involve people, technology, business processes, and supply chains. As the owner and operator of an online service you should seek confidence in the way these work and confidence that they deliver and maintain security effectively and as expected. In the cyber security context, this confidence is often referred to as security assurance or simply assurance. The amount and type of assurance you need should be based on a clear understanding of the risks your online system faces. Therefore you should seek to gain assurance in:

- the people who manage and maintain your systems
- the processes and technology you use
- the data centres that house your systems
- the way information is stored and processed and your supply chain

More detailed information on how cyber security risks can be identified, assessed, and managed is available within the NCSC's Risk management guidance.

Identity and access management

Identity and access management is fundamental to gaining confidence in the people interacting with your service as well as the way in which they interact with it. This section discusses this topic further as well as giving useful resources to help manage and control access to your service.

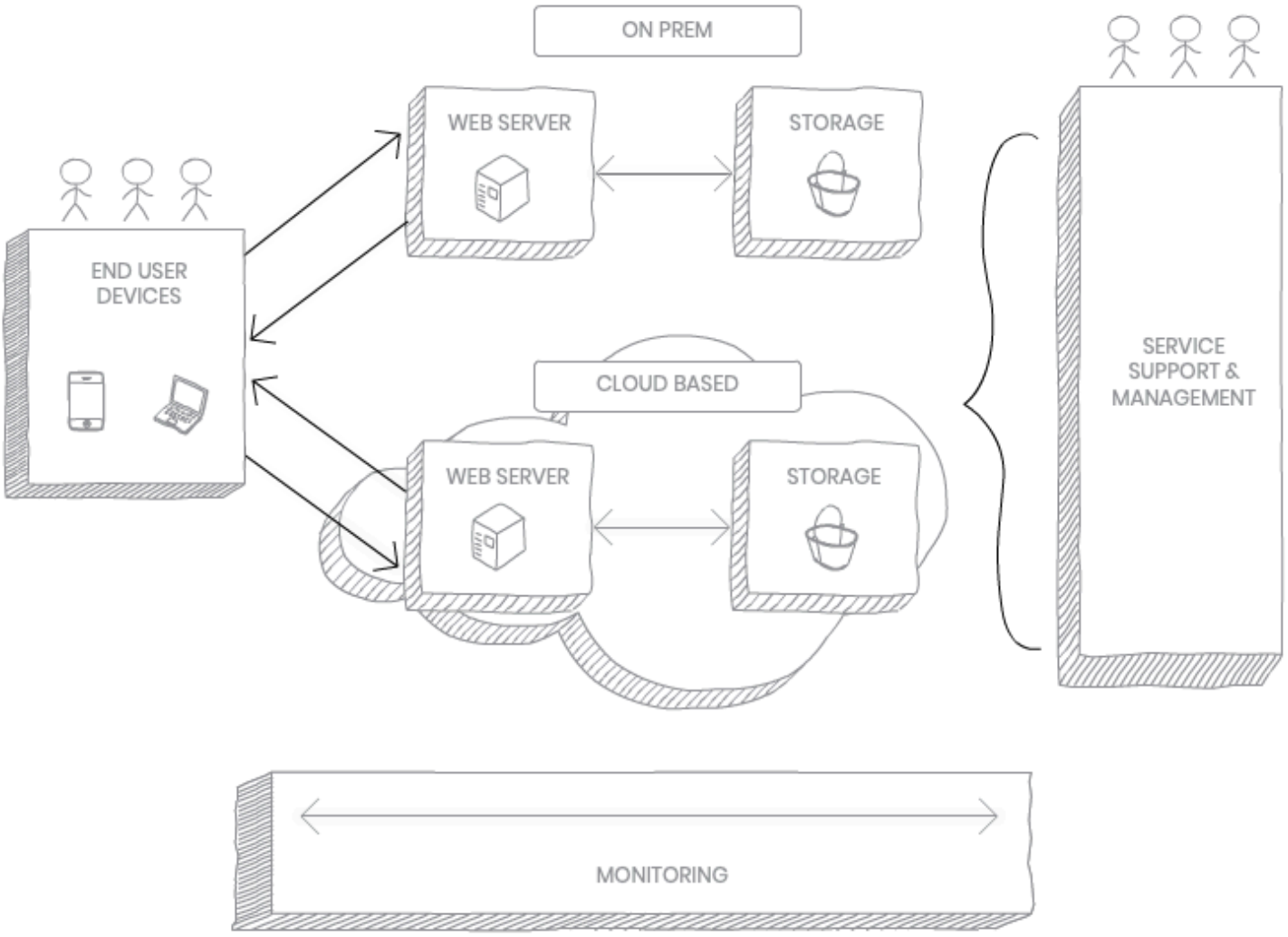

Figure 2: Identity and access management

The front door of an online service is accessible to everyone. This means that it is important that only those who are authorised to access your online service can do so.

In some cases, the platform may be open to everyone and there is no need to have any confidence in their identity. But in other cases, you will require the ability to control access to your service and to gain confidence and trust in the identity

of those that use it. In these circumstances, the steps you take to gain confidence will depend on the risk associated with what the service does and what people can do when they have access to it.

For example, when someone is able to gain access to sensitive information stored and processed by your service (or can make changes to the service itself) then you will need to put in place stronger identity, authentication, and authorisation controls than in a scenario where someone can simply access the service to read any information published for general consumption.

The NCSC's Introduction to identity and access management and GOV.UK's How to prove and verify someone's identity (GPG 45) will help you understand how to effectively manage identity and control access to your service.

Securing your service

Online services have a number of elements, as shown in the diagram below. Securing each of these components is important in order to provide a secure service. This section covers a vast selection of topics from managing data within your service to securing its different components.

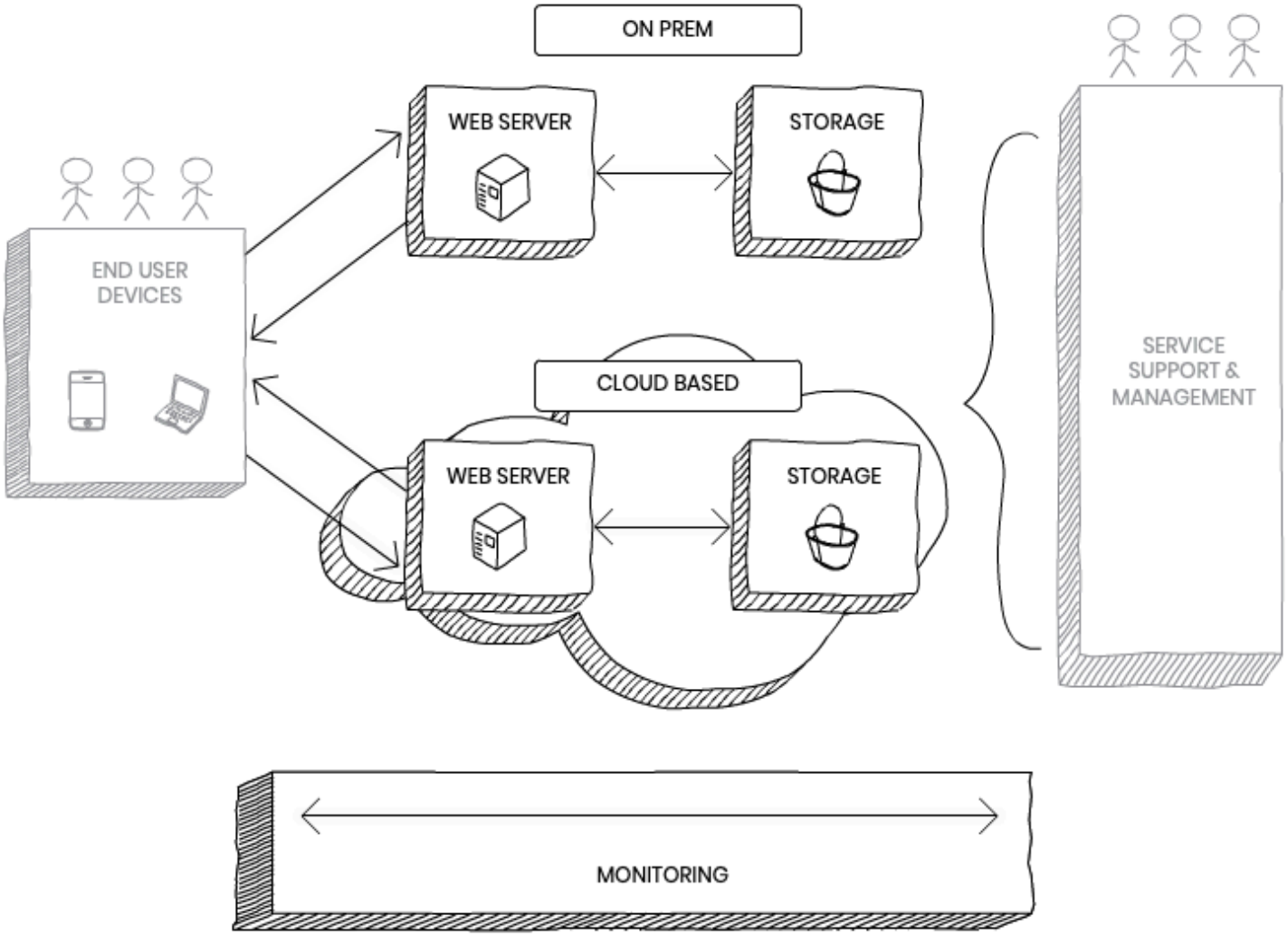

Figure 3: Securing your service

It is not possible to say that any system is 100% secure. However, aiming to design, develop and deliver an online service that is as robust as is needed should always be the aim. This section will help organisations gain confidence in the security of the online service components they are responsible for, in order to provide assurance of the overall end-to-end service.

Secure development and design

It is important that security is considered from the outset when designing and developing an online service. Security should be implemented by default into all aspects of the service and into the ways you deliver, manage, and maintain it. The NCSC's Secure design principles and our Digital service security guidance provide a baseline that will help give your service the best possible start, discussing the key elements to consider when creating a new system. The OWASP Top 10 Web Application Security Risks offers a view of the most common

attacks in this space, defending against these should be considered throughout the development of the system.

It is important to follow secure development practices. The NCSC's Secure development and deployment guidance will help with this. More specific application guidance, including mobile applications, can be found in our Application development guidance, and our advice to help organisations to produce clean and maintainable code provides the foundations for securely building applications that deliver an online service.

Additionally, the NCSC blog post Defending software build pipelines against malicious attacks outlines the importance of protecting your development pipelines and following best practice.

When implementing an API solution, it is important to understand the security risks associated with it, the OWASP API Security Top 10 provides a detailed overview of the common threats. A thorough summary of how to implement a secure API solution can be found in the GDS API technical and data standards.

Platform and server security

The NCSC has published a selection of guidance cover how best to secure your platforms and servers. These comprise:

- For guidance on specific platforms, refer to the NCSC's Device security guidance on how to choose, configure and use devices securely. Whilst we focus on desktop versions (Android, Chrome OS, iOS and ipadOS, macOS), our Ubuntu and Windows guidance can be used as starting points for setting up their server counterparts. These cover many aspects that can be applied to servers as well - deployment scripts and policy settings are just two examples. In addition, our Device security principles (that is, the basis for our guidance on the configuration of specific devices) can be applied to platforms not addressed in specific sections.
- Management interfaces perform privileged actions on systems on servers, and as such require locking down. We have useful blog posts on how to Protect your management interfaces, and Protecting your privileged access

management. Our white paper on Security architecture anti-patterns and guidance on Systems administration architectures should also help.

- Where the delivery of an online service includes the use of cloud technology, for example to host applications or store data, then ensure that the risks are understood and take steps to verify that they are fit for your service. We recommend that you make use of the security guidance and advice provided by cloud service vendors to help you build your services so that they are secure. For example, Microsoft Azure Well-Architected Framework and AWS Well-Architected. In addition, the NCSC's Cloud security guidance should help you make best use of cloud technology.
- You should seek confidence in the hardware, operating systems, services, and applications you use to build and deliver your online service. For example, you could also consider building your system using products and services that have been independently assessed against the NCSC standards.

Network and service security

It is important that you design your online service so that it is not connected directly to untrusted networks such as the internet. Its design should make it hard for attackers to move around within your systems (should they gain access to it) which is known as 'lateral movement'.

Make use of network and application layer security technologies such as security groups and firewalls to provide boundary protection and segment your network and service. Further useful information is provided in the NCSC's guidance on Architecture and configuration and Preventing Lateral Movement.

Online services will need to protect denial of service (DoS) attacks . A common DoS attack is to flood the host server with requests, making it unavailable to its users or 'slow down' the service response. The NCSC's Denial of Service (DoS) guidance discusses how to prepare and respond to such an event.

When bringing data of any kind into your platform from an unknown source there are always risks. Many attacks against online services stem from malicious input. The NCSC's pattern for Safely Importing Data explains how to defend your system when bringing in data from an external source.

Data Security

All data and information stored and processed by an online service needs to be protected against unauthorised access, change and deletion, this includes personally identifiable and other sensitive information. The NCSC's Protecting bulk personal data guidance provides further guidance on scenarios where the use of encryption to protect personally identifiable information should be the norm, and scenarios where the use of encryption may be challenging. Our secure design principles and our cloud security guidance can be used to help you make decisions about how best to protect the data stored and processed by your online service.

Failure to properly protect personally identifiable information can result in legal action, financial losses, and damage to reputation. The NCSC's GDPR security outcomes guidance outlines appropriate security measures under the UK General Data Protection Regulation.

Attackers will often target online service data stores with the aim of misusing the data and information they access. This information could include a customer's personal information such as user credentials. If stolen, this information could be used to breach other accounts owned by the victim (this is known as credential stuffing). Further information can be found in the NCSC's Use of credential stuffing tools advisory.

Secure disposal of data

When data and information stored by an online service is no longer required, it should be disposed of securely. This includes removing the information and data associated with a customer's online account and making sure that data does not persist on equipment or cloud-based storage. The NCSC's Secure sanitisation of storage media guidance further discusses this topic. Failing to remove and dispose of information and data securely when it is no longer required could result in its unauthorised release, and or legal and reputation damage for the organisation.

Data in transit

'Data in transit' refers to any data that is moving from one location to another. This could be over the internet, a private network, between programs or even

between people and systems on removable media. Whilst sensitive data will need to move within the system, it is not guaranteed to be protected against interception, unauthorised viewing, and alteration before arriving at its destination.

Any sensitive information should be protected against these attacks. This is usually done using encryption and other cryptographic techniques. The NCSC has produced guidance on Using TLS to protect data and Using IPsec to protect data, both of which can help you to secure data in transit across your platform. You should consider the risk associated with data that is in transit to and from your online service and in some cases it may be appropriate to prevent the connection of devices to your service that cannot support the latest versions of these security protocols.

Secure administration

Managing and administering an online service will mean giving someone privileged access to your systems. The systems, accounts, and credentials used to gain management and maintenance access to online services are very attractive targets for attackers. Exploiting privileged access can result in damage to your service and the way it works, loss of or unauthorised access to sensitive information and damage to your reputation. To avoid this, you should seek to use multi-factor authentication (MFA) for all management, maintenance, and administration access. Privileged access management solutions should be used which only allow access from trusted workstations, such as browse-down or privileged access workstations (PAWS). The following NCSC guidance will help you manage your online service securely.

- Multi-factor authentication for online services
- Gain trust in your management devices
- Use privileged access management
- Security architecture anti-patterns
- Operating a secure digital service

Supply chain

The security of the supply chain related to your online service is pivotal to the security of your online service itself. Any vulnerability introduced to your online service by any hardware, software or supporting service you source from a third party could result in compromise of your service and any information it stores and processes. Understanding the risks posed by your suppliers and ensuring that their cyber security responsibilities are properly covered in contracts and service agreements will help you gain confidence in these relationships, and our supplier assurance questions will help you gain confidence in their cyber security. Our further guidance on supply chain security presents 12 principles to help you establish effective control and oversight of your supply chain.

Support

All online services require some element of human support, you need to be confident that all employed staff, or third-party service providers, have the required technical knowledge to perform their role without putting your online service at risk. User education and awareness will help provide you with confidence in this area. You can also gain confidence in those people who manage and maintain your online service through things like pre-employment checks and security vetting.

Operational Security

Operational security covers the what is required to ensure your service is as secure as necessary, through security testing, vulnerability management and updates and patching.

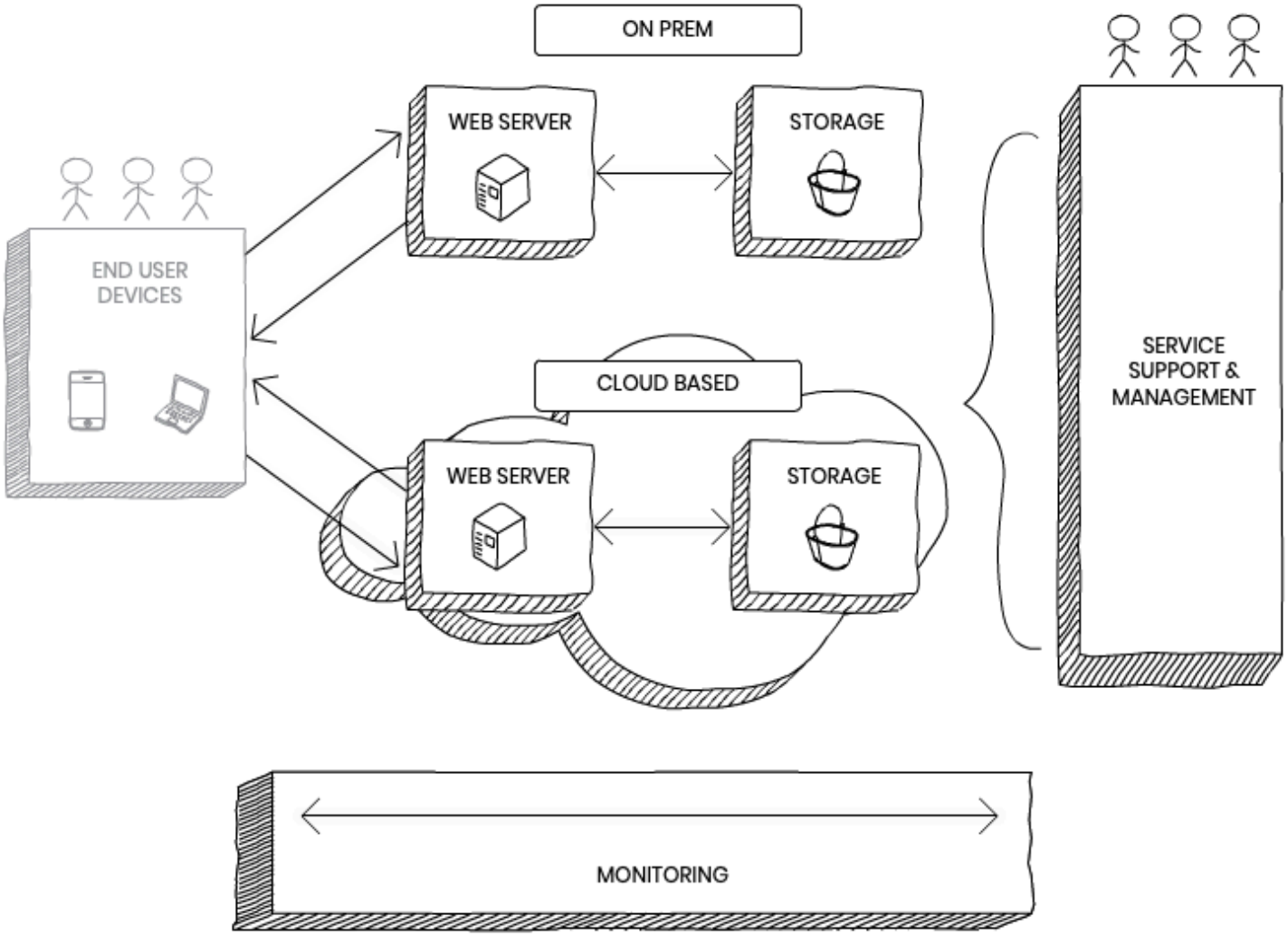

Figure 4: Operational Security

Security testing

Security testing comes in many forms, a lot of which should be implemented into a robust development lifecycle as discussed earlier, in our secure development and design section. Security testing can be carried out using manual and automated methods and tools and often a blend of these approaches is best, automated tests are often based on sets of rules aimed at picking up flaws and logical errors, whereas manual testing can pick up less logical flaws and errors. In the application security world, testing can be either dynamic or static, static testing involves the review of code without executing the application whereas dynamic testing tests an application that has been executed. All these testing approaches are different and have their pros and cons, and usually, a mix of testing types is best.

Penetration testing is a commonly used method to help gain confidence in your system's technical implementation and business processes, as well as the

through life controls put in place to protect it. This is provided through a thorough review of the individual components that make up the service as well as the communications between them. The scoping of a penetration test is very important to gain the most value. It should be tied into the business logic of the service and look to inspect specific areas of identified risk within the platform.

When scoping a penetration test of a cloud-based platform, the shared security model should be well understood. Knowing what falls within the user/ cloud providers' responsibilities will help ensure necessary areas are tested. The NCSC's How to get the most from penetration testing guidance explains the importance of good penetration testing, the various different types and what questions should be considered in order to get the most benefit from it. Further information relating to security testing can be seen in our building a secure digital service guidance.

Vulnerability management

Exploiting a known vulnerability is a common starting point for most cyber security attacks, especially against online services. The NCSC's vulnerability management guidance offers a step-by-step guide from identifying vulnerabilities through to managing them effectively. Vulnerability scans should be implemented into your development pipelines so that before release you can have confidence that there is nothing easily exploitable present. There are a range of tools available to aid with this, often they will reference resources such as the CIS Benchmarks to check the configuration of components within the service, these relate to the many known vulnerabilities of specific components as seen in the CVE dataset.

Updates and patching

Keeping hardware and software up to date can help protect your online service from attacks that seek to exploit known vulnerabilities. To gain confidence in your system components, ensure that your management and maintenance plans include a regime to update and patch the hardware, firmware and software used to deliver your online service. A benefit of using cloud services can be their auto-patching and updating features, allowing your service to stay automatically up-to-date without the need for your intervention.

Logging and monitoring

The section provides a summary of the various monitoring functions your service requires, namely logging, security monitoring and transaction monitoring.

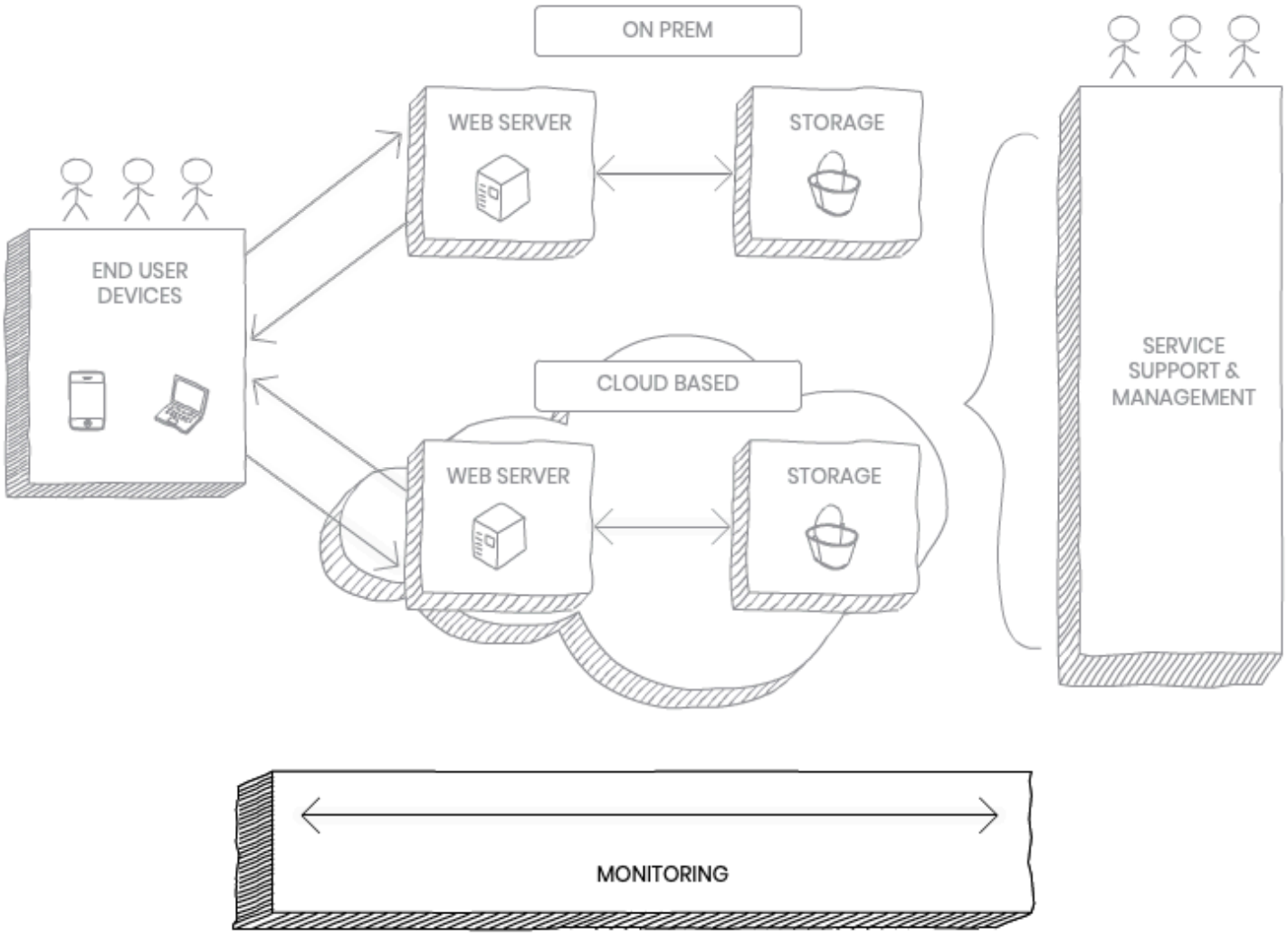

Figure 5: Logging and Monitoring

Logging

Good logging is necessary for any effective monitoring solution. Collecting data on activity across your system provides a baseline understanding of your online services health, showing what is normal and providing traceability when something is flagged as being a security or functional problem or issue. To collect valuable logs, a robust logging strategy should be devised.

Details on how to do this can be found in the NCSC's Introduction to logging for security purposes guidance. This will include making decisions on which logs to generate or retain, how best to collect logs in your system, how to store the logs and how to ensure your logging capability is working as intended. Further details about finding a logging approach that works for your system can be found in the NCSC blog post What exactly should we be logging?

Security monitoring

Security monitoring allows your online service to effectively detect and respond to an attack. This is achieved by building and understanding of what 'normal' looks like (in terms of the way your online system works) and then watching out for anomalies to the perceived normal in logs and other sources of monitoring information. A good monitoring system can identify and potentially stop an incident before it has lasting impact.

Information on developing a monitoring strategy can be found in the NCSC's 10 Steps to Cyber Security: Monitoring guidance and in our blog post Keeping your security monitoring effective.

Transaction monitoring

Online transactions, like those in the real world, attract criminals who seek to commit fraud by - for example - impersonating online service customers for financial gain. It is therefore important that if you operate an online service that you can detect these kinds of attacks and respond to them effectively, in a timely way to minimise their impact.

Further information on how to apply transaction monitoring effectively to your online service can be found in the Transaction monitoring for online services guidance.

Proactively protect your online service

The NCSC offers several Active Cyber Defence (ACD) services that can help online service providers assess, monitor, and maintain the security of their services.

For example:

- **Mail Check** helps organisations secure their email, in particular standards that prevent criminals from spoofing their email domains (DMARC), encryption-in-transit (TLS and MTA-STS).
- **Web Check** helps owners of public sector websites to identify and fix common security issues, making sites in the UK a less attractive target to attackers.

Should you be eligible, we recommend that online service providers make use of relevant ACD services. Not all ACD services will be applicable but further information on the ACD services offered by the NCSC can be seen here: NCSC's Active Cyber Defence programme.

Protecting your service from bots

It is important to understand when your service is interacting with a human and not a computer when new accounts are being created, or when you are providing access to the resources provided by your service. This should also be considered during any transaction within your system.

To achieve this, ensure you include checks to gain confidence in the user you are interacting with. This should sit within your approach to protecting and monitoring, the setup of and access to accounts, access to resources, and the conduct of transactions.

Incident management

Most online services will experience a security incident at some point, however secure. Organisations should assume that they will be breached at some point and therefore plan accordingly. Investment in effective incident management policies and processes greatly improves resilience, business continuity, and customer and stakeholder confidence as well as reducing impact in the event of

a compromise. It is important that any incident management procedures are both well thought through and thoroughly tested.

- The NCSC's incident management guidance talks about how best to prepare and deal with an incident.
- The NCSC's Exercise in a Box toolkit allows organisations to find out how resilient they are to cyber attacks and practise their response in a safe environment.

PUBLISHED

2 March 2022

REVIEWED

2 March 2022

VERSION

1.0

WRITTEN FOR

Large organisations

Cyber security professionals

Public sector