Overview of The DNS Resolution Process

01

User Query

Browser sends domain name to DNS resolver (ISP or public DNS like Google/Cloudflare)

02

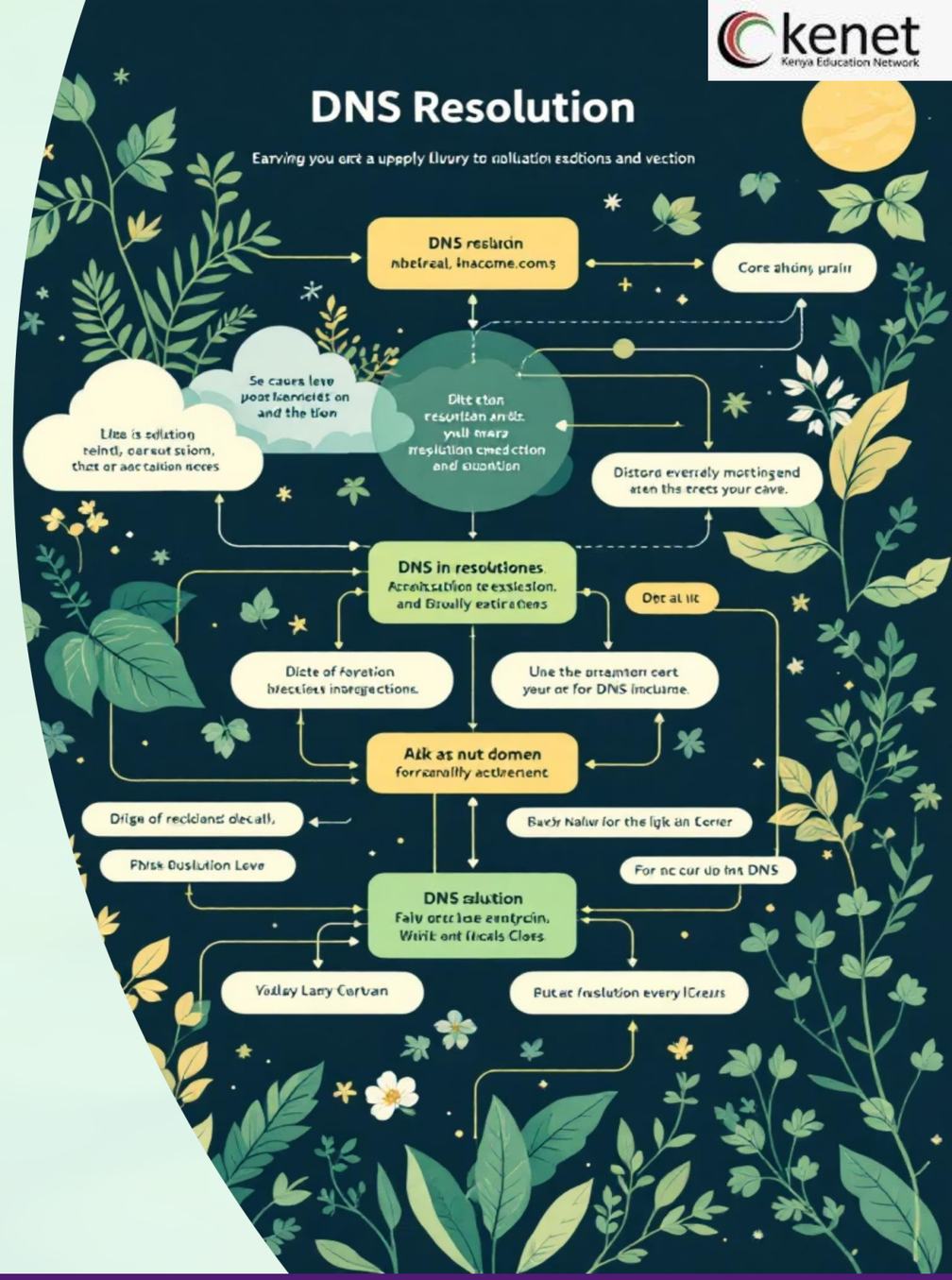
Recursive Query

Resolver contacts DNS servers hierarchically: Root nameserver → TLD nameserver → Authoritative nameserver

03

IP Address Response - Resolution Complete

The authoritative server returns the definitive IP address, enabling your browser to establish a direct connection to the target website and load the requested content.



The DNS Resolution Process - Lookup Journey

Understanding the resolution process is key to grasping how DNS works. It's a series of steps that occurs every time you type a domain name into your browser.

01

User Enters Domain Name

When you type www.kenet.or.ke into your web browser and press enter, the process begins.

02

Local DNS Cache Check

Your computer first checks its own local DNS cache. If the IP address for www.kenet.or.ke is found here, the process stops, and the browser can connect directly.

03

Query Sent to DNS Resolver

If not in the cache, the query is sent to your configured DNS resolver (usually provided by your ISP).

04

Resolver Queries Root Server

The resolver asks a Root Name Server for the IP address of www.kenet.or.ke. The Root Server responds by directing the resolver to the appropriate TLD Name Server (e.g., for .com .ke etc).

05

Resolver Queries TLD Server

The resolver then queries the TLD Name Server for www.kenet.or.ke. The TLD server responds by directing the resolver to the authoritative name server for kenet.or.ke.

06

Resolver Queries Authoritative Server

Finally, the resolver queries the Authoritative Name Server for kenet.or.ke. This server provides the actual IP address for www.kenet.or.ke.

07

IP Address Returned & Cached

The IP address is sent back to your DNS resolver, which then sends it to your browser. The resolver also caches the IP address for future use.

08

Browser Connects to Website

Your browser uses the received IP address to connect to the web server hosting www.kenet.or.ke, and the website loads.

DNS Caching Speeds Everything Up

Caching stores DNS data closer to users, reducing lookup time and bandwidth consumption.

Browser Cache

1

First location checked. Modern browsers cache DNS records for set time periods to minimize processing steps.

Operating System Cache

2

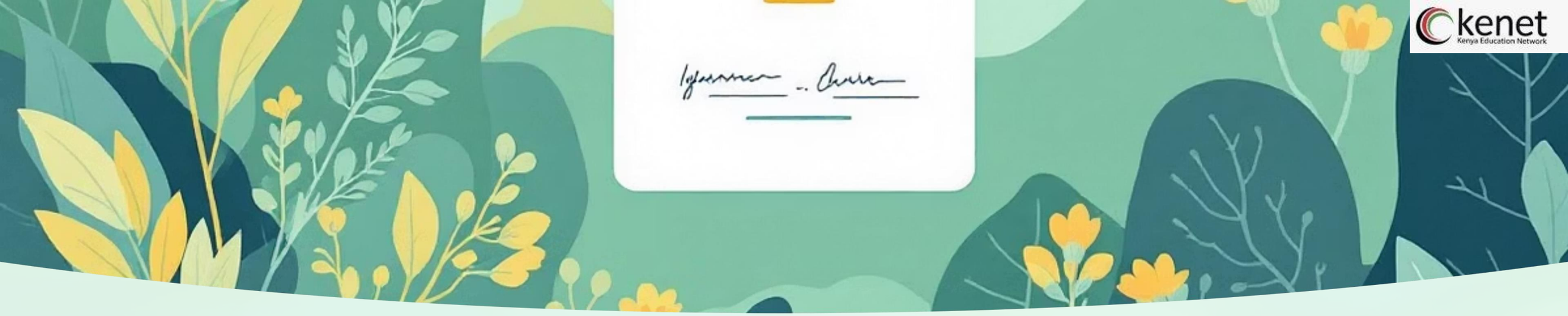
Second local stop. OS-level DNS resolver checks its cache before sending queries outside the local network.

ISP Recursive Resolver

3

Final cache layer. ISP's recursive resolver stores records and can bypass multiple lookup steps when cached data exists.

Introduction to DNSSEC: Securing the Internet's Address Book



What is DNSSEC? Adding Trust to DNS

Cryptographic Protection

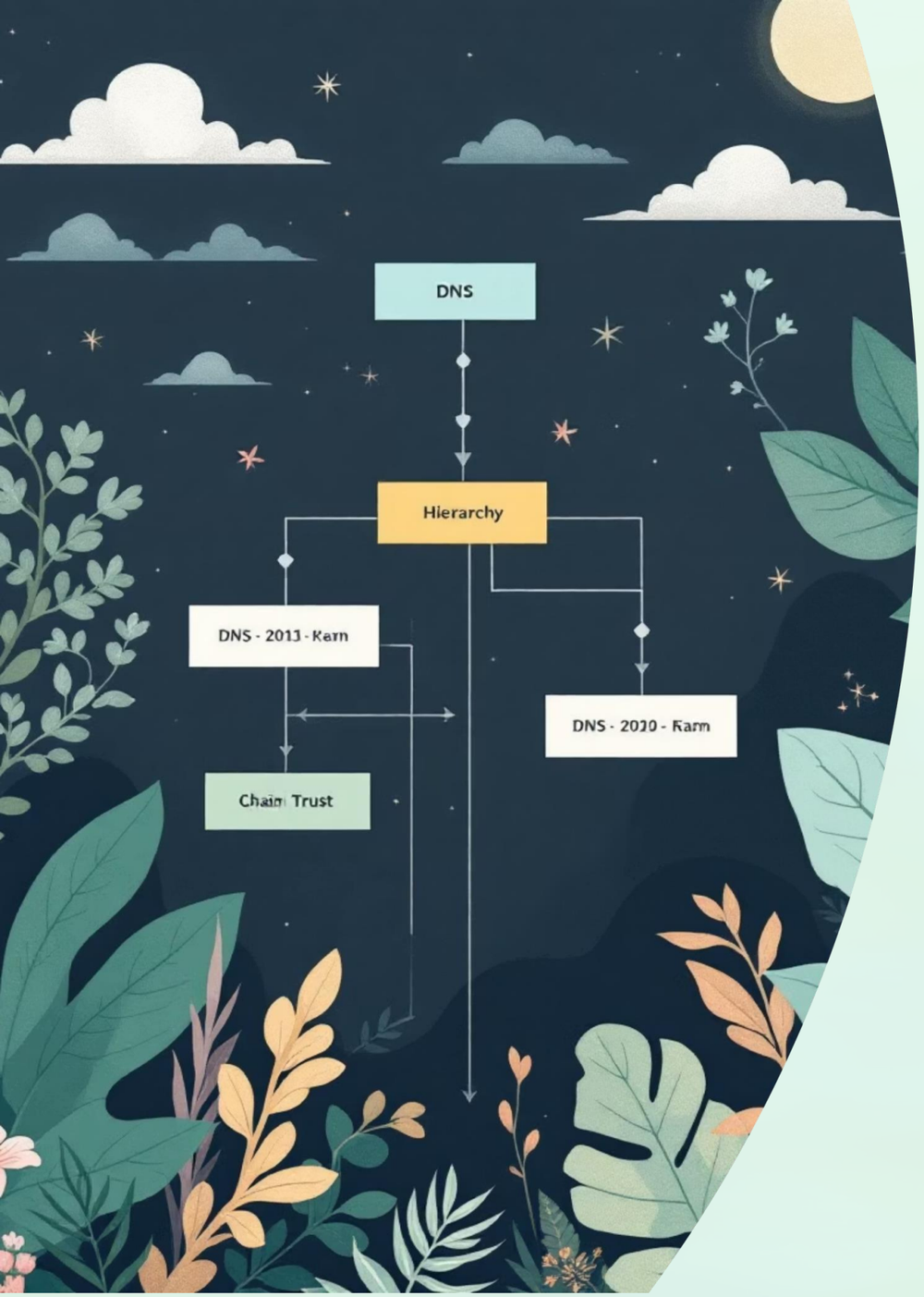
DNSSEC (**Domain Name System Security Extensions**) adds cryptographic signatures to DNS data.

Authentication Layer

It verifies that DNS responses are authentic and unaltered, preventing attackers from forging DNS information.

Digital Seal

Think of DNSSEC as a digital seal of authenticity on every DNS answer.



How DNSSEC Works: The Chain of Trust

Dual Key System

DNSSEC uses two key types: Zone Signing Key (ZSK) signs DNS records; Key Signing Key (KSK) signs the ZSK.

Parent Validation

Each DNS zone's public key is validated by its parent zone via Delegation Signer (DS) records.

Hierarchical Trust

This creates a hierarchical chain of trust from the root zone down to individual domains.

Rejection Protocol

If any link in the chain is broken or invalid, DNS responses are rejected.

Visualizing DNSSEC: Before and After

Before DNSSEC

"Without DNSSEC (Unsecured DNS Resolution)"

Illustration idea:

A user → DNS Resolver → Attacker intercepting/forging → Fake Website.

*"**DNS responses not digitally signed - vulnerable to spoofing or cache poisoning.**"*

After DNSSEC

Title: "With DNSSEC (Validated and Secure DNS Resolution)"

Illustration idea:

A user → DNS Resolver (validates signature) → Authoritative Server → Legitimate Website.

*"**DNS responses are digitally signed - authenticity and integrity verified.**"*

Benefits of DNSSEC: Why It Matters

Attack Prevention

Protects users from DNS spoofing and cache poisoning attacks.

Enhanced Trust

Enhances overall internet security and user trust.

Critical Services

Critical for safeguarding sensitive services like banking, email, and government websites.

Standards Compliance

Supports compliance with modern cybersecurity standards.

Challenges in DNSSEC Implementation

Technical Complexity

Requires managing cryptographic keys, signing zones, and maintaining chain of trust.

Key Management Burden

Secure storage, regular rotation, and backup of keys are critical but error-prone processes.

Compatibility Issues

Not all DNS resolvers support DNSSEC, risking access issues if misconfigured.

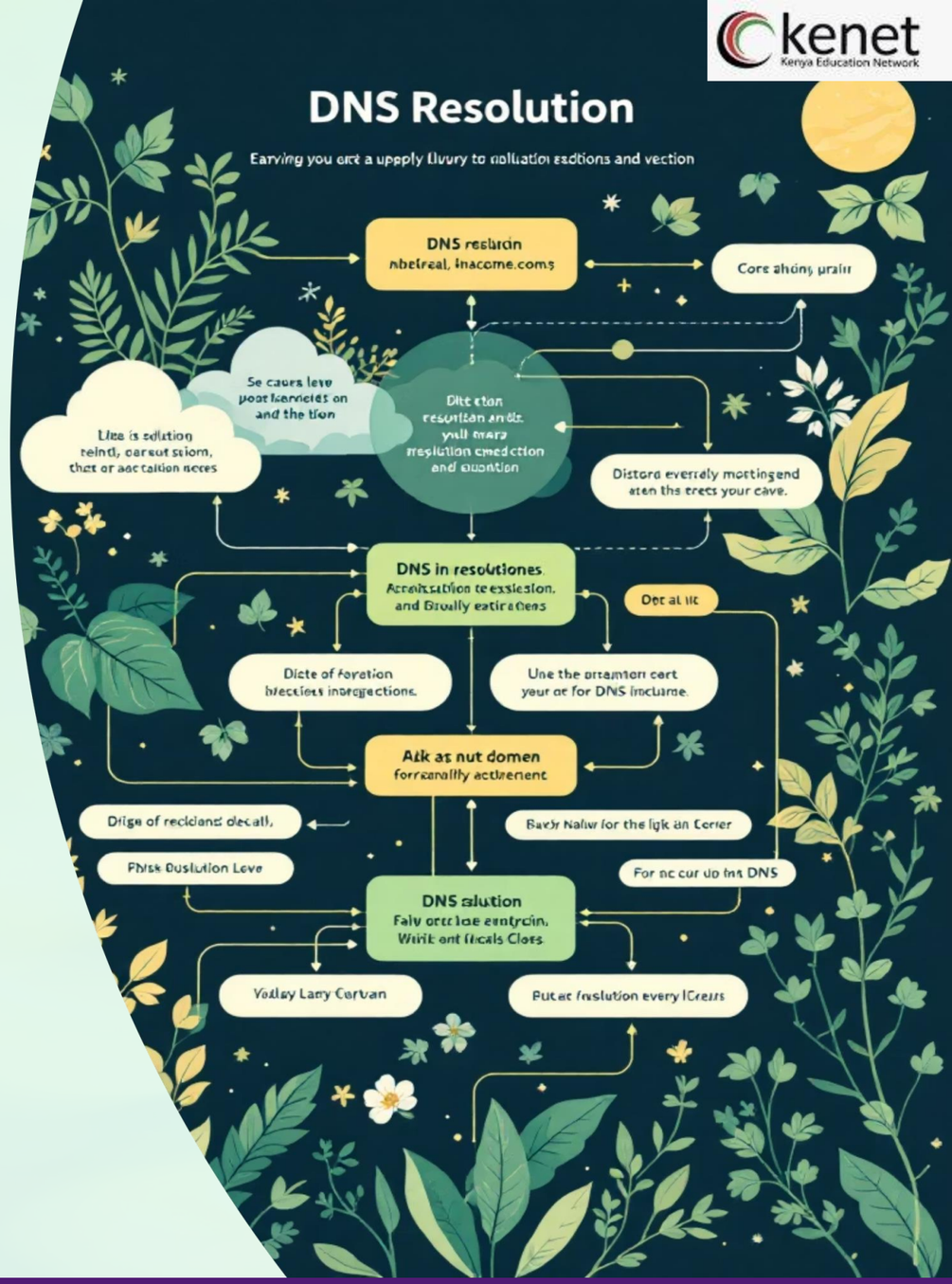
Resource Demands

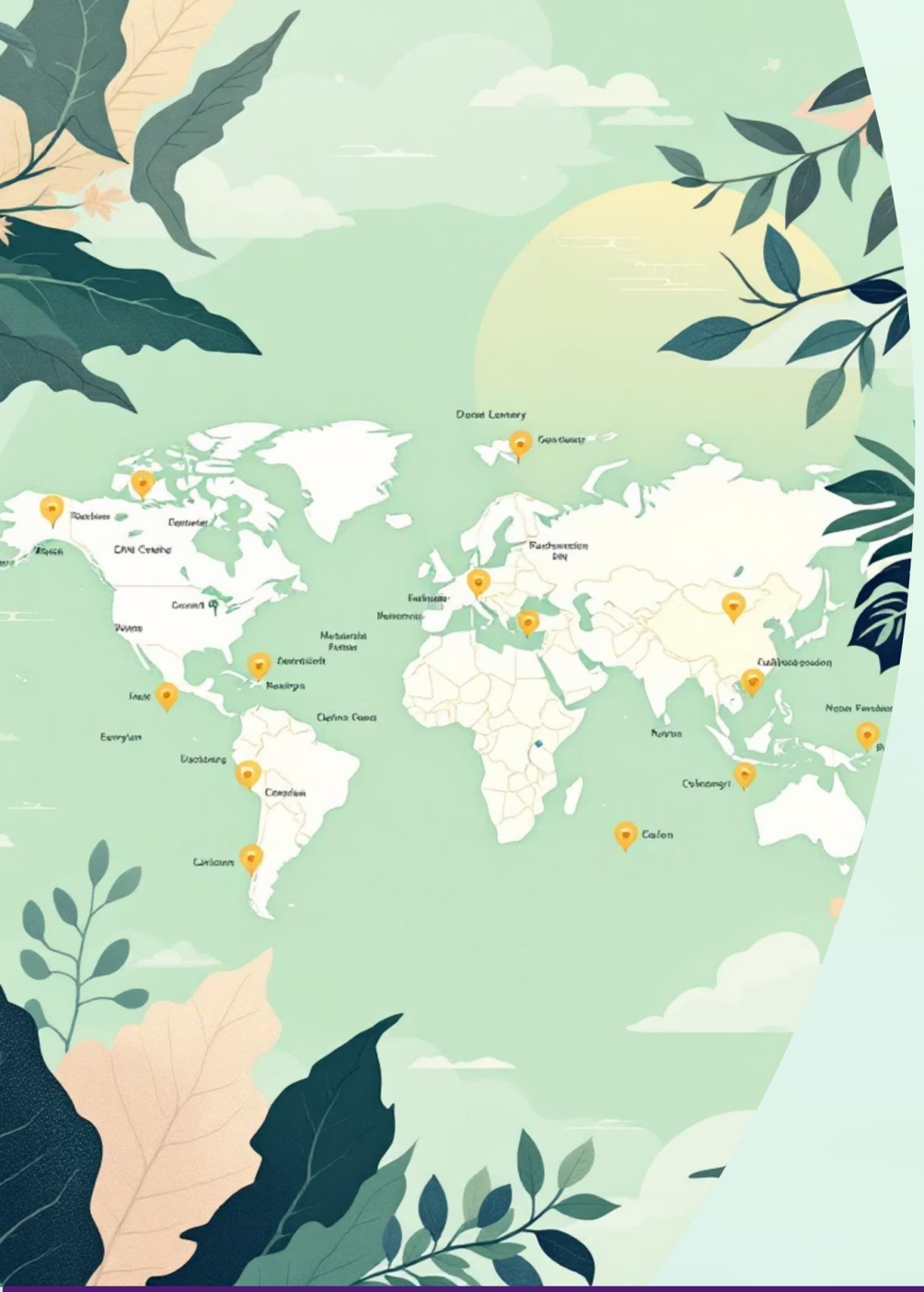
Larger DNS responses increase bandwidth and server load requirements.

Privacy Concerns

Potential exposure of subdomain information due to DNSSEC's proof-of-nonexistence records.

Overview of Threats to DNS Security and Mitigation Strategies





Real-World Impact: Lessons from Past Attacks

1

2011 Brazil Attack

DNS poisoning redirected users to fake banking sites, causing widespread financial fraud across multiple institutions.

2

2018 DNSpionage Campaign

Sophisticated attack hijacked DNS to spy on government and private sectors, compromising sensitive data.

3

Prevention Power

DNSSEC adoption helps prevent such large-scale, damaging attacks from succeeding.

Overcoming Challenges: Best Practices

01

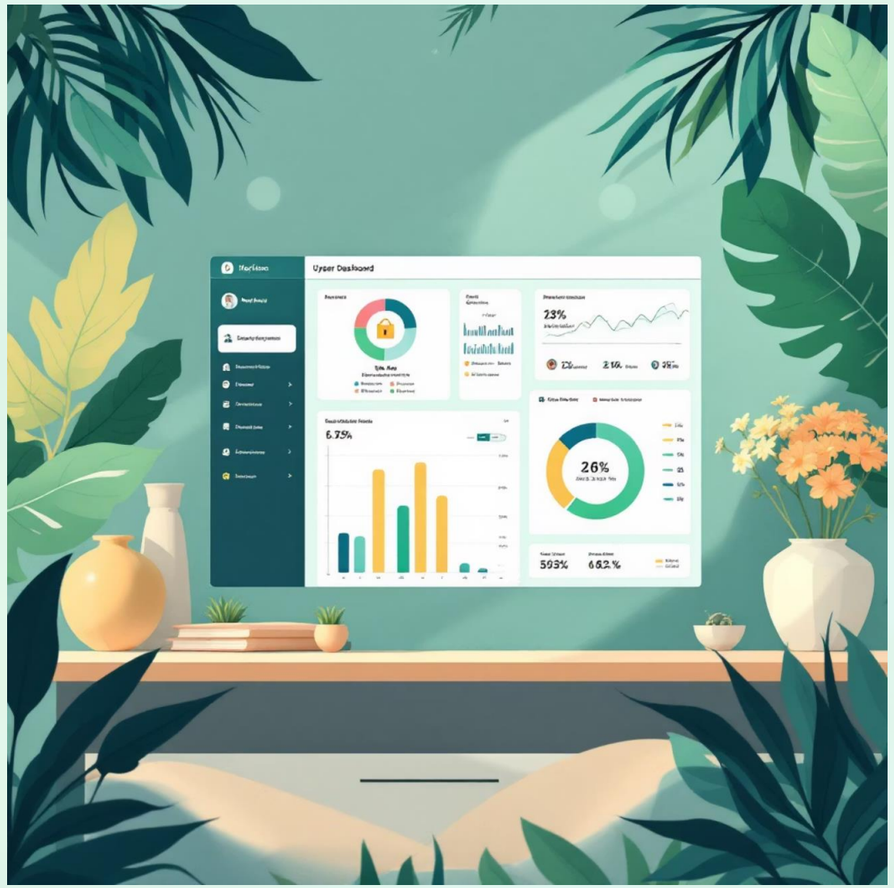
Managed Solutions

Use DNSSEC-aware tools and managed DNS providers to simplify key management.

02

Invest in Expertise

Train technical teams or hire experts familiar with DNSSEC implementation.



03

Test Thoroughly

Thoroughly test DNSSEC deployment to avoid user disruptions.

04

Automate Key Management

Monitor and rotate keys regularly with automation to reduce errors.

05

Balance Security & Privacy

Balance security needs with privacy concerns about zone data exposure.

Common DNS Attacks & Their Impact

1

DNS Spoofing/Cache Poisoning

Maliciously corrupts DNS cache records to redirect unsuspecting users to fraudulent websites that steal credentials or install malware, compromising user safety and data integrity.

2

DDoS & Amplification Attacks

Overwhelms DNS servers with massive traffic volumes using amplification techniques, causing widespread service outages and rendering websites completely inaccessible to legitimate users.

3

DNS Tunneling

Exploits DNS queries as covert communication channels to secretly exfiltrate sensitive data from compromised networks or maintain persistent control over infected systems.

4

DNS Hijacking

Systematically alters DNS configuration settings to redirect all traffic to attacker-controlled servers, enabling large-scale data interception and service manipulation.

DNS Spoofing: The Cache Poisoning Attack

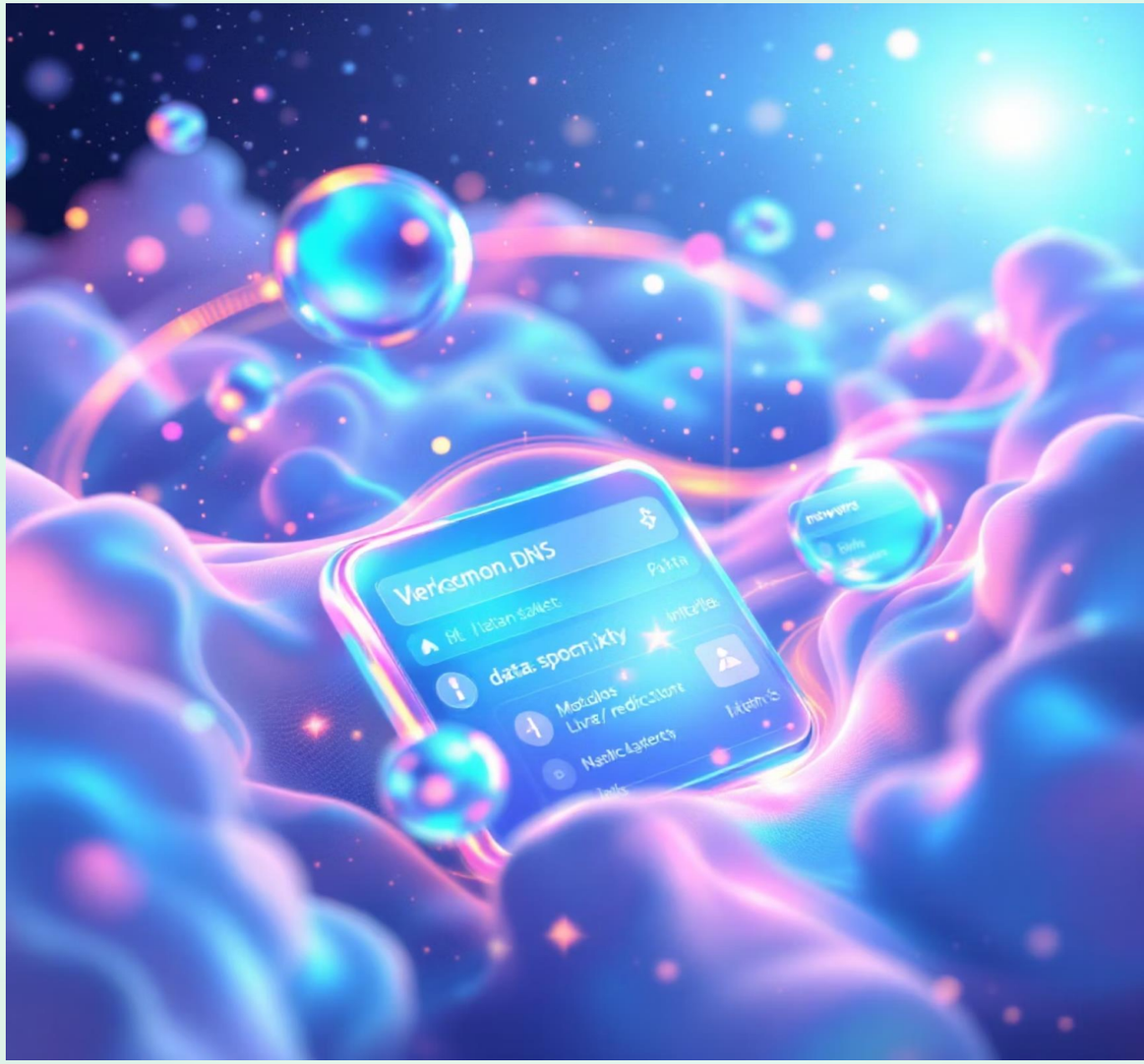
How It Works

Hackers inject false information into DNS resolver cache, redirecting users to malicious websites instead of legitimate ones.

- Exploits UDP protocol vulnerabilities
- Redirects traffic to hacker-controlled domains
- Used for phishing and malware distribution

Protection Methods

DNSSEC and HTTPS provide security layers requiring digital handshakes between servers.



DNS Tunneling: Bypassing Firewalls

Malware Infection

Hacker infects target device with tunneling malware

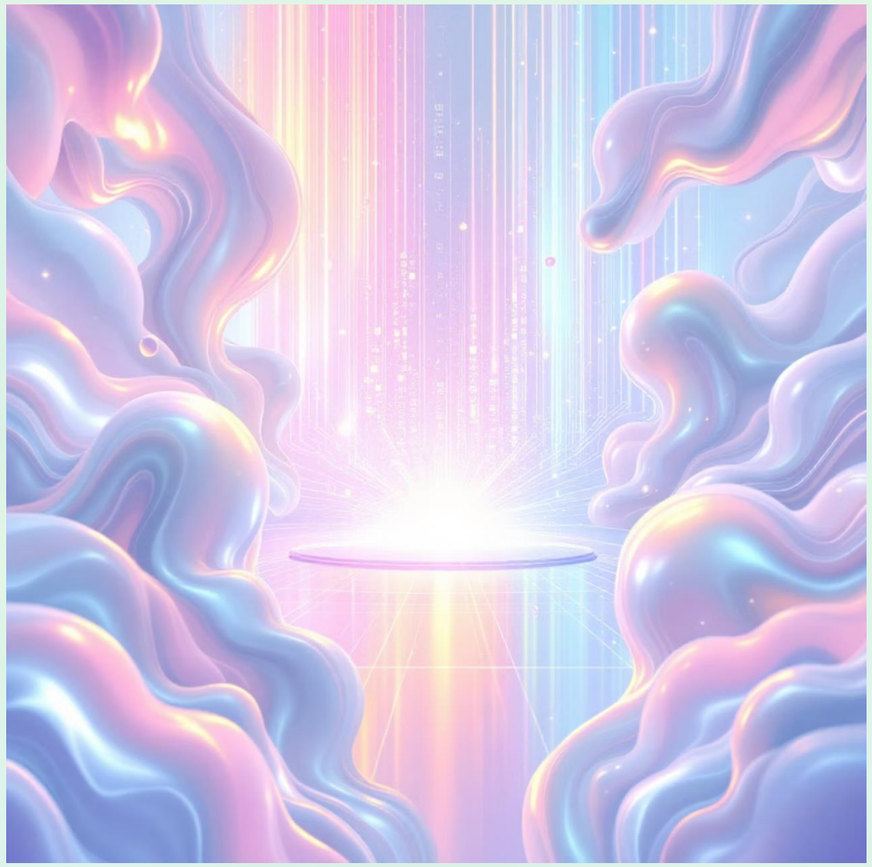
Tunnel Creation

Malware creates backchannel to hacker's domain

Data Exfiltration

Traffic routed through hacker's server for data theft

DNS Amplification: Weaponizing Responses



Attack Mechanism

Hackers send small queries using spoofed IP addresses, generating massive responses that overwhelm target servers.

⊗ **Impact:** Can take entire services offline by flooding them with DNS responses

Defense Strategy

Configure DNS resolvers to only serve trusted domains and implement rate limiting.

Additional DNS Attack Vectors

DNS Rebinding

Circumvents same-origin policy by manipulating TTL values to access internal networks

DNS Typosquatting

Registers common misspellings of popular domains to capture mistyped URLs

UDP Flooding

Overwhelms servers with UDP packets, using DNS defense systems against themselves

Advanced DNS Threats

1

Phantom Domain Attack

Sets up slow-responding DNS servers that delay responses, causing request pile-ups and service denial.

2

Random Subdomain Attack

Floods recursive servers with requests for randomly generated non-existent subdomains.

3

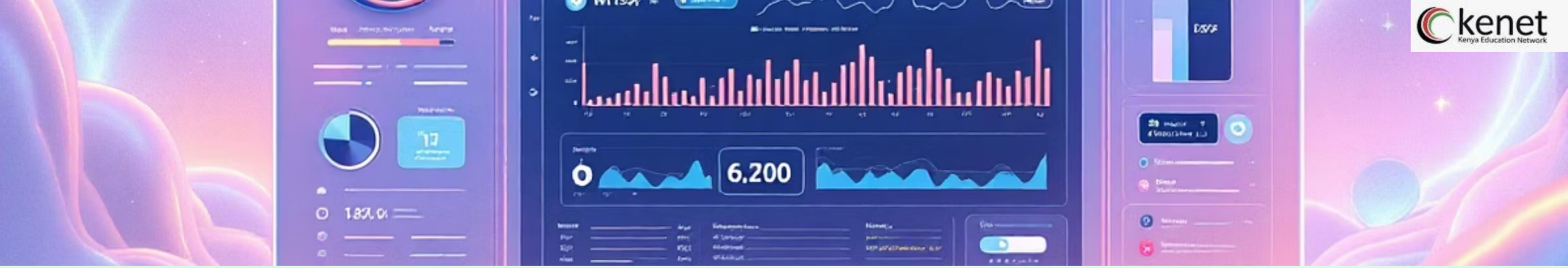
DNS Amplification

Exploits open DNS resolvers to magnify attack traffic volume toward targeted systems.

Advance DNS Security

DNS Security Measures

- **Rate Limiting & DDoS Protection:** Implementing measures to detect and mitigate large-scale DNS query floods targeting servers.
- **Anycast DNS:** Distributing DNS queries across multiple servers globally, improving redundancy, resilience, and reducing latency, which also aids in DDoS protection.
- **Regular Audits & Monitoring:** Continuously checking DNS configurations for vulnerabilities and monitoring for unusual activity.



Emerging DNS Security Technologies

DNS over HTTPS (DoH)

Encrypts DNS queries during transmission to prevent interception and manipulation by malicious actors.

1

AI-Powered Detection

Machine learning algorithms enable advanced anomaly detection and automated responses to DNS threats.

3

2

DNS over TLS (DoT)

Provides encrypted DNS communication while maintaining network visibility for security monitoring.

A Safer Internet

Foundation Strength

DNSSEC strengthens the foundation of internet security by ensuring DNS data integrity.

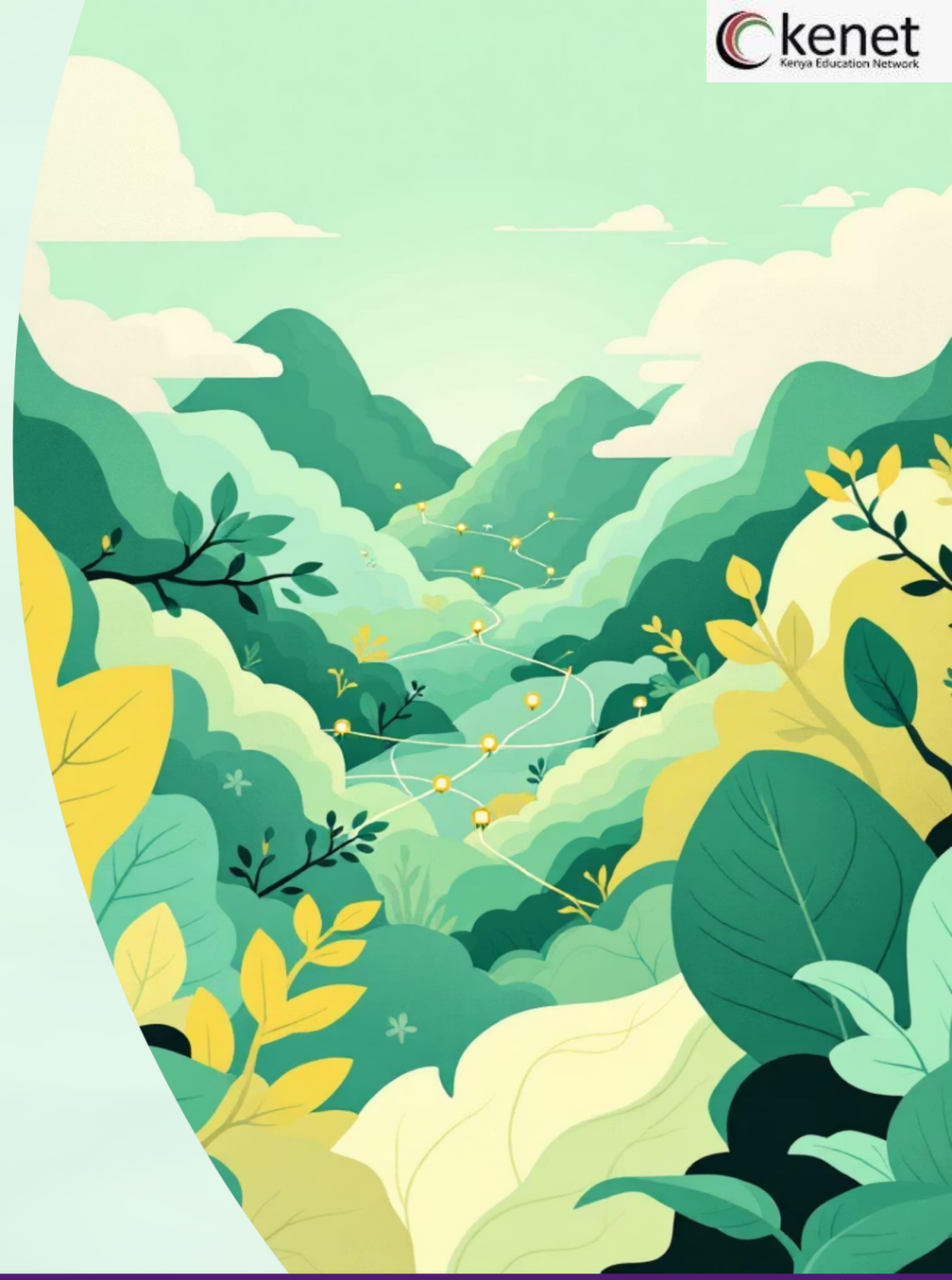
Strategic Investment

While implementation is complex, its benefits in preventing cyberattacks are indispensable.

Future Security

Organizations should prioritize DNSSEC adoption as part of their cybersecurity strategy to protect users and maintain trust.

> The future of a secure internet depends on securing its address book - DNSSEC is key.



Questions & Discussion