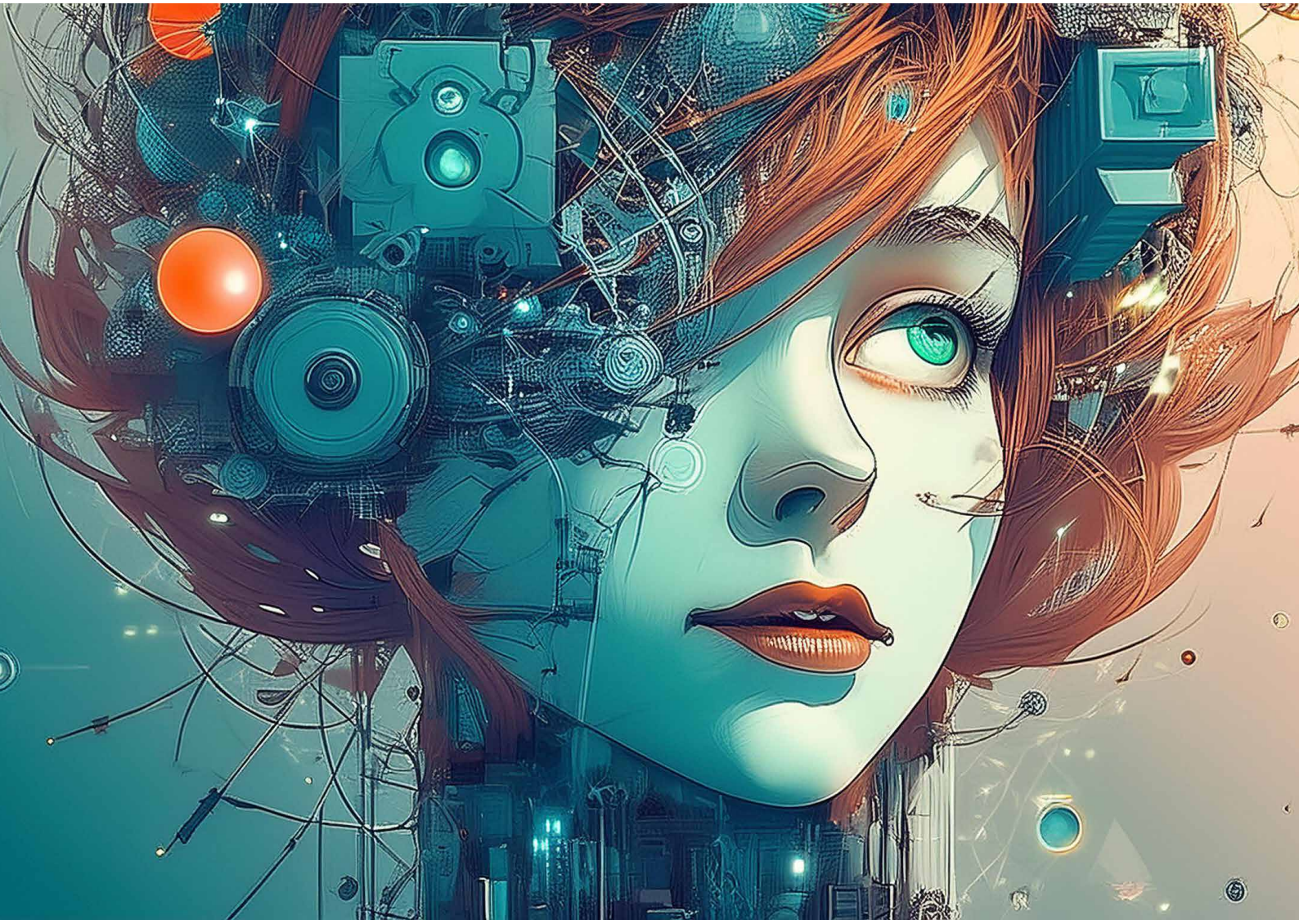
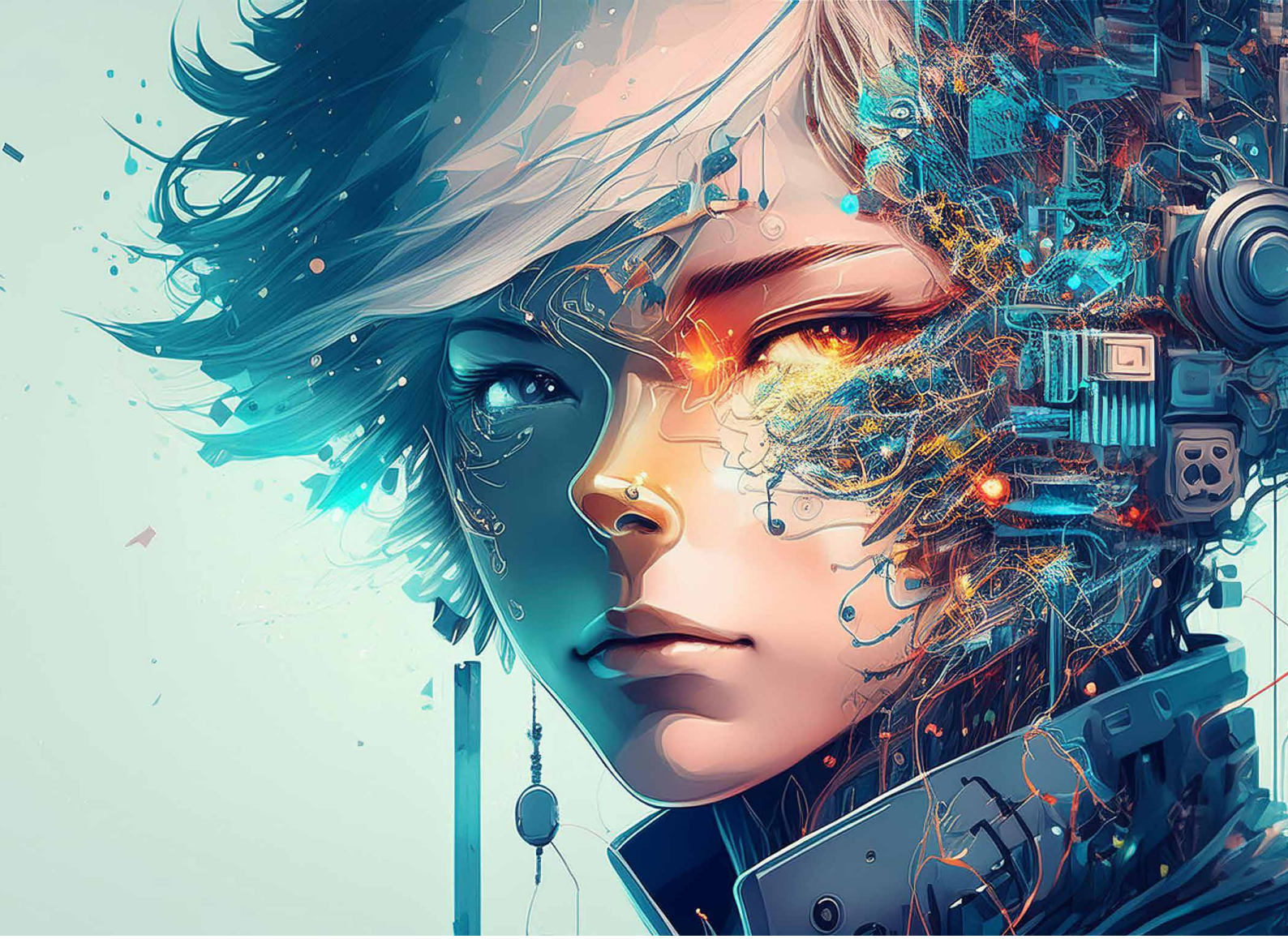
kaizen



The 6 pillars of IT that all businesses must have

A practical framework for modern businesses



In today's digital landscape, many businesses believe they have IT under control simply because they can fix problems as they arise, set up new devices and manage their cloud tenancy. However, this reactive approach often overlooks critical security and management practices that protect against modern cyber threats.

This white paper outlines the six essential pillars of IT that every business must have in place to ensure robust security, operational efficiency and business continuity. Understanding these fundamentals is the first step towards protecting your organisation from the evolving threat landscape.

1. Protect Your Network

The Foundation of IT Security

Your network is the gateway to your entire business infrastructure. Without proper protection, cybercriminals can easily penetrate your systems and access sensitive data.

Firewalls: Your First Line of Defence

A properly configured firewall acts as a barrier between your internal network and external threats. Modern firewalls go beyond simple packet filtering to provide:

- Application-level inspection and control
- Intrusion prevention systems (IPS)
- Advanced threat detection
- Content filtering and web security

Network Segmentation and Rules

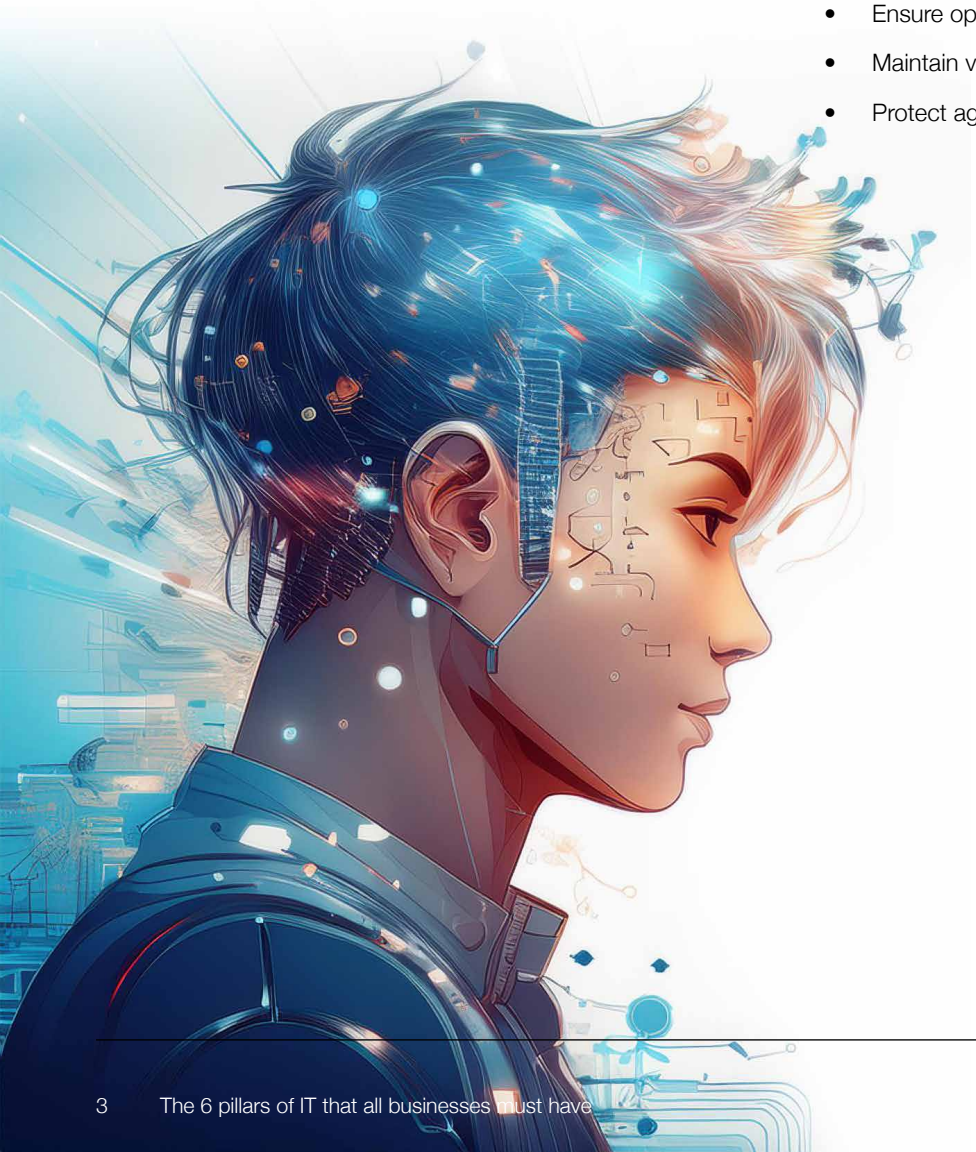
Implementing proper network rules and segmentation ensures that:

- Critical systems are isolated from general user access
- Lateral movement by attackers is restricted
- Compliance requirements are met
- Network traffic is monitored and controlled

Regular Patching: Closing Security Gaps

Cybercriminals actively exploit known vulnerabilities in network infrastructure. Regular patching of network devices, including routers, switches and firewalls, is essential to:

- Close security vulnerabilities before they can be exploited
- Ensure optimal performance and stability
- Maintain vendor support and compliance
- Protect against zero-day exploitscontrolled



2. Access Controls

Managing Who Can Access What

Access control is about ensuring the right people have access to the right resources at the right time and preventing everyone else from accessing them.

Identity Management

Modern identity management systems provide centralised control over user identities, ensuring that:

- User accounts are properly provisioned and deprovisioned
- Identity verification is strong and consistent
- User lifecycle management is automated
- Audit trails are maintained for compliance

Access Privilege and Least Privilege Principle

Implementing the principle of least privilege means users only have access to the resources they need to perform their job functions:

- Reduces the attack surface
- Limits damage from compromised accounts
- Prevents accidental data modification or deletion
- Supports compliance with data protection regulations

Conditional Access Policies

Conditional access adds context-aware security by evaluating factors such as:

- User location and device health
- Time of access and risk level
- Application sensitivity
- Network location

Multi-Factor Authentication (MFA/2FA)

Passwords alone are no longer sufficient. Multi-factor authentication requires users to provide additional verification, such as:

- Something they know (password)
- Something they have (phone or token)
- Something they are (biometrics)

This dramatically reduces the risk of account compromise, even if passwords are stolen.

Single Sign-On (SSO)

SSO improves both security and user experience by:

- Reducing password fatigue and poor password practices
- Centralising authentication management
- Simplifying user onboarding and off-boarding
- Providing comprehensive access logging

Data Leakage Prevention

Protecting sensitive data from unauthorised disclosure requires:

- Data classification and labelling
- Monitoring and controlling data movement
- Encryption of data at rest and in transit
- Policy enforcement across all endpoints and channels

3. Manage Your Vulnerabilities

Proactive Security Management

Vulnerability management is about identifying, assessing and remediating security weaknesses before they can be exploited.

Operating System Patching

Unpatched operating systems are one of the most common entry points for cyberattacks. A robust OS patching programme includes:

- Regular scanning for available updates
- Testing patches before deployment
- Automated patch deployment where possible
- Tracking and reporting on patch compliance

Third-Party Application Patching

Many breaches occur through vulnerabilities in third-party applications. Effective third-party patching involves:

- Maintaining an inventory of all installed applications
- Monitoring vendor security bulletins
- Prioritising patches based on risk
- Automating updates where feasible

Restriction of Administrative Accounts

Administrative accounts have elevated privileges that, if compromised, can lead to complete system takeover. Best practices include:

- Limiting the number of users with administrative access
- Using separate accounts for administrative tasks
- Implementing just-in-time (JIT) administrative access
- Monitoring and auditing all administrative activities

Antivirus and Endpoint Protection

Modern antivirus solutions go beyond signature-based detection to include:

- Behavioural analysis and machine learning
- Exploit prevention and ransomware protection
- Endpoint detection and response (EDR)
- Automated threat remediation

Vulnerability Scanning and Assessment

Regular vulnerability assessments help identify weaknesses before attackers do:

- Automated scanning of networks and systems
- Risk-based prioritisation of findings
- Tracking remediation progress
- Validation of security controls

4. Your Team Are Your Firewall

Building a Human Security Layer

Technology alone cannot prevent all security incidents. Your employees are both your greatest vulnerability and your strongest defence against cyber threats.

Security Awareness Training

Regular security awareness training ensures employees understand:

- Common cyber threats and attack vectors
- How to recognise suspicious emails and links
- Best practices for password management
- The importance of reporting security incidents
- Company security policies and procedures

Phishing Simulation

Phishing remains one of the most effective attack methods. Regular phishing simulations:

- Test employee awareness in a safe environment
- Identify individuals who need additional training
- Measure the effectiveness of security awareness programmes
- Reinforce training through real-world scenarios

Creating a Security-Conscious Culture

Building a culture of security involves:

- Leadership commitment to security initiatives
- Open communication about security threats and incidents
- Recognition and rewards for good security practices
- Making security everyone's responsibility

Incident Reporting Procedures

Employees need clear, simple procedures for reporting security concerns:

- Easy-to-remember reporting channels
- No-blame culture that encourages reporting
- Quick response and feedback to reporters
- Regular communication about reported incidents (where appropriate)

5. Hackers Never Sleep

24/7 Security Monitoring and Response

Cyber threats don't operate on business hours. Attacks can happen at any time and delayed detection can mean the difference between a minor incident and a catastrophic breach.

Security Operations Centre (SOC)

A 24/7 SOC provides continuous monitoring and response capabilities:

- Real-time threat detection and analysis
- Immediate response to security incidents
- Expert security analysts available around the clock
- Coordination of incident response activities

Virus and Malware Detection

Advanced malware can evade traditional antivirus solutions. Modern threat detection includes:

- Behaviour-based detection of unknown threats
- Sandboxing of suspicious files
- Integration of threat intelligence feeds
- Automated containment and remediation

Unusual Behaviour Detection

Security Information and Event Management (SIEM) systems identify anomalies that may indicate a breach:

- Unusual login patterns or times
- Abnormal data access or transfer
- Suspicious process execution
- Changes to critical system files

Impossible Travel Detection

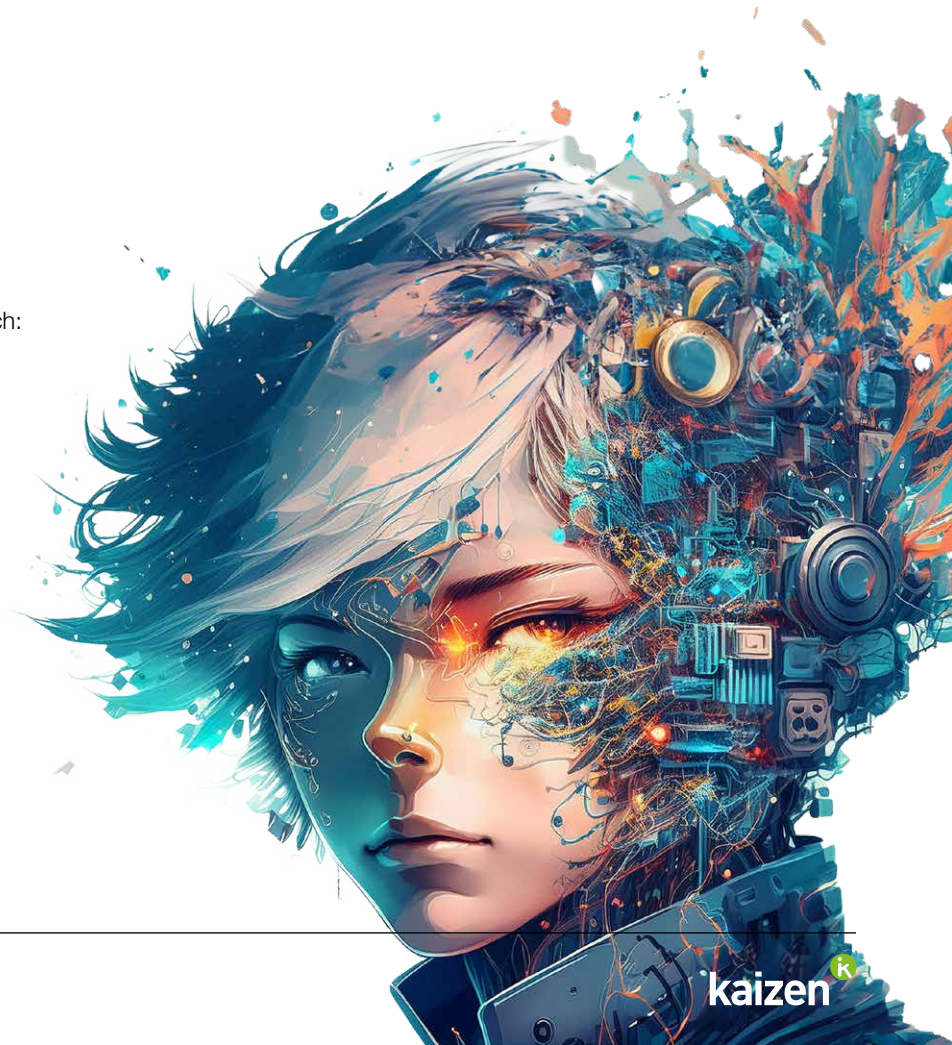
Impossible travel alerts identify when accounts are accessed from geographically distant locations within an implausible timeframe:

- Indicates potential account compromise
- Triggers immediate security response
- Helps identify credential theft
- Protects against distributed attack patterns

Incident Response and Remediation

When threats are detected, rapid response is critical:

- Automated containment of affected systems
- Expert-led investigation and analysis
- Coordinated remediation efforts
- Post-incident review and improvement



6. Backups and Recovery

Your Safety Net When Things Go Wrong

Even with strong security controls, incidents happen. Mistakes get made, devices fail, files are deleted, and ransomware can encrypt data in minutes. Reliable backups and a tested recovery process are what turn a potential disaster into a short interruption.

Backups Are Not the Same as “Sync”

Cloud sync tools are useful, but they are not designed to protect you from:

- Accidental deletion and overwrite
- Ransomware encryption syncing across devices
- A compromised account making bulk changes
- Retention limits and missing historical versions

The 3-2-1 Rule (A Simple Standard)

A strong baseline approach is:

- **3 copies** of your critical data
- **2 different storage types** (for example, cloud and immutable storage)
- **1 copy kept offsite** and protected from your main environment

Recovery Objectives: RPO and RTO

Backups only matter if they meet the business need:

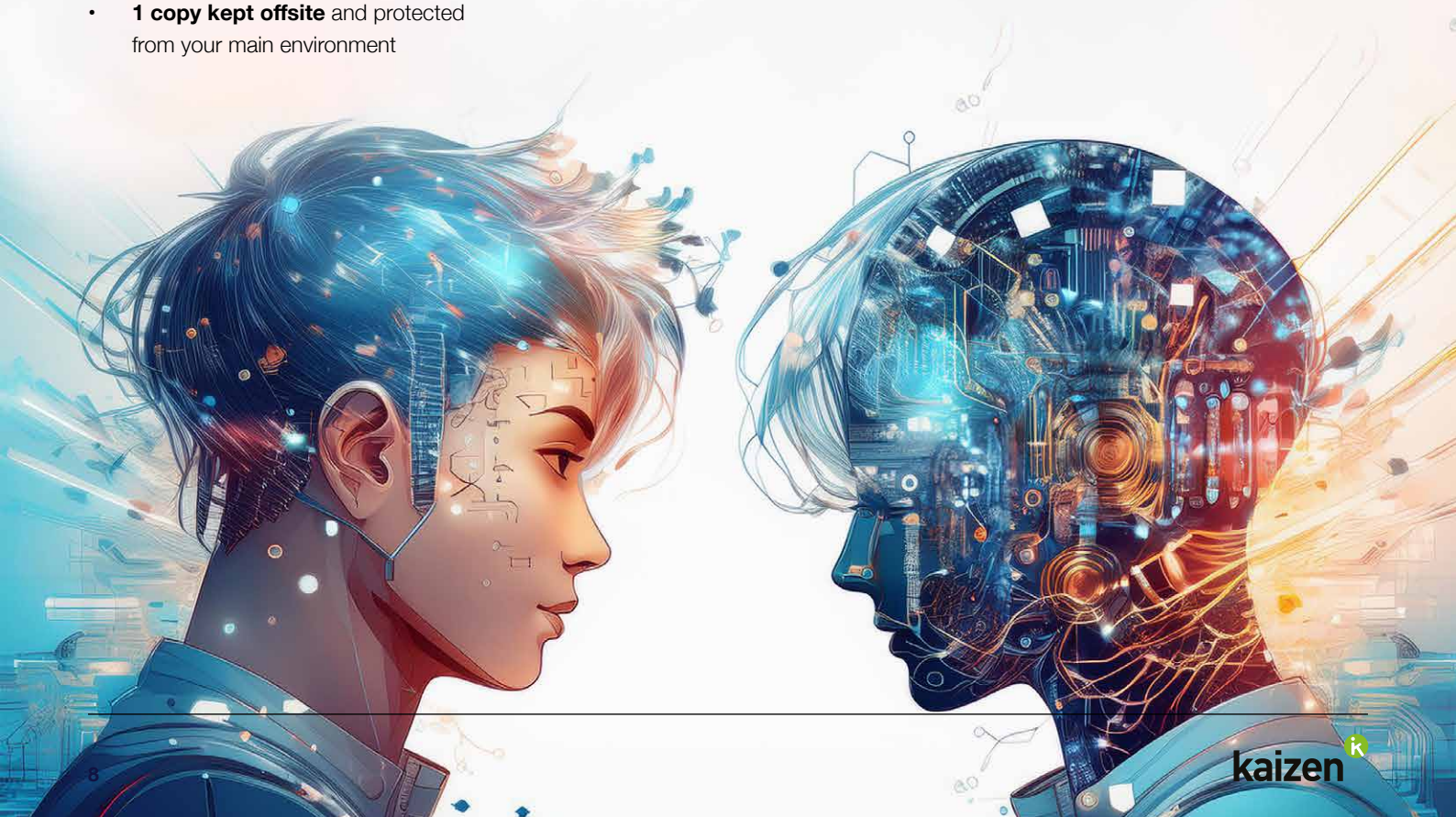
- **RPO (Recovery Point Objective):** How much data you can afford to lose
- **RTO (Recovery Time Objective):** How quickly you need systems back online

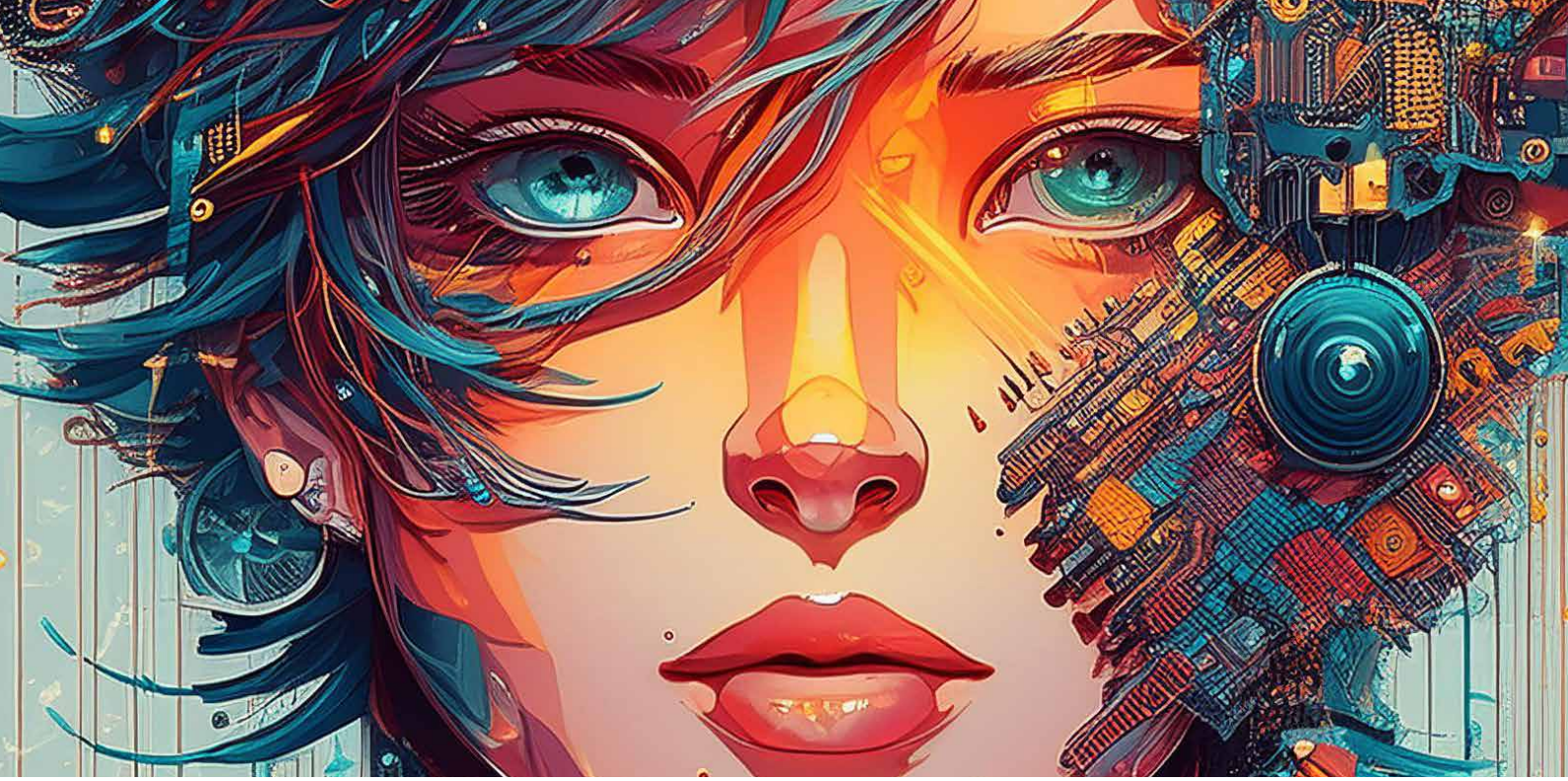
Defining these upfront ensures your backup plan matches the reality of your operations.

Test Restores and Document the Process

A backup you have never restored from is an assumption. Best practice includes:

- Scheduled restore testing
- Clear ownership and runbooks
- Regular reporting, alerts and audit trails
- Separation of backup admin access from everyday accounts





Conclusion

Managing IT in-house is more than just fixing problems and setting up new devices. True IT management requires a comprehensive approach that addresses network security, access controls, vulnerability management, user awareness, continuous monitoring and reliable backups.

Many businesses operate with significant security gaps simply because they don't know what they don't know. Understanding these six pillars is the first step towards assessing your organisation's IT maturity and identifying areas where you may be exposed to risk.

The question isn't whether your business can afford to implement these pillars but whether you can afford not to. In today's threat landscape, a single security incident can result in significant financial losses, reputational damage and regulatory penalties.

Next Steps

If you're uncertain about where your organisation stands in relation to these six pillars, consider:

1. Conducting a comprehensive IT security assessment
2. Reviewing your current policies and procedures
3. Engaging with experienced IT security professionals
4. Developing a roadmap to address identified gaps
5. Validating your backup and recovery capabilities with restore testing
6. Investing in ongoing security monitoring and continuous improvement

Your IT infrastructure is too important to leave to chance. Take the time to understand where you stand and what steps you need to take to protect your business, your data and your reputation.

How Kaizen IT Can Help

Your Partner in IT Excellence

At Kaizen IT, we understand that implementing and maintaining these six pillars can be overwhelming, especially for businesses without dedicated IT security teams. That's where we come in.

Comprehensive IT Security Solutions

We provide end-to-end IT security services that cover all six pillars:

- **Network Protection:** We design, implement and manage robust network security solutions tailored to your business needs
- **Identity and Access Management:** Our experts configure and maintain advanced IAM systems, including MFA, SSO and conditional access policies
- **Vulnerability Management:** We provide proactive patch management, vulnerability scanning and endpoint protection services
- **Security Awareness Training:** Our engaging training programmes and phishing simulations turn your team into a strong security layer
- **24/7 Security Monitoring:** Our Security Operations Centre provides round-the-clock threat detection and rapid incident response
- **Backup and Recovery:** We design, implement and manage resilient backup solutions, define RPO/RTO targets, and run regular restore tests so you can recover quickly and confidently

Why Choose Kaizen IT?

- **Expertise:** Our team of certified security professionals stays ahead of emerging threats and best practices
- **Proactive Approach:** We focus on reducing issues through preventative best practices, regular monitoring and continuous improvement
- **Scalable Solutions:** Our services grow with your business, adapting to your changing needs
- **Peace of Mind:** Focus on your core business while we handle the complexities of IT security

Get Started Today

Ready to assess your IT security posture and discover how we can help protect your business? Contact Kaizen IT today for a complimentary security consultation. We'll help you understand where you stand and create a roadmap to achieve robust IT security across all six pillars.

Book a free online consultation with our team today.

Call 0345 141 1400 or email hello@kaizenit.co.uk

Sheffield
The Courthouse,
2 to 6 Townend Road,
Sheffield, S35 9YY

London
Kings Cross Business Centre,
180 to 186 Kings Cross Road,
London, WC1X 9DE

kaizenit.co.uk
0345 141 1400
hello@kaizenit.co.uk

Premium Technical Partner | CERTIFIED RESELLER | Microsoft Partner | ISO/IEC 27001:2022 | ISO 9001:2015