Essential Cloud & Web Security Checklist

How to Use This Checklist

This checklist helps businesses identify crucial security measures for their cloud and web presence. Each item includes:

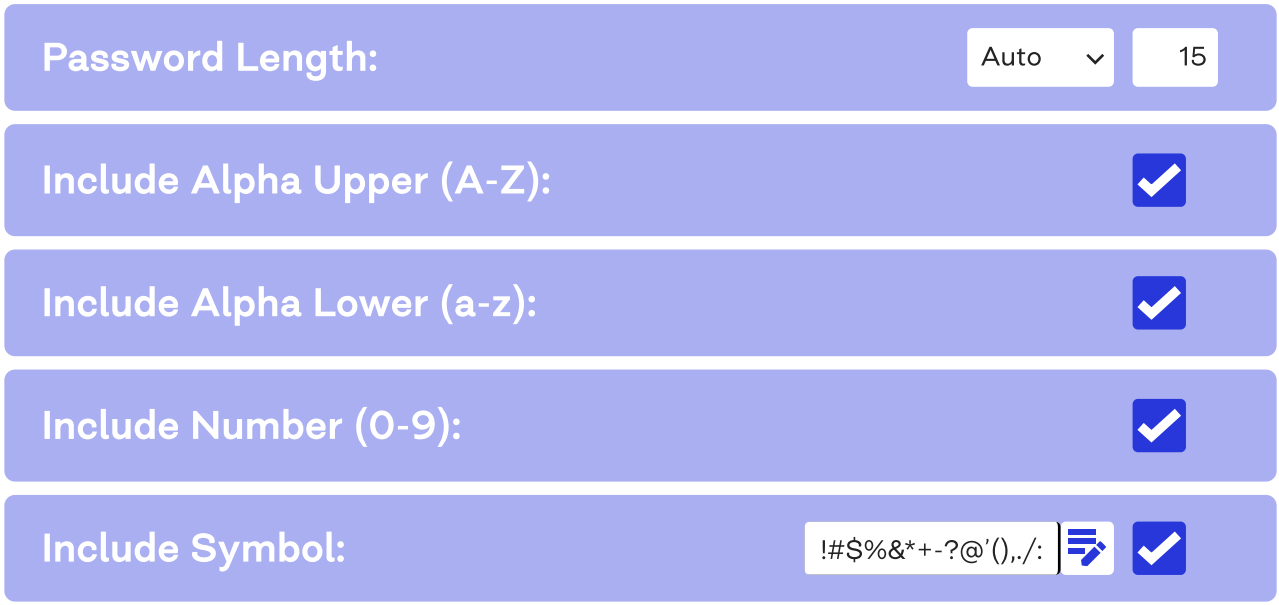
- **Business importance**
- **Potential impact if not addressed**
- **Estimated cost level** (💰 Low, 💰💰 Medium, 💰💰💰 High)
- **Implementation expertise** (🏢 In-house possible, 🤝 External help recommended)

1. Account & Access Security

Strong Password Policy

Why It Matters: Prevents unauthorized access to your business systems
Business Impact: Account breaches can lead to data theft and business disruption
Cost: 💰 Low
Expertise: 🏢 In-house possible

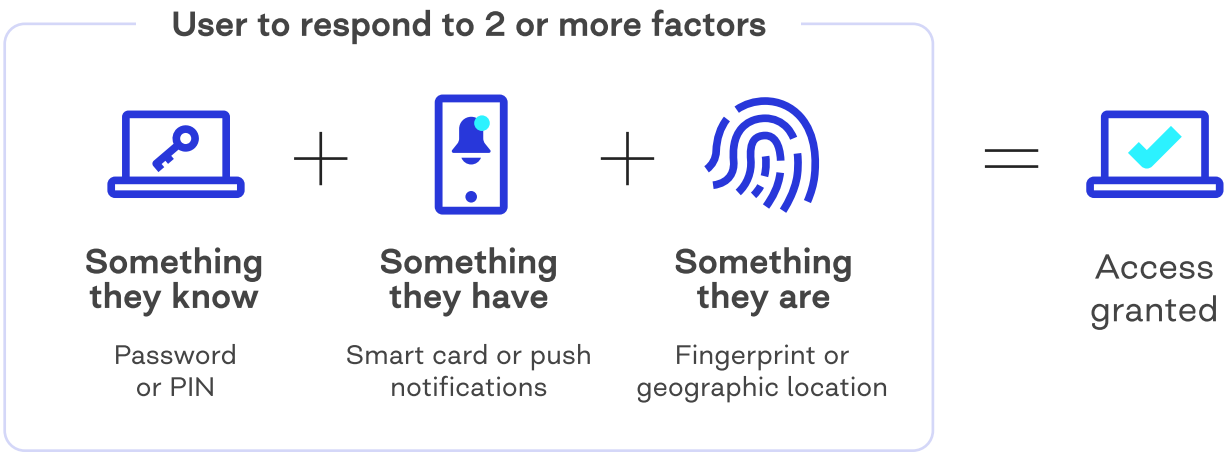
- Implement minimum password requirements
- Regular password changes
- Unique passwords for different services



Multi-Factor Authentication (MFA)

Why It Matters: Adds an extra layer of security even if passwords are compromised
Business Impact: Prevents unauthorized access even if credentials are stolen
Cost: 💰 Low
Expertise: 🏢 In-house possible

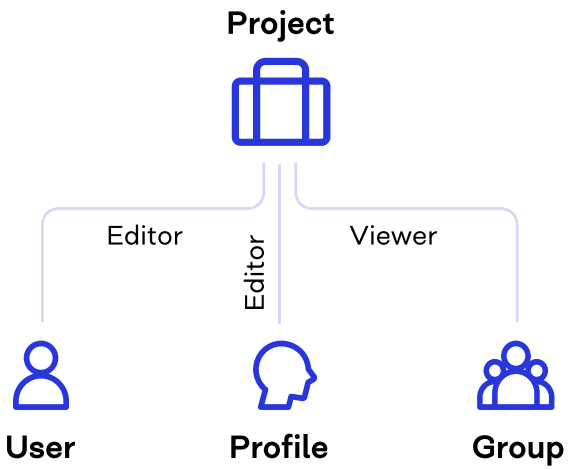
- Enable MFA for all cloud service accounts
- Enable MFA for employee email accounts
- Enable MFA for admin access to websites

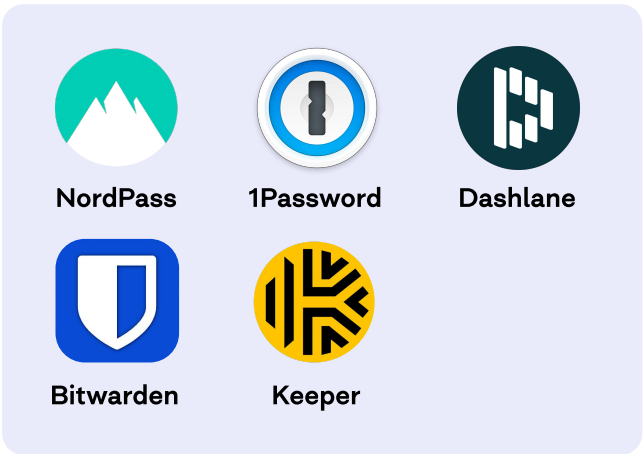


Access Management

Why It Matters: Ensures employees only access what they need for their work
Business Impact: Reduces risk of internal data breaches and accidents
Cost: 💰💰 Medium
Expertise: 🤝 External help recommended

- Define employee access levels
- Regular access review process
- Monitor unusual access patterns





Real-World Impact Examples:

- **SolarWinds (2020):** Weak MFA implementation contributed to a major supply chain attack
- **Twitter (2020):** High-profile accounts, including Apple, Uber, and Bill Gates, were compromised through the social engineering of employees with administrative access.
- **Facebook (2021):** Data of 533 million users exposed due to insufficient access controls.
- **Colonial Pipeline (2021):** The ransomware attack succeeded through a compromised VPN account that only required single-factor authentication.
- **Uber (2022):** Hackers gained admin access through stolen credentials and lack of MFA.

Statistics:

- Microsoft reports that over 99.9% of compromised accounts don't use MFA.
- 80% of breaches involved identity as a key component. (Duo by Cisco)

2. Cloud Infrastructure Security

Cloud Accounts Security

Why It Matters: Protects your business's cloud-based operations and data
Business Impact: Prevents unauthorized charges and data exposure
Cost: 💰 Low
Expertise: 🤝 External help recommended

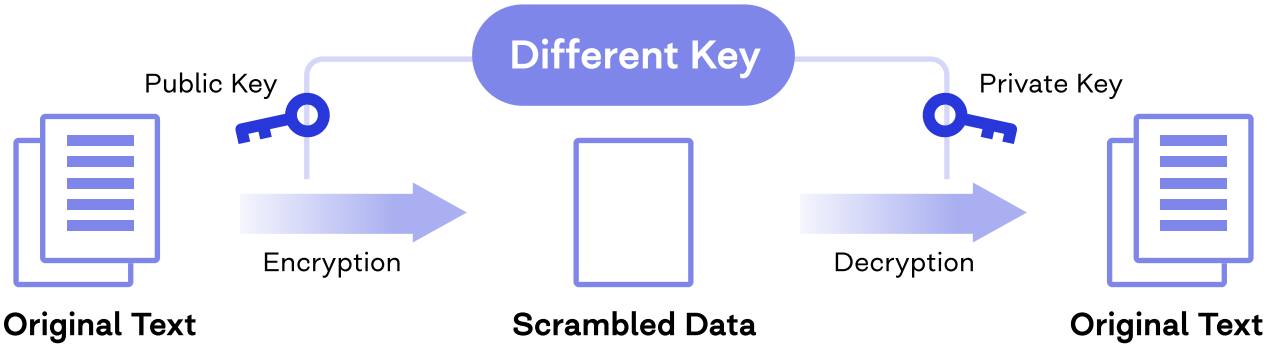
- Review cloud service security settings
- Monitor unusual usage patterns
- Set up billing alerts

Cloud Data Security

Why It Matters: Ensures business continuity in case of data loss or system failure
Business Impact: Protects sensitive business data loss
Cost: 💰💰 Medium
Expertise: 🤝 External help recommended

- Regular data backup schedule
- Encrypt sensitive data
- Regular permission audits

Data encryption

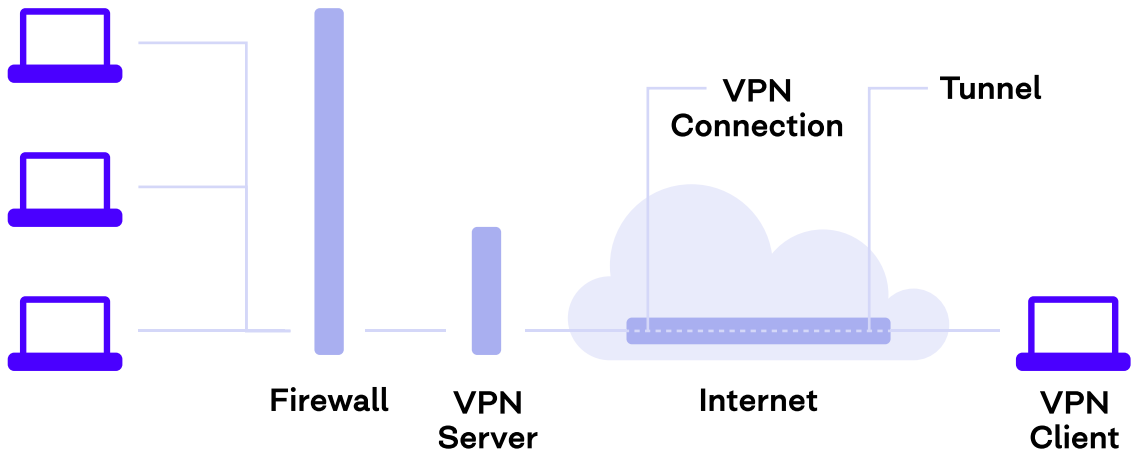


Cloud Network Protection

Why It Matters: Protects your business network from unauthorized access and attacks

Business Impact: Prevents network breaches and maintains business operations
Cost: 💰💰 Medium
Expertise: 🤝 External help recommended

- Firewall and VPN configuration
- Network monitoring
- Regular access scans
- Network segmentation



Real-World Impact Examples:

- **AT&T Data Breach Involving Snowflake Cloud Platform (2024):** Compromised data resulted from customers not adequately securing their accounts.
- **DNA Diagnostics Center (2023):** Network intrusion exposing genetic data.
- **KidSecurity (2023):** User data compromised after the app failed to set password protection

Statistics:

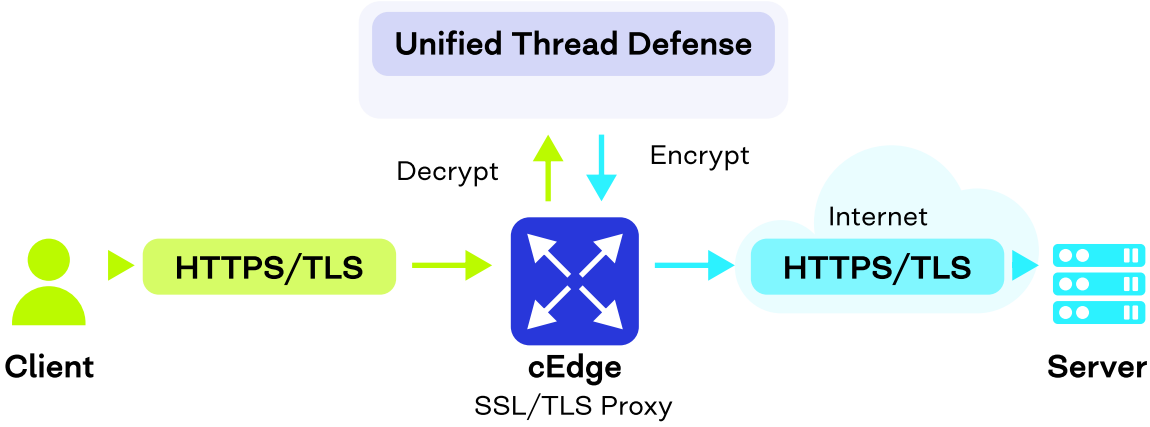
- There was a 75% increase in total cloud environment intrusions from 2022 to 2023. (Crowdstrike)
- 80% of companies have experienced at least one cloud security incident in the last year. (ExpertInsights)

3. Web Security

TLS Certificate

Why It Matters: Encrypts website traffic and shows visitors your site is secure
Business Impact: Builds customer trust and prevents data interception
Cost: 💰 Low
Expertise: 🏢 In-house possible

- Use the latest possible version of the TLS protocol
- Regular certificate renewal process
- Redirect HTTP to HTTPS



Website Software Updates

Why It Matters: Fixes security vulnerabilities in your website software
Business Impact: Prevents website hacks and defacement
Cost: 💰💰 Medium
Expertise: 🤝 External help recommended

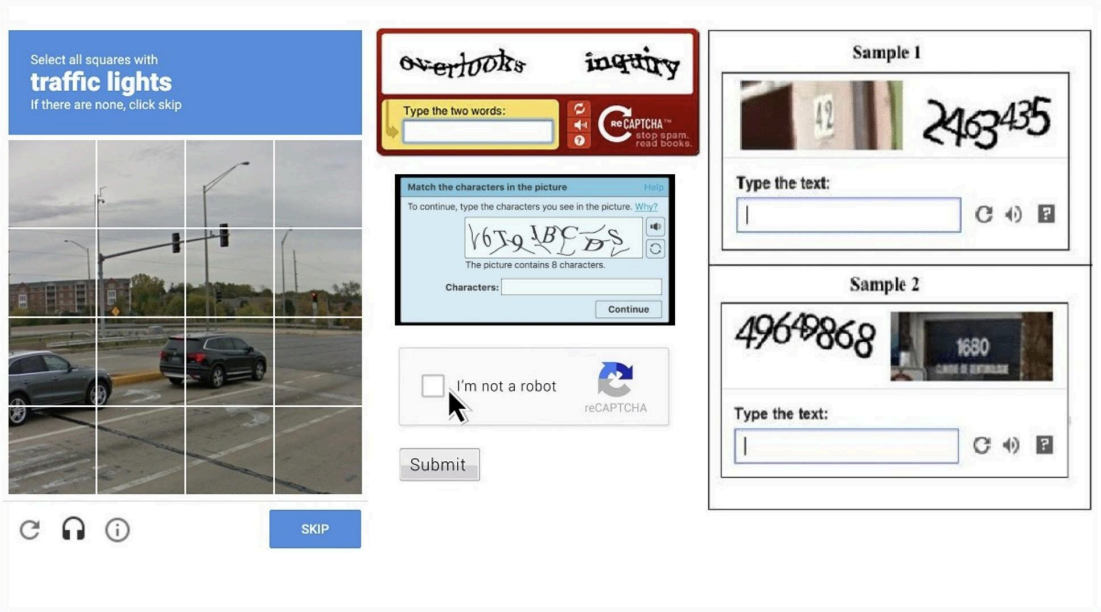
- Regular software updates
- Regular security scans
- Automated update notifications

Form & Input Security

Why It Matters: Prevents abuse of your website's interactive features
Business Impact: Prevents spam and malicious submissions
Cost: 💰💰 Medium
Expertise: 🤝 External help recommended

- CAPTCHA on forms
- Input validation
- File upload restrictions

Types of CAPTCHA

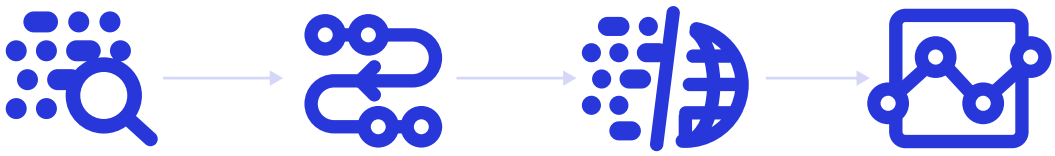


DDoS Protection

Why It Matters: Prevents attackers from overwhelming and crashing your online services
Business Impact: Maintains business continuity and prevents revenue loss from downtime
Cost: 💰💰 Medium to 💰💰💰 High
Expertise: 🤝 External help recommended

- DDoS mitigation measures
- Traffic monitoring
- Incident response plan for DDoS attacks

DDoS Mitigation Stages



Detection
Abnormal traffic flows are identifird

Diversion
Traffic is redicrected (BGPqDNS rounting

Filtering
DDos traffic is weeded out while clean traffic is passed on

Analysis
Security logs are used to improve resilience

Real-World Impact Examples:

- **TLS Bootstrap Attack on Azure Kubernetes Clusters (2024):** Gain access to all secrets used by running workloads.
- **WordPress Breaches (2024):** Multiple issues with WordPress and Plugins.
- **Meta (2024):** Form submission vulnerability allowing account takeover.

Statistics:

- Based on an analysis of 7 million websites, SiteLock reports that websites currently experience an average of 94 attacks every day.
- DDoS attacks spiked in 2024, with Netscout reporting approximately 8 million DDoS attacks in the first half of 2024 -13% up compared to the previous six months.

What To Do Next?

1. Review each item in this checklist.
2. Prioritize based on your business needs and risks.
3. Consult with IT professionals for complex items.
4. Schedule regular security reviews.

Contact COAX security experts to get a free cloud and web security review.