

# RANSOMWARE PROTECTION CHECKLIST

Ransomware attackers are increasingly employing more sophisticated AI-powered attacks and defeating existing defenses. Use this checklist to develop an effective protection plan for your organization.

## 1. Protect your email.

Ransomware attacks often start with a phishing email to capture admin or user credentials.

1a	<p><b>Block phishing attacks</b></p> <p>Attackers use social engineering tactics to bypass traditional email security. Use an email security solution that includes AI-enabled phishing and account takeover protection, as well as alerts when malicious activities are detected.</p>	
1b	<p><b>Train users</b></p> <p>Your users are your last line of defense against phishing attacks. Training needs to be an ongoing effort, as attacks often become more sophisticated over time.</p>	
1c	<p><b>Implement remediation</b></p> <p>Email attacks that evade email security and land in users' inboxes need to be addressed quickly. Choose an email security solution that enables proactive threat discovery and automates remediation.</p>	

## 2. Secure your applications.

Attackers hack your applications and use stolen credentials to gain access to your data.

2a	<p><b>Protect web applications</b></p> <p>Applications often have open vulnerabilities that can be exploited to gain access to your data. Use an application security solution that defends against web application vulnerabilities such as OWASP Top 10, zero-day and brute force attacks.</p>	
2b	<p><b>Protect access to applications</b></p> <p>For internal applications, you should only allow access for authorized users and devices. Choose a zero-trust access solution for secure access to the applications and data authorized specifically for that user. Zero-trust can enable continuous verification of user and device identity.</p>	
2c	<p><b>Protect access to your environment</b></p> <p>Protect your entire network infrastructure to securely connect all users and devices no matter where they are located, to the resources they need, while keeping unauthorized users/attackers out.</p>	

## 3. Back up your data.

Attackers encrypt your data and demand ransom.

3a	<b>Back up your data</b> You need to back up all of your data. Remember your on-prem data as well as data in the cloud/SaaS applications such as Microsoft 365.	
3b	<b>Protect access to applications</b> Attackers often target your backups to prevent you from being able to recover. Encryption, access control, and elimination of network sharing protocols are all important here. You want to make sure that accessing your data is easy for you, but difficult for attackers.	
3c	<b>Develop a recovery plan</b> If you are under attack, you need to be able to quickly deal with the attack, recover your data and avoid paying ransom. Consider not only your technical response, but also your business response. Test your plan in full before there is a problem. Forensics can be helpful in the aftermath of an attack to find vulnerabilities.	

### Other Recommendations

- **Patching** – Make sure software is patched and up to date. Attackers look for known vulnerabilities first, so don't make it easy for them.
- **Multifactor Authentication** – At a minimum, consider requiring a phone app or text based second factor authentication for all applications and resources. This is useful in preventing brute-force login attempts.

**Build your ransomware plan.**

<https://www.barracuda.com/ransomware>

