Ransomware Defense
Best Practices Checklist

Ransomware is the fastest growing malware threat today. Utilize these security best practices and risk mitigation strategies to improve your overall security posture.

**Before an attack: Discover, enforce, and harden**

- **Conduct regular security awareness training** with the latest information on threats and tactics

- **Perform ongoing risk assessments** to identify any security weaknesses and vulnerabilities in your organization:
  - Conduct periodic port and vulnerability scans
  - Ensure solid and timely patch management
  - Disable unnecessary and vulnerable services
  - Enforce strong authentication
  - Centralize security logging

- **Implement a new “best-of-breed” security architecture** that leverages an integrated approach that is simple, open, and automated:
  - Deploy domain name system (DNS) layer protection
  - Automatically enable endpoint protection (incl. mobile devices)
  - Enable email gateway security
  - Restrict lateral attack movement
  - Enforce the principle of least privilege
  - Regularly backup critical systems and data
  - Assess and practice incident response
## During an attack: *Detect, block, and defend*

- Activate incident response
- Communicate timely and accurate information
- Automatically share new security intelligence

## After an attack: *Scope, contain, and remediate*

- Resume normal business operations
- Collect and preserve evidence
- Analyze forensic data
- Perform root cause analysis

### Discover how to:

- Reduce risk of ransomware
- Get immediate protection against attacks
- Prevent malware from spreading laterally

To find out how to keep your business protected, we recommend *Ransomware Defense For Dummies.*

**READ THE EBOOK**