CSNP
CYBERSECURITY NON-PROFIT

Endpoint Security Guide

A comprehensive framework for protecting your organization's devices and data

CSNP SECURITY SERIES

FOR BUSINESS & NONPROFITS

Understanding Endpoint Security

What Are Endpoints?

Endpoints are any devices that connect to your network—laptops, desktops, smartphones, tablets, and servers. Each endpoint represents a potential entry point for cyber threats.

Why It Matters

With remote work and mobile devices becoming standard, endpoints are the front line of your cybersecurity defense. A single compromised device can expose your entire organization.

70% of breaches

Start at endpoint devices

Multiple layers

Required for comprehensive protection

Continuous monitoring

Essential for threat detection

Layer 1: Antivirus & Anti-Malware Protection

Deploy Enterprise-Grade Protection

Install reputable antivirus and anti-malware software on all endpoints. Free solutions exist, but paid enterprise options offer better management and support.

Enable Real-Time Scanning

Configure automatic, real-time threat detection. Schedule regular full system scans during off-hours to minimize performance impact.

Keep Definitions Updated

Ensure virus definitions update automatically daily. New threats emerge constantly—outdated protection is ineffective protection.

Configure Centralized Management

Use a central console to monitor all endpoints, deploy updates, and review threat reports across your organization.

Layer 2: Endpoint Detection & Response (EDR)

Beyond Traditional Antivirus

EDR solutions provide advanced threat detection, investigation, and response capabilities. They monitor endpoint behavior continuously, identifying suspicious activities that traditional antivirus might miss.

Key Capabilities

- Behavioral analysis and anomaly detection
- Threat hunting and forensic investigation
- Automated response to contain threats
- Historical activity tracking and reporting

Monitor

Continuous activity tracking

Detect

Identify suspicious behavior

Investigate

Analyze threats in detail

Respond

Contain and remediate quickly

Layer 3: Patch Management

01

Inventory All Software

Maintain a complete inventory of operating systems and applications across all endpoints.

02

Monitor for Updates

Use automated tools to track available patches and security updates from all vendors.

03

Test Before Deployment

Test critical patches in a non-production environment to avoid compatibility issues.

04

Deploy Systematically

Roll out patches across your organization using a phased approach with clear timelines.

05

Verify Installation

Confirm successful patch deployment and document any devices requiring attention.

Critical patches should be deployed within 48 hours. Regular updates should follow a monthly schedule at minimum.

Layer 4: Device & Data Encryption

Full Disk Encryption

Encrypt all hard drives and storage devices using built-in tools like BitLocker (Windows) or FileVault (Mac). This protects data if a device is lost or stolen.

Email & File Encryption

Implement encryption for sensitive emails and files, both in transit and at rest. Use secure file sharing platforms with end-to-end encryption.

Storage Encryption

Protects data at rest on all devices

Network Encryption

Secures data during transmission

Mobile Device Encryption

Essential for smartphones and tablets

Layer 5: USB & Removable Media Controls

1

Establish Clear Policies

Define who can use removable media, what types are allowed, and under what circumstances. Document approval processes for exceptions.

2

Implement Technical Controls

Use endpoint protection software to disable or restrict USB ports and other removable media. Allow only approved, encrypted devices.

3

Scan All External Media

Configure automatic scanning of any removable media before files can be accessed. This prevents malware from spreading via USB drives.

4

Monitor and Audit Usage

Track all removable media connections and file transfers. Review logs regularly for suspicious activity or policy violations.

Layer 6: Browser & Application Security

Standardize Secure Browsers

Deploy updated browsers with security features enabled. Configure automatic updates and disable unnecessary plugins.

Implement Application Allowlisting

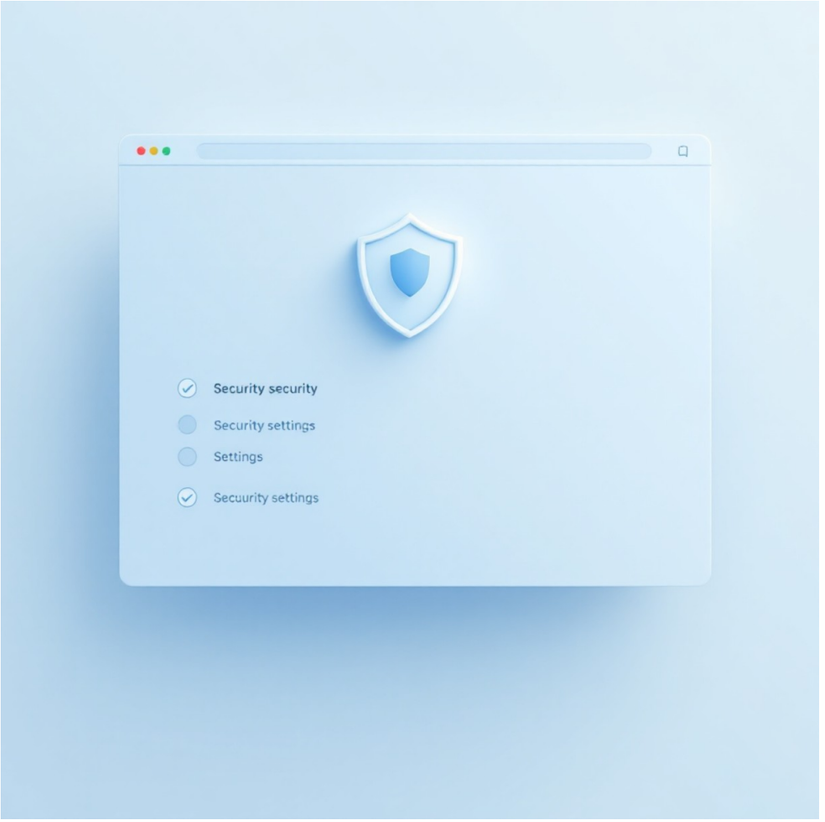
Only permit approved applications to run on endpoints. This prevents unauthorized or malicious software from executing.

Control Browser Extensions

Restrict browser extensions to pre-approved options. Malicious extensions are a common attack vector.

Enforce Safe Browsing Practices

Enable built-in browser security features and deploy web filtering to block malicious sites automatically.



Pro tip: Create separate browser profiles for work and personal use to minimize risk exposure.

Layer 7: Continuous Endpoint Monitoring

Real-Time Monitoring

Track endpoint activity 24/7

Automated Alerts

Immediate notification of threats

Compliance Audits

Verify policy adherence

Regular Reporting

Weekly security status reviews

Establish a monitoring routine that includes daily log reviews, weekly security reports, and monthly comprehensive audits. Use SIEM (Security Information and Event Management) tools when possible to centralize and analyze endpoint data across your organization.

BYOD: Bring Your Own Device Considerations

The BYOD Challenge

Personal devices accessing company resources introduce unique security risks. Balance employee flexibility with organizational security through clear policies and technical controls.

- **Enrollment Requirements**

  All BYOD devices must be registered and meet minimum security standards before accessing company resources.

- **Mobile Device Management (MDM)**

  Deploy MDM solutions to enforce security policies, manage apps, and enable remote wipe capabilities.

- **Data Separation**

  Use containerization to separate work and personal data on devices, protecting both privacy and company information.

Required Controls

- Strong passcode/biometric authentication
- Automatic screen lock
- Encryption enabled
- Remote wipe capability
- Regular security updates

Endpoint Security Implementation Checklist

Essential Security Controls

- Antivirus/anti-malware deployed on all endpoints
- EDR solution installed and configured
- Automated patch management system active
- Full disk encryption enabled
- USB/removable media policies enforced
- Browser security settings standardized
- Application allowlisting implemented

Ongoing Management

- Daily monitoring and log review
- Weekly security status reports
- Monthly compliance audits
- Quarterly security assessments
- Regular employee security training
- Incident response plan testing
- Documentation and policy updates

Download our complete endpoint security checklist and implementation templates at **csnp.org/resources**

Cybersecurity Non-Profit (CSNP)

> "Making cybersecurity knowledge accessible to everyone through education, community, and practical resources."

Business & Non-Profit Security

Practical cybersecurity guidance for organizations of all sizes

Family Cybersecurity

Protecting your household in the digital age

Kids Safety

Age-appropriate online safety education

Senior Digital Safety

Empowering older adults with digital confidence

Women's Security

Addressing unique digital safety challenges

Parents & Educators

Tools to teach and protect the next generation

100% Free Resources

All our programs, guides, and tools are completely free for everyone

Visit csnp.org

Explore our full library of cybersecurity education and resources