ManageEngine
Endpoint Central

The CISO's Endpoint Security Checklist

Table of Contents

1. About this Checklist
2. Reduce Risk and improve governance
3. Empower Security teams
4. Converge visibility and control
5. Maximize Returns and deliver impact
6. Bonus: Going above and beyond
7. Suggested additional reading

About this Checklist

In an era of relentless cyber threats, securing endpoints is no longer an option but a strategic imperative for government and federal agencies. This checklist is designed to empower CISOs with a strategic framework to reduce risk, optimize security operations, and deliver tangible business value.

By focusing on reducing tool sprawl, empowering security teams, gaining comprehensive visibility, and maximizing the return on security investments, Endpoint Central can help Government CISOs fortify their department's digital infrastructure and protect sensitive data. This checklist offers practical guidance and highlights actionable steps to securely deliver mission-critical operations.

Reduce Risk and improve governance

- □ **Get a regular snapshot of your IT :** Identify and inventory all systems, applications, and devices connected to the network based on OS, age and department

- □ **Optimize your security stack :** Assess tools used and take steps to control tools sprawl

- □ **Tie loose ends :** Limit the number of agents/clients used to implement overall endpoint security

- □ **Stay informed :** Streamline threat intelligence alerts/feed to receive timely information on vulnerabilities, bugs and exploits.

- □ **Compliance gaps are non-negotiable :** Identify compliance mandates that need to be adhered for your region and conduct regular security audits.

- □ **Maintain audit trails :** Monitor endpoint activities and maintain detailed logs for incident investigation.

- □ **Lead from the front :** Provide direction and guidance in identifying, evaluating, and prioritizing security risks.

Empower Security teams

- □ **Make every second count :** Optimize time required by security personnel to detect and remediate threats and vulnerabilities

- □ **Allocate personnel judiciously :** Rethink resource allocation across multiple endpoint security verticals (included security for workstations, peripheral devices, browsers, BYOD etc.)

- □ **Automate if you can :** Automate patching of critical apps along with the ability to rollback and test it out on a control group without manual intervention

- □ **Regularize assessments :** Champion endpoint security education and conduct Security awareness/assessments for employees on a regular basis (at least once in six months) and advise operating units at all levels on security issues, best practices, and vulnerabilities.

- □ Make insights more accessible: Have a dedicated view/report that empowers personnel to break down data silos (such as a DPO dashboard)

- □ Share accountability beyond the security team: Rethink incident response playbooks and divest the accountability of breach response beyond the security team.

Converge visibility and control

- □ **Total visibility :** Have a complete and consolidated view of all IT assets in a single window on a granular level
- □ **Establish a security benchmark :** Configure a security baseline and define an 'ideal state' for your endpoints
- □ **Regulate app usage :** Strictly vet allowed/denied list of applications and executables on end user machines.
- □ **Mandate BYOD policy :** Frame policies to secure personal devices at work (BYOD) so that they comply with the organization's security policies
- □ **Access control :** Set up Role based-access management for IT technicians and ensure if existing policy complements with principle of least privilege
- □ **Extensibility :** Can existing endpoint solutions integrate with helpdesk and change management tools to provide a cohesive user experience

Maximize Returns and deliver impact

- □ **Analyse Return on investment (ROI) :** Perform a cost-benefit analysis of the number of tools used to implement effective endpoint security and take corrective measures.

- □ **Reduce Total cost of ownership (TCO) :** Analyze the cost incurred to securing an endpoint against relevant industry benchmarks while also taking into account how frictionless the deployment and onboarding of the solution is.

- □ **Prioritize Time to value (TTV) :** Ensure that endpoint security tool has minimum to zero learning curve. User-friendliness is a crucial indicator of long-term commitment.

- □ **Accomplish financial objectives :** Understand the operating budget and prepare an annual budget incurred for security tools to ensure expenditures remain within projected parameters. Review this periodically to provide proper accountability.

Bonus: Going above and beyond

□ **Resiliency is key :** In addition to devising endpoint protection, take efforts to anticipate how cyberattacks will change over time and how it will pave the way for future shocks—and then create a plan to plug potential issues.

□ **Perform investigative forensics :** Allocate resources or set up a team to study past high profile breaches in the same or adjacent domains for improved breach-preparedness and crisis management.

□ **Prepare for setbacks :** It's essential to fully understand the ground reality while calling the shots. Prioritize taking into account-- setbacks and revisions to ensure a feasible endpoint security execution along with experience or best practices.

□ **Enable Non-IT staff :** Communicate IT issues in a timely manner, and collaborate with staff to create responsive solutions to non-IT staff data for a more technologically inclusive approach.

Suggested additional reading

1. Resources from the National Cyber Security Centre
2. Cyber security breaches survey 2024
3. Cybersecurity Best Practices by CISA
4. Guidelines on Information security practices for government entities

About Endpoint Central

Having been a key player in the market for more than 18 years, ManageEngine Endpoint Central offers IT management and security solutions for any possible requirement you'd have for keeping tabs on a company's endpoints. Endpoint Central centrally manages devices like servers, desktops, laptops, and mobile devices across multiple OSs from a single console. Crafted for SMBs and enterprises alike, Endpoint Central simplifies and automates routine IT tasks while securing your network against cyberattacks.

VISIT ENDPOINT CENTRAL

TRY IT FOR FREE

Follow us on

Find us on Gartner

sales@manageengine.com | +1-925-924-9500

ManageEngine
a division of Zoho Corp.