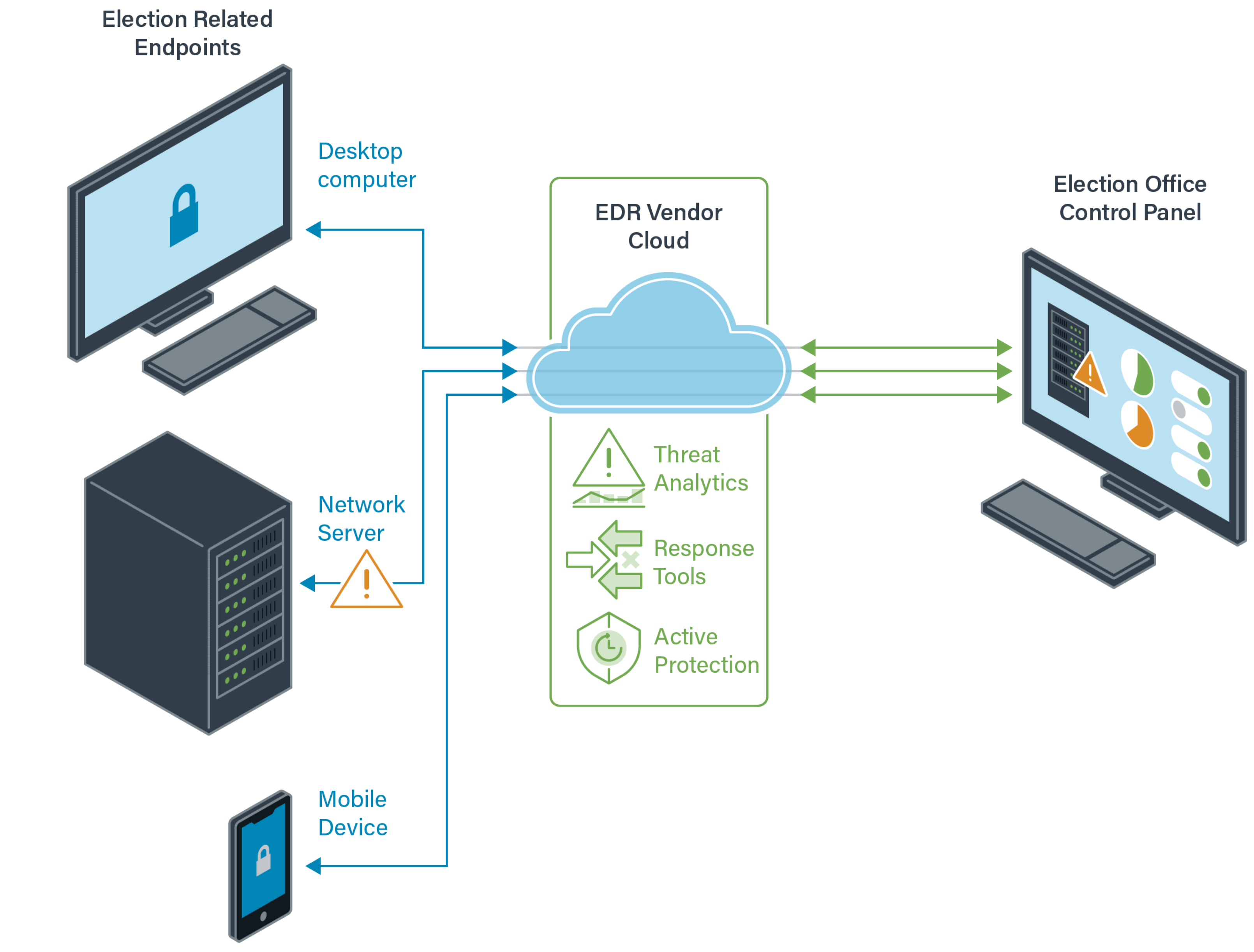
Endpoint Protection

Endpoint protection is security software that is deployed on workstations and servers, which are commonly referred to as “endpoints.” A common name for this is Endpoint Detection and Response, or EDR. EDR collects technical data from these endpoints and transmits it back to the vendor or a local server. The data is then analyzed for suspicious patterns and threats.

If a threat is identified, it is blocked, and an alert is generated. Administrators can typically view alerts through a vendor control panel or a connection to their own security platform. Also, many EDR solutions include a traditional antivirus functionality and the ability for responders to remotely access compromised systems for remediation.



Election offices can use EDR to:

- Detect and stop active attacks on election infrastructure,
- Protect against malware,
- Quarantine suspicious files,
- Isolate compromised systems,
- Remediate malware infections,
- Enable analysis to find and mitigate threats, and
- Disable and restrict the ability of suspicious users on your network to cause harm.

Election officies should put EDR on internet-connected and critical endpoints, including workstations, mobile devices, webservers, and other important networked systems. EDR should not be deployed on voting systems.

Goals

1. Get EDR services through the EI-ISAC or commercial vendors (Level 1 maturity)

Actions

For Endpoint Protection, the necessary actions vary by maturity as detailed below.

Level 1 Maturity

1. Deploy EDR on systems throughout your network. EDR should not be deployed on voting systems.
   - All your systems and endpoints that touch administrative election processes are covered at no cost to you by the federally-funded EDR program. Additionally, your jurisdiction’s non-election endpoints can also sign up for the same services at a discounted cost. Contact elections@cisecurity.org for more information.
   - For commercial solutions, you may also review CIS’s Guide for Ensuring Security in Election Technology Procurements for best practices in crafting proposals and other necessary documents.
2. Take advantage of vendor-offered user training for usage of EDR tools, including when you sign up for the EI-ISAC EDR program.
3. Implement best practices for EDR:
   - Delegate personnel to monitor and act on detections.
   - Export information regularly from the control panel to local hardware backups, so you always have access to data needed for audits and investigations.
   - Consider available staffing resources to support any new security infrastructure and the associated responsibilities. Many EDR providers offer solutions supported by a 24×7 team to manage and respond to identified incidents.
   - Refer to the EI-ISAC Cyber Incident Checklist to manage security events.

Level 2 and Level 3 Maturities

For the Level 2 and Level 3 maturities, all of the guidance for the Level 1 maturity applies, but the specifics of your network configuration and the number of endpoints you serve may affect whether you can implement EDR through the EI-ISAC. Contact elections@cisecurity.org for more information.

Cost-Effective Tools

- EI-ISAC EDR program: EDR services at no charge to state and local election offices. Contact elections@cisecurity.org.

Learn More

- EI-ISAC EDR program brochure

Mapping to CIS Controls and Safeguards

- 10.1: Deploy and Maintain Anti-Malware Software
- 10.6: Centrally Manage Anti-Malware Software

Mapping to CIS Handbook Best Practices

- 32, 40

‹ Previous
Firewalls and Port Restrictions

Next ›
Malicious Domain Blocking and Reporting

Made with Sphinx and @pradyunsg's Furo
Last updated on Jan 12, 2023