MINNESOTA IT SERVICES

Malicious Domain Blocking and Reporting

Minnesota IT Services (MNIT) offers Malicious Domain Blocking and Reporting (MDBR), a web security service, through a trusted vendor partner.

MDBR delivers a proven, effective, and easily deployable layer of cybersecurity defense. MNIT's vendor designed this service in partnership with the Cybersecurity and Infrastructure Security Agency (CISA).

How MDBR works on your network

MDBR is a cloud-based solution that uses recursive domain name system (DNS) technology to prevent information technology (IT) systems from connecting to harmful web domains. This helps state, local, and Tribal governments limit infections related to known malware, ransomware, phishing, and other cyber threats.

- MDBR blocks and logs attempts to access known malicious domains such as those associated with malware, phishing, and ransomware, among other threats.
- Once an organization routes its protective DNS requests to our security servers, MDBR checks each lookup against a list of known and suspected malicious domains.
- Your organization can block or allow domains based on your organization's risk tolerance.
- The vendor will provide a weekly report that includes log information for all accepted and blocked requests reaching out to known or suspected malicious domains.

Benefits

- Uses technology to prevent IT systems from connecting to known harmful web domains.
- Limits infections related to malware, ransomware, phishing, and other cyber threats.
- Deploys quickly and easily.
- Requires little maintenance.
- Protects users in the office or working remotely.
- Provides visibility into risky web traffic, potential compromise indicators, and areas of greatest vulnerability.
- Event reports can be scheduled to the cadence that works with your organization.
- Available at no cost to eligible local governments in Minnesota.

Eligibility and cost

MDBR is available to eligible entities in Minnesota, including any city, township, local public authority, school district, special district, intrastate district, county, Tribal Nation, council of governments, regional or interstate government entity, or agency or instrumentality of a local government.

MDBR is a free service, subsidized through the federal government's State and Local Cybersecurity Grant Program (SLCGP).

Steps to enroll in MDBR service

- Email MNIT's Cyber Navigator Team with questions or to sign up for MDBR: CN.MNIT@state.mn.us. They will work through the registration process with your organization.
- After you sign up, a no-charge contract will be sent for signature. A contract is required to participate.
- You will need to provide:
  - Your contact information.
  - Technical contact(s) for MDBR setup, troubleshooting, and general technical support.
  - Reporting contact(s) for receiving reports on your MDBR service.
  - Public IP addresses or Classless Inter-Domain Routing (CIDR) netblocks from which your organization's DNS queries are sent.
- As the final step, you will need to point your DNS requests to the vendor's DNS server IP addresses. This will enable MDBR to prevent attempts to access known malicious domains.

The MDBR service can be implemented quickly and requires virtually no maintenance.

More information

- Contact MNIT's Cyber Navigator Team: CN.MNIT@state.mn.us
- Visit MNIT's Whole-of-State participant page for more information: mn.gov/mnit/about-mnit/security/whole-of-state-cybersecurity-plan/wos