IRONCORE Product Datasheet

Free Network Scan for CBI Banks

Gain critical insights into endpoints, devices and users & identify known vulnerabilities, missing security controls and common misconfigurations of your network assets.

Common Network Security Vulnerabilities:

Unauthorized Devices
Unidentified assets on the network are not good. Ensure only approved devices have access. (Domain 1: Inventory and Classification of Assets)

Network Structure
Many bank networks are "open" or "flat" meaning once inside, bad actors have access to all parts of the network. (Domain 3: Configuration Management)

Missing Updates
Devices and programs must be patched and upgraded. Windows applications are updated. (Domain 3: Patch Management)

Stale or Overprivileged Identities
Incorrect privileges assigned, default credentials used, stale users and unused groups are not removed. (Domain3: Disable Dormant Accounts and Restrict Administrator Privileges)

Unauthorized Third-party Applications
Properly licensed software only installed on network assets. Unapproved applications open the bank to exploitable vulnerabilities. (Domain1: Software Inventory and Classification)

Actively managing cyber risk includes network vulnerability scans.

Community banks should anticipate higher regulatory standards and more cyber-related enforcement actions in 2022-2023. Regulators continue to regard cyberattacks as a major threat to the safety and soundness of individual banks and the broader financial system.

Additionally, many banks are experiencing time-consuming and complex cybersecurity insurance renewals. Insurers are limiting coverage, charging more and changing underwriting standards to require proof of preventative cyber security controls including multi-factor authentication (MFA), more rigorous data backup practices, employee training and event log management.

However, the foundation of any layered cybersecurity defense is a network vulnerability assessment, and now **IRONCORE is offering a free, no-obligation Rapidfire network scan to benefit Community Bankers of Iowa member banks.**

Network Scan vs Penetration Test

Network vulnerability scans are used to identify current network users, determine the state of systems and devices, and take an inventory of network elements to help identify and categorize vulnerabilities found on your network. The network assessment is only one tool used to evaluate the health of your network devices. **Penetration Testing** simulates an attack to exploit weaknesses and prove the effectiveness of your network's perimeter security. It involves a team of security professionals who actively attempt to break into your bank's network and is far more intrusive than a vulnerability scan. Penetration testing can take 1-3 weeks to complete, while a Rapidfire network scan is usually completed in less than an hour.

What is a Rapifire Scan?

The Rapidfire Network scan is a non-intrusive process that takes about 30 minutes total to run. During a scan, the Rapidfire Network Detective is used to log into your network providing a map of the entire system. The scan builds inventories which IRONCORE then utilizes to evaluate possible weaknesses. The real value of the assessment is not the scan itself, but the IRONCORE Vulnerability Assessment Report, Debrief Call and Executive Summary included with each scan. The assessment, debrief and summary give banks the opportunity to discuss findings with IRONCORE's cybersecurity experts to determine their best next steps.

How much does a network scan typically cost?

There are several factors that can affect the cost of a vulnerability scan based on the bank's IT environment. On average, network vulnerability scans cost between $2,500 – $5,000 depending on the number of IP addresses, servers or applications scanned. However, in coordination with IRONCORE, the **Rapidfire Network scan is available to CBI member banks at no charge.**

Why do I need this service?

As community banks continue to innovate and add to their IT infrastructure, they are unknowingly adding security threats and potential vulnerabilities. It is vital for community banks to scan their entire network to provide greater visibility and monitor potential threats on all device connected to the network.

Make your IT environment more secure.

The assessment is only one tool used to evaluate the health of your network devices. A more complete assessment of the bank's security posture would include elements such as:

- Routine penetration testing
- Developing cybersecurity policies
- A review of security controls and procedures
- Implementing security awareness training
- Implementing a SIEM solution
- Creating a data loss prevention (DLP) program
- Next -generation antivirus and threat hunting
- Intrusion detection & prevention (IDS/IPS)

About IRONCORE

Founded more than 10 years ago in concert with leaders from the Fiserv Precision® Data Center Team; IRONCORE has developed a national presence helping community banks across the country manage the security, performance and scalability of their hardware, software and network resources. Located in Onalaska, Wisconsin our state-of-the-art data center is SOC2 audited and FFIEC examined. Community banks of all sizes rely on the IRONCORE Managed IT Portfolio for: Backup & Disaster Recovery – SIEM/SOC – Private Cloud – Monitored & Managed Networks – SDWAN – Helpdesk – Unified Threat Management (UTM) – Hardware & Software Procurement – Project Implementation – Pentration Testing.

IRONCORE
Strong · Trusted · Secure

www.ironcore-inc.com
608-779-9400

IRONCORE
Craig Arendt
Mobile: 319-330-6331
craig.arendt@ironcore-inc.com

CBI
COMMUNITY BANKERS OF IOWA

Associate Member