mamori.io

FREE Solution for Small Businesses to Achieve Cyber Resilience

Mamori's FREE cybersecurity solution is the only solution you need to secure **7 of the 12 areas** recommended by the:

FEDERAL TRADE COMMISSION

Homeland Security

SBA U.S. Small Business Administration

NIST National Institute of Standards and Technology U.S. Department of Commerce

www.mamori.io

Only One Step Away from Cyber Resilience

As a small business, you should already have a firewall, VPN, and Windows defender or malware scanner implemented. **Mamori is the only solution you need to add** to help you secure the 7 most technical areas recommended by the FTC, NIST, SBA and DHS, shown below.

Mamori offers **FREE** licenses to support small businesses. Request your free license now at **mamori.io/free**.

What Mamori Secures


Cybersecurity Basics


Cyber Insurance


NIST Cybersecurity Framework


Phishing


Ransomware


Secure Remote Access


Vendor Security


Business Email Imposters


Email Authentication


Physical Security


Hiring a Web Host


Tech Support Scams

Source: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity

How Mamori Secures Small Businesses from Cyber Attacks

The features mentioned below are expensive and complex, which is why they are only deployed at companies with large budgets and the required technical expertise. With Mamori, not only are the same features free, deployment is also extremely simple.

Are you a small business? Request a **FREE** license now at **mamori.io/free**.

CYBERSECURITY BASICS

Knowing the basics of cybersecurity greatly reduces your risk of a cyber attack. This includes regularly training your staff, updating your software, requiring strong passwords, encrypting data, and using multi-factor authentication.

The Difference with Mamori

Two Factor Authentication (2FA) Logins to your company database and file storages are secured with 2FA. If you don't have a 2FA provider like Okta or DUO, you can use Mamori's 2FA mobile app for Apple and Android devices.

Encryption Mamori encrypts data in transit and at rest. Mamori has built-in key management service, and you can choose between symmetric or assymetric data encryption.

CYBER INSURANCE

The increase in cyber and ransomware attacks has led many cyber insurers to hike rates substantially and other insurers to stop cyber insurance coverage altogether. With Mamori's cybersecurity solution implemented, your business cybersecurity risks will be lowered significantly. ***Mamori customers' cyber insurance bills are typically reduced by 30-60%, depending on coverage.***

Cyber insurance protects your business against losses from cyber attacks. You should consider what's covered in the policy and what services the cyber insurance provides in case there is a breach. Depending on the nature of your business, you might consider first-party coverage, third-party coverage, or both.

Cyber insurance premiums are calculated based on your organization's revenue and risks, and risks are assessed by how many of the following 10 safeguards you have. Mamori provides 5 of the following 10 safeguards, which is why Mamori customers' cyber insurance bills are significantly lower.

Provided by Mamori	NOT Provided by Mamori
Credentials Security	Daily Backups
Multi-Factor Authentication	Disaster Recovery Plan
Firewalls	Annual Security Awareness
Intrusion Prevention and Detection	Written Data Security Policies
Limiting Data Access	Antivirus Software

How Mamori Lowers Cyber Insurance Bill

Two Factor Authentication (2FA) Mamori offers 2FA on all types of access, ranging from users and applications to databases. This is the number one solution insurance carriers look for. Some carriers may require details on how your 2FA policy protects admin users, remote accesses, and other types of accesses. This meets the following safeguard required by insurance companies:

Multi-Factor Authentication

Network Microsegmentation Mamori allows you to allocate network resources based on roles, such as restricting third party vendors to particular desktops and applications. This effectively prevents ransomware attacks by reducing its attack surface. Plus, network access can be further secured by 2FA. This meets the following safeguards required by insurance companies:

Limiting Data Access

Multi-Factor Authentication

Intrusion Detection and Activity Monitoring Mamori for IP (M4IP) offers 24/7 intrusion detection and activity monitoring, which detects unauthorized access based on device's identity and access permissions, as well as identifying any suspicious activity. More and more carriers are beginning to require this safeguard as a qualification for cyber insurance.

Intrusion Prevention and Detection

Database Activity Monitoring and SQL Firewall M4PAM monitors and records all access connections to the database and how the database files were operated. Data access policies can be set by table, row, and column. Data operations can be limited by role. All access and operations history are logged, and admins are notified immediately when an anomaly occurs. This meets the following safeguards required by insurance companies:

Firewalls

Limiting Data Access

Intrusion Prevention and Detection

Data Privacy Solutions Mamori provides data privacy safeguards to ensure that you meet compliance and prevent personal information from being mishandled or misused. Access to database objects and data (column and row) can be limited. Displayed data can also be limited with data masking and encryption.

Limiting Data Access

Administrator Access Management Some insurers require an administrator access management tool layered on top of the directory to increase security. This includes 2FA, credential security, password reset policies, and ability to integrate with identity management with session recording (database, SSH, and RDP). That is what Mamori for Privileged Access Management (M4PAM) is built for. M4PAM with 2FA can easily be implemented by rolling over all existing directory and access settings and satisfies the following safeguards required by insurance companies:

Credentials Security

Limiting Data Access

Multi-Factor Authentication

NIST CYBERSECURITY FRAMEWORK

NIST is the National Institute Standards and Technology at the U.S. Department of Commerce. It outlines the best practices for cybersecurity protection:

- **Identify** all company equipment and devices and create a policy for employees, vendors and anyone else with access to sensitive data.
- **Protect** data by encrypting sensitive data, conducting regular backups, and controlling who logs onto your network and on what device.
- **Detect** unusual activities through monitoring your network and your computers for unauthorized access.
- **Respond** to attacks by notifying those who are at risk and reporting the attack to authorities.
- **Recover** from an attack by repairing and restoring the equipment or network while keeping employees and stakeholders informed.

Mamori Helps You Identify, Protect and Detect

Zero Trust Network Access (ZTNA) Mamori's M4IP identifies all company equipment, devices and network by providing a registry of all devices and resources (network). It also provisions which devices can access which resources.

Securing Devices Mamori enables you to secure each device using device registry and links each device to a directory user. All devices that connect to your network can easily be managed and monitored. Devices that can be secured include desktops, laptops, mobile devices, internet of things (IoT), as well as servers and databases.

Intrusion Detection Mamori for IP (M4IP) detects unsolicited access based on device's identity and access permissions. It also detects and blocks network scans from hackers and automatically identifies and locks the compromised devices from further access.

Database Activity Monitoring M4IP monitors and records all access connections to the database and how the database files were operated. All access and operations history are logged, and admins are notified immediately when an anomaly occurs.

Administrator Access Management Mamori for Privileged Access Management (M4PAM) enables you to create data access rules by the user's role and by device. These access controls extend to database, limiting what a user is able to see and do inside the database.

Real-Time Alerts Mamori provides alerts based on access policies you want to track. For instance, you can choose to receive an alert whenever the financial database is accessed after-hours.

PHISHING

Phishing is when you get an email that looks like it's from someone you know. Typically, these emails create a sense of urgency that makes you click on a malicious link that allows a hacker to install malware on your device. The data stored on that device is compromised, and so are the passwords stored on the device to access your company's network.

Mamori Minimizes Phishing Damage

Two Factor Authentication (2FA) Even if the hacker tries to access the company network from a compromised device, 2FA will stop the hacker at the doorsteps.

Administrator Access Management Although Mamori cannot stop an employee from clicking on a malicious link, Mamori prevents the malware from spreading, limiting the damage to the single compromised device. M4PAM eliminates the need to store passwords on devices, so even when a device is compromised, the hacker has no administrator credentials to access other accounts.

Microsegmentation Mamori's M4IP with Zero Trust Network Access (ZTNA) provides "edge networking" so connected device gets a virtual IP address instead of a network IP address. This effectively prevents hackers from scanning the network, reduce lateral movement, and minimize phishing damage.

RANSOMWARE

Ransomware encrypts your data, locks you out of the network and asks you to pay a ransom to recover your data. Ransomware hackers typically use phishing and scam emails, server vulnerabilities, and malicious links to gain an entry point into one of your devices. Then, the hacker will use the compromised device as an entry point to spread to other devices and equipment on the company network. Ransomware attacks have more than doubled since 2020 because of the gaining popularity of working from home.

Mamori Minimizes Ransomware Damage

Administrator Access Management If a ransomware hacker compromises a device, no passwords will be compromised because M4PAM eliminates admin password storage on devices.

Intrusion Detection If a ransomware gains entry to a network, their first step is to scan the network for files, data and the presence of other devices. Mamori for IP (M4IP) detects and blocks all unauthorized network scans. Meanwhile, the compromised device conducting the network scan will be immediately blocked from further access.

Microsegmentation Micro Segmenting networks prevents ransomware from moving laterally and greatly reduces its attack surface. Mamori allows you to micro segment a network based on roles or identity workload, such as segmenting a network for all third parties that you work with. Thus, even if a third party was compromised by a ransomware hacker (similar to the Colonial Pipeline ransomware attack), the hacker will have no access to the other networks within your company.

Database Activity Monitoring All database connection and activity are monitored 24/7. Any anomaly will be detected, and administrators will be notified immediately.

SECURE REMOTE ACCESS

Secure Remote Access allows your employees, vendors and contractors to securely connect to your network remotely. Companies should require the devices connecting remotely to be secure. Utilizing virtual private network (VPN) should be required, especially when they're using a public Wi-Fi.

Mamori Provides Same Security Level for Internal and Remote Staff

Securing Devices Only authorized devices can connect onto the company network. These devices include desktops and laptops, mobile devices, internet of things (IoT), as well as servers and database.

Two Factor Authentication (2FA) Access is granted only when the person's identity is authenticated using 2FA, ensuring the right person is behind the right device.

Secure Remote Access Both internal and remote staff go through the same level of security check before accessing the company network. The types of access secured include secure shell (SSH), remote desktop protocol (RDP), direct database access and IP address.

VENDOR SECURITY

The vendors that you work with may have access to sensitive company information. If they do, make sure those vendors are securing their own devices and networks. The best practice is to include provisions for security in your vendor contracts and establish processes to confirm your vendors are following those rules.

Mamori Enhances Vendor Security

Administrator Access Management Your vendors should only have access to the data they need to do their job, and Mamori's Privileged Access Management (M4PAM) ensures that. You can use M4PAM to create a least-privilege access policy to protect how third parties (or your employees) access and use company data.

Microsegmentation With Mamori's ZTNA, you can segment a network for third party vendors and set policies that governs which devices can have access to what resources (network). This is the common practice because you have no control over their cybersecurity practices. With a segmented network for vendors, your main company networks are safe even if the segmented network is hacked because of vendor negligence.

Data Privacy Solutions Vendor's access to database objects and data (column and row) can be limited. Displayed data can also be limited with data masking and encryption. All of these is to ensure that your vendors do not mishandle or misuse personal information.

Two Factor Authentication (2FA) With Mamori, you can require your vendors to use 2FA when they access your network.

Secure Remote Access If your vendors need remote access to your network, they will have the same level of security as those within your work premises.

If you're a small business, you can cybersecure your business for free and lower your cyber insurance bill at the same time.

See if you're qualified. Request a free license at **mamori.io/free** now!

Mamori is More than a Cybersecurity Solution

Mamori protects you from cyber attacks and lowers your cyber insurance bill. But that's not all. Mamori also helps you:

- **Prevent** data theft and breaches
- **Comply** with security and data privacy regulations
- **Accelerate** digital transformation and growth
- **Simplify**, **scale** and **automate** DevOps and resource access

Data powers what we do, and Mamori ensures what we do doesn't get disrupted. Get a demo at **mamori.io/appointment** to see how we can help.