mamori for IP resources

Comprehensive ZTNA Solution

- Multi-factor access to all networked resources
- Micro-segmentation of resources
- Intrusion detection and device isolation
- Activity monitoring & auditing
- Workflow approval process
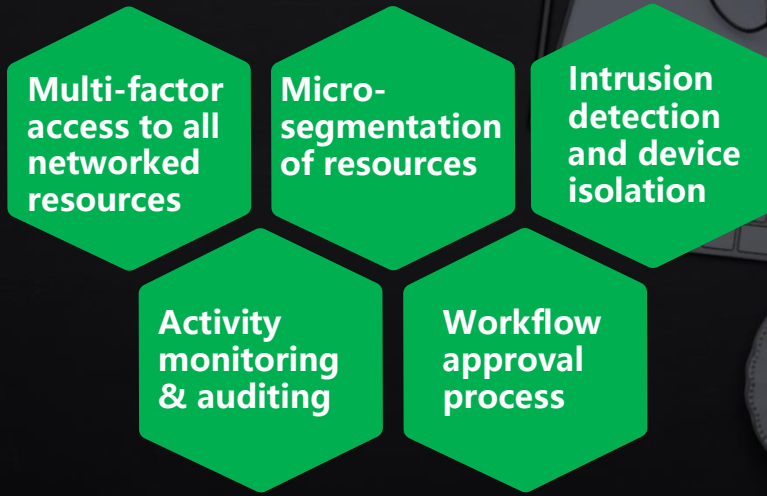
Protect against ransomware & meet compliance

Improve developer, DBA and DevOps productivity

Mamori for IP resources (M4IP) is a comprehensive zero-trust network access (ZTNA) solution that protects internal and remote access to self-deployed cloud or on premise resources like file shares, applications, servers, databases, and IoT devices.

M4IP allows businesses to quickly overlay zero trust security on all or part of their networked resources. It delivers a consistent and modern access experience to staff, consultants and external vendors whether they are in the office or remotely working.

Key Features

- Plug and play key based virtual private network (WireGuard) that is 2x faster than legacy VPNs.

- Multi-factor authentication on access to all controlled resources.

- Device Registry – manage and monitor user devices that are able to access resources.

- Micro-segmentation – break down data centre and cloud environments into segments down to the individual workload level.

- Detect and block devices that attempt to scan your network.

- Replace manual provisioning processes with a user friendly on-demand access solution

- Integrated monitoring, alerting and auditing by identity and device.

FAST TO DEPLOY
Protect thousands of severs and applications in weeks not months.

MONITORED & AUDITED
User & device access activity is continuously monitored and audited.

LOW IMPACT
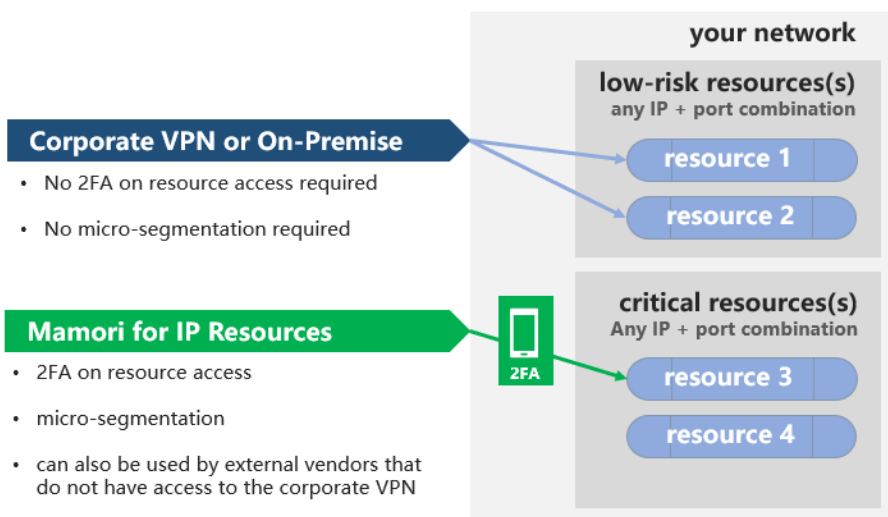Only change network rules. No changes to servers, applications or databases required.

COMPLIANT
Meets technical safeguards for all major security regulations.

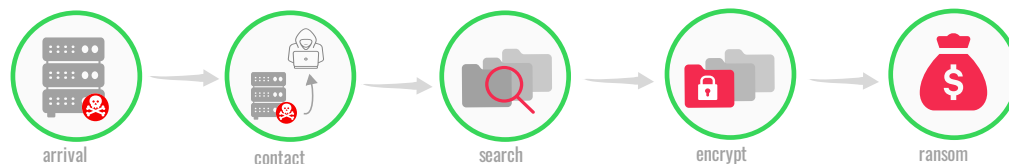**Mamori Difference** – 6 improvements over traditional VPNs

	Traditional VPN or Virtual Desktop	M4 IP
Client device check		✅
Initial login verfication	✅	✅
Restrict resources by role		✅
2FA on resource access		✅
Intrusion detection		✅
Access on demand		✅
Same security - internal or remote access		✅

Compliment your existing VPN or Virtual Desktop Security

your network

Corporate VPN or On-Premise
- No 2FA on resource access required
- No micro-segmentation required

low-risk resources(s)
any IP + port combination
- resource 1
- resource 2

Mamori for IP Resources
- 2FA on resource access
- micro-segmentation
- can also be used by external vendors that do not have access to the corporate VPN

2FA

critical resources(s)
Any IP + port combination
- resource 3
- resource 4

Intrusion detection & threat isolation

RANSOMWARE ATTACK WITHOUT 2FA ON RESOURCE ACCESS & INTRUSION DETECTION

arrival → contact → search → encrypt → ransom

RANSOMWARE ATTACK WITH M4IP PROTECTION

arrival → contact → M4 IP

2FA resource access & scan detection blocks the search