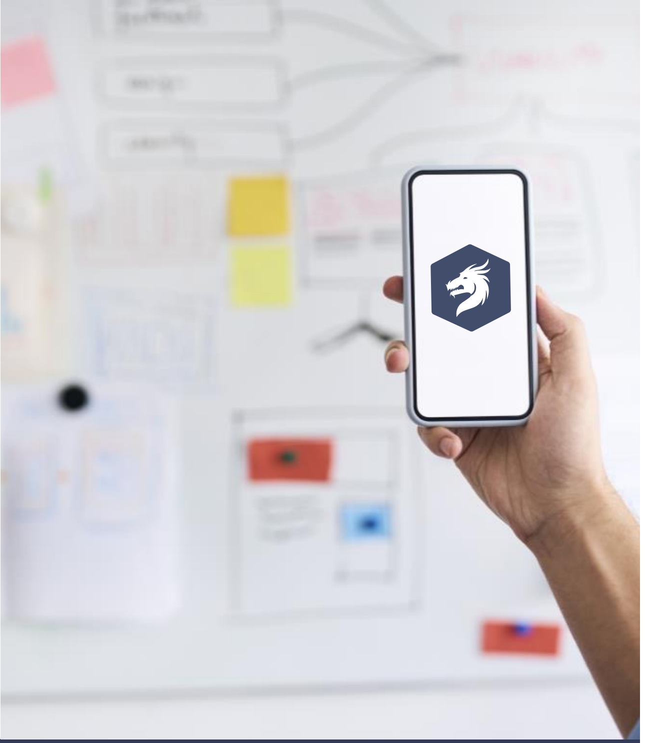
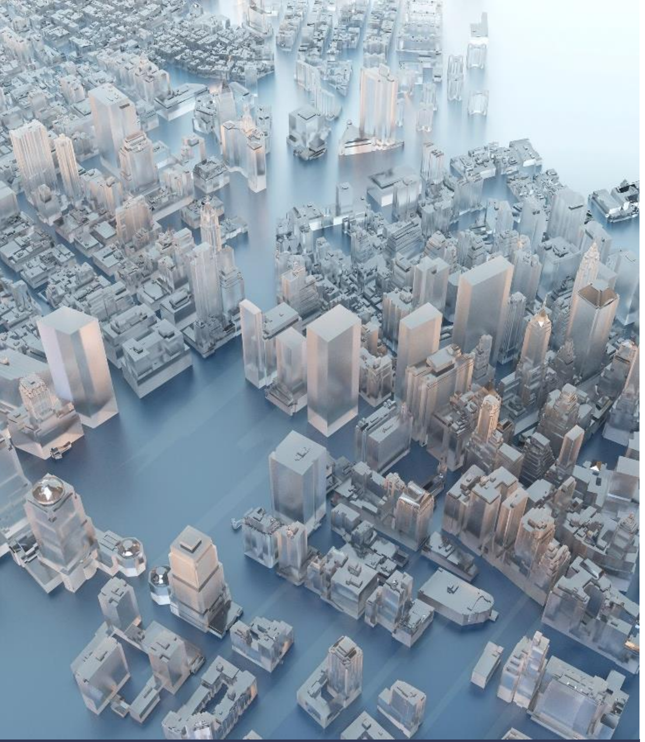


mamori.io

module overview

mamori for IP resources (M4IP)

A comprehensive zero-trust network access (ZTNA) solution that simplifies resource access management and protects self-deployed resources from ransomware and other network penetration attacks.

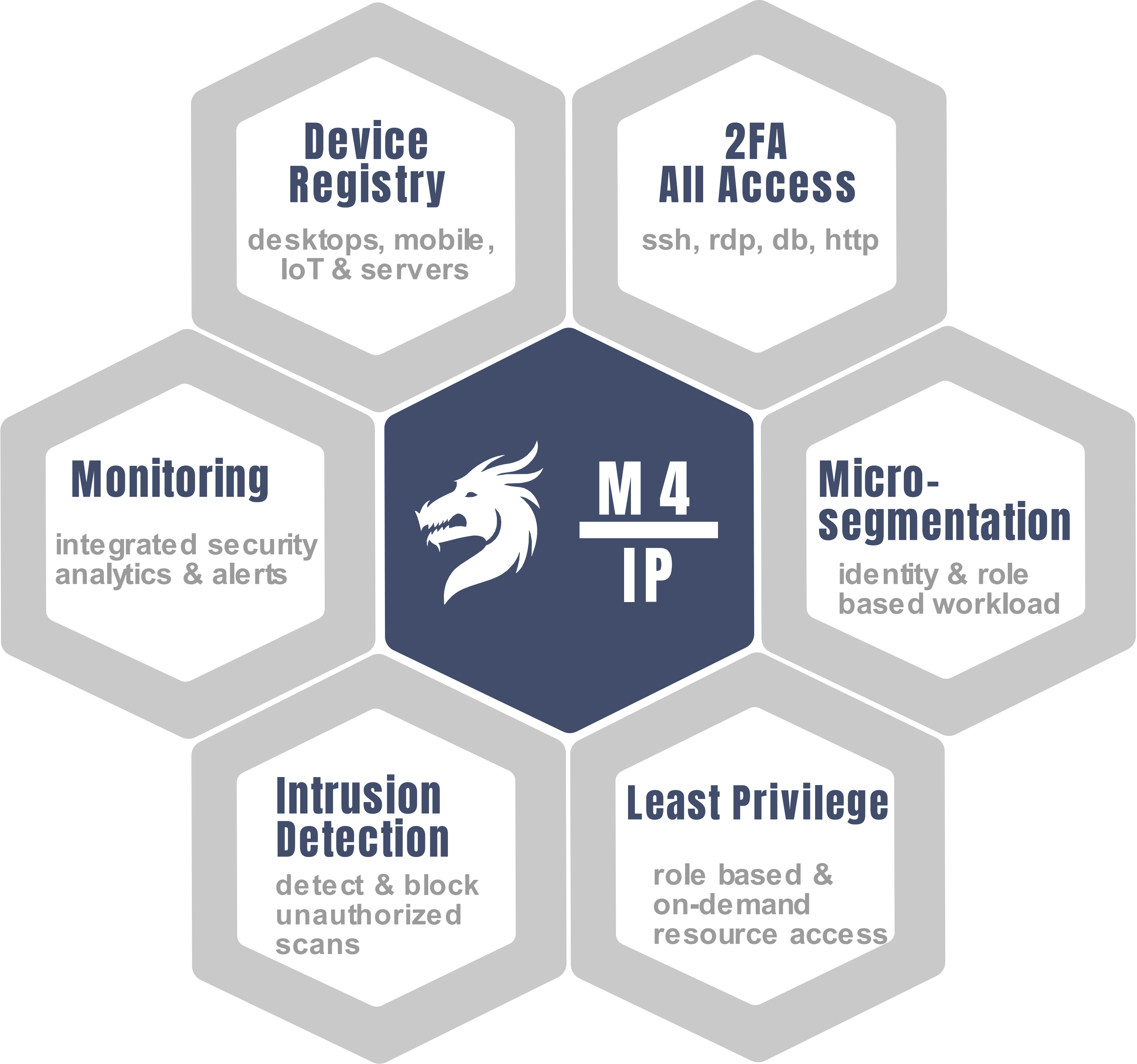


M4IP

solution features

technical safeguards for

- Ransomware protection
- Remote and internal access
- Network penetration attacks



M 4
IP

Device Registry
desktops, mobile, IoT & servers

2FA All Access
ssh, rdp, db, http

Monitoring
integrated security analytics & alerts

Micro-segmentation
identity & role based workload

Intrusion Detection
detect & block unauthorized scans

Least Privilege
role based & on-demand resource access

mamori for IP resources

M 4 IP

mamori.io

Protects

Applications, file shares, servers, databases and IoT resources from unverified access

technical safeguards for

- Ransomware protection
- Remote and internal access
- Network penetration attacks

key features

- Device Registry
- Multi-factor authenticate everything
- Micro-segmentation of resources down to role based or identity workload
- Intrusion detection and threat isolation
- Monitor & audit by user/device
- Least privilege via access on-demand

key benefits

- Protected thousands of applications and resources in weeks
- 2FA community free web applications and other resources without SAML integration
- Simplifies administration of access to resources.
- Users can visualize their own permissions and request if needed

M4IP

versus traditional VPN

6 security improvements that protect from modern threats

mamori.io

	Traditional VPN or Virtual Desktop	M4IP
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		✓

Complement your existing network

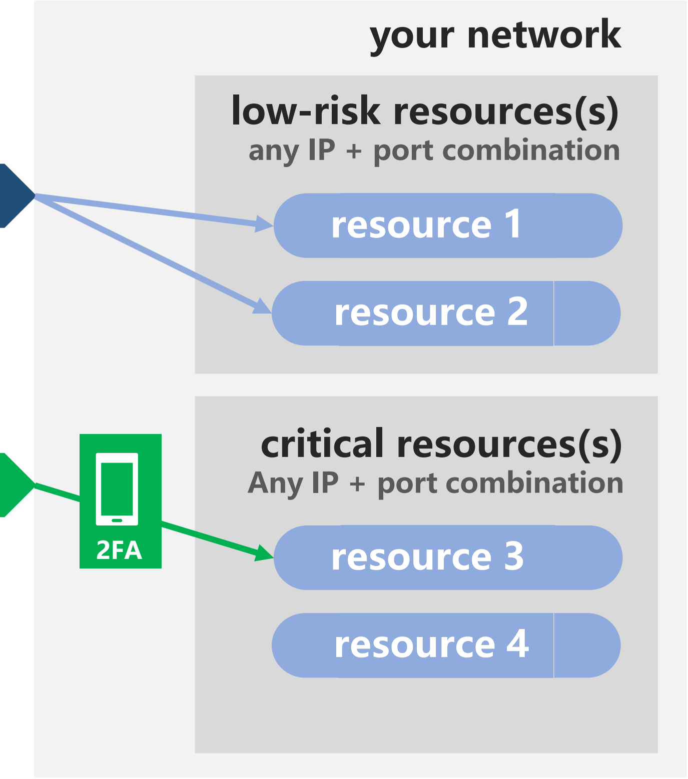
Easily zero-trust a part or all of your data center and cloud resources

Corporate VPN or On-Premise

- No 2FA on resource access required
- No micro-segmentation required

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



Secure Vendor Remote Access

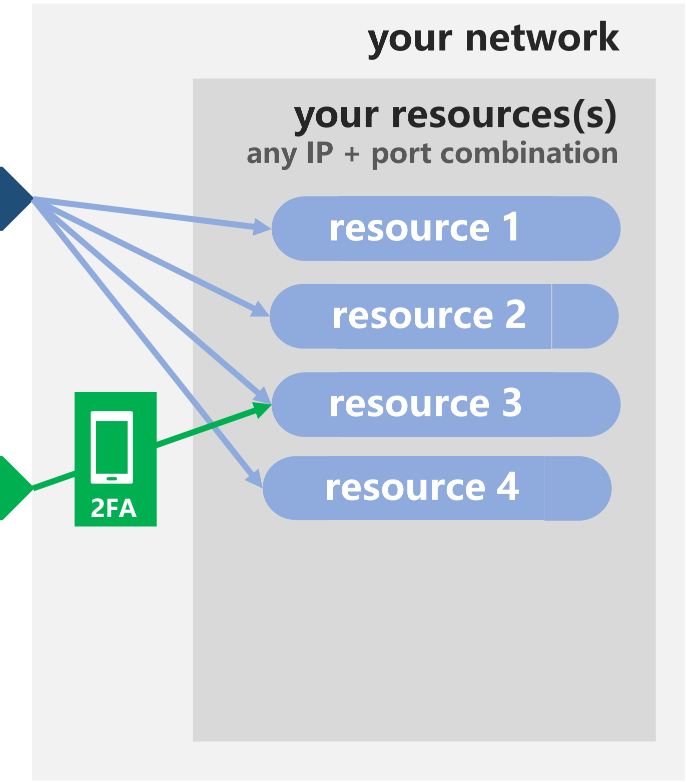
Easily 2FA and micro-segment access to external vendors and consultants

Corporate VPN or On-Premise

- No 2FA on resource access required
- No micro-segmentation required

Mamori for IP Resources VPN

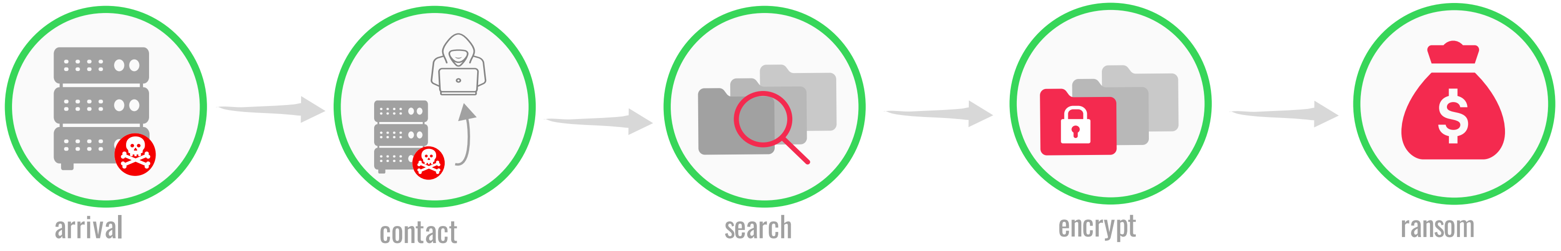
- 2FA on resource access
- Micro-segmentation of resources down to role or identity based workload



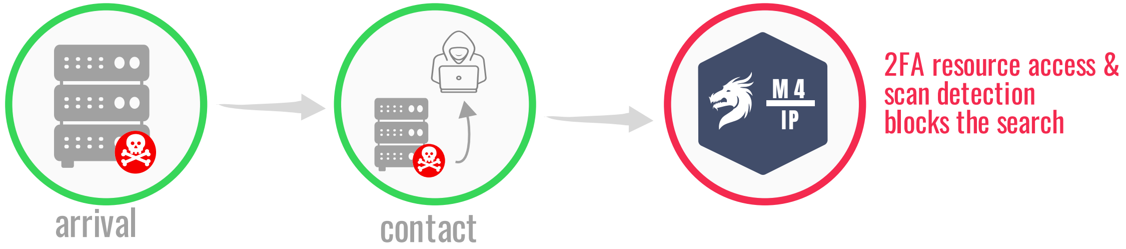
Intrusion Detection and Isolation

Safeguard from network penetration attacks or unauthorized insider access

RANSOMWARE ATTACK WITHOUT 2FA ON RESOURCE ACCESS & INTRUSION DETECTION



RANSOMWARE ATTACK WITH M4IP PROTECTION



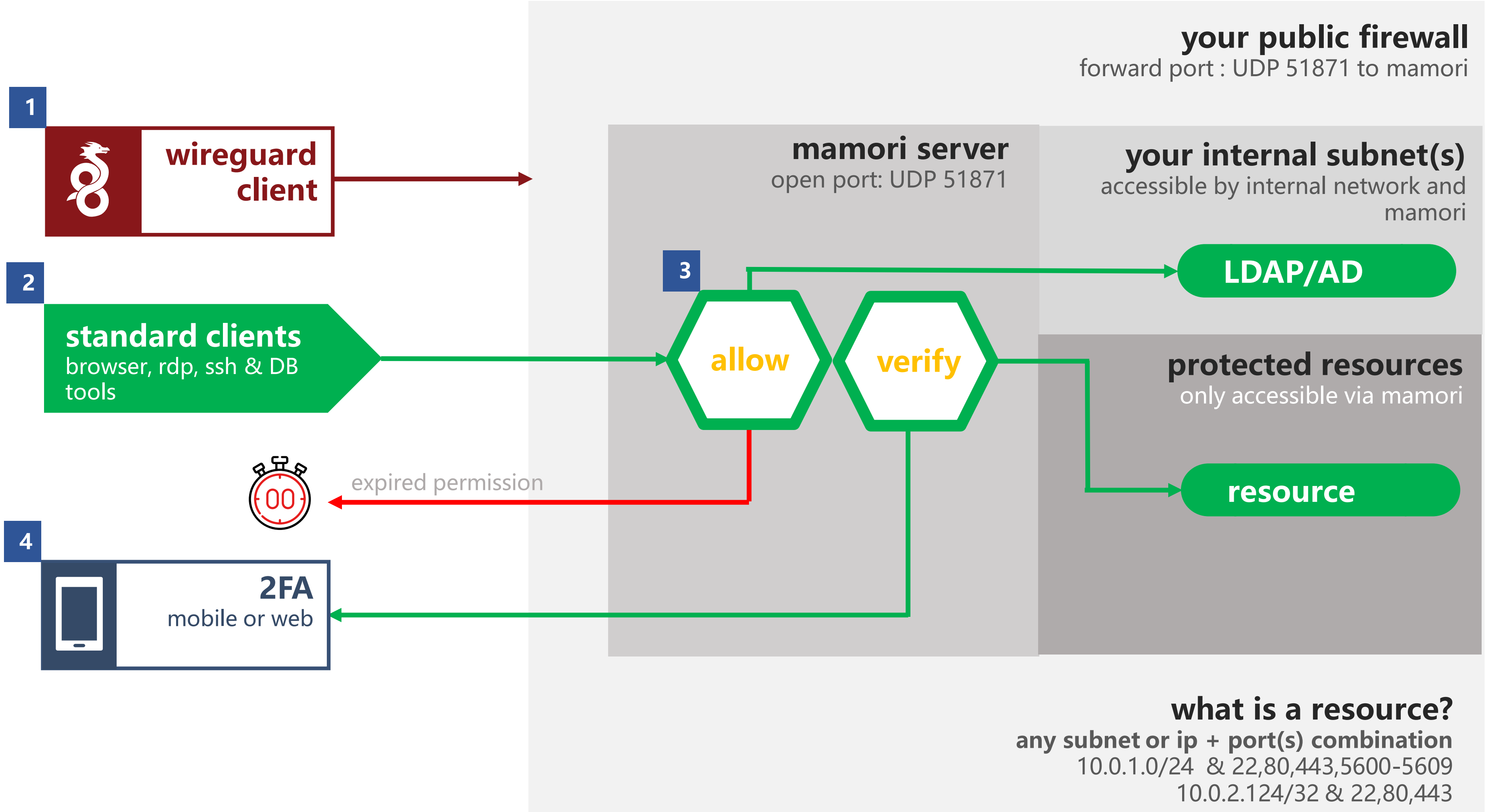
key features

- User notified if their device makes unsolicited access to resources
- Any attempts of a network scan is detected and blocked.
- Device is locked from further access and administrators notified

resource access

remote or internal

1. Activate network
2. Access an IP resource from a standard tool
3. Resource permission check
4. Multi-factor verification



your public firewall

forward port : UDP 51871 to mamori

1

wireguard client

2

standard clients

browser, rdp, ssh & DB tools

mamori server

open port: UDP 51871

3

allow

verify

your internal subnet(s)

accessible by internal network and mamori

LDAP/AD

protected resources

only accessible via mamori

resource

expired permission

00

4

2FA

mobile or web

what is a resource?

any subnet or ip + port(s) combination

10.0.1.0/24 & 22,80,443,5600-5609

10.0.2.124/32 & 22,80,443

Configuration

Server Configuration

1. Integrate directories & extend with 2FA
2. Configure SMTP & WireGuard settings
3. Set user device auto-enrollment settings
4. Define IP resources and grant them to roles/users

A resource is any subnet or ip + port(s) combination
10.0.1.0/24 & 22,80,443,5600-5609
10.0.2.124/32 & 22,80,443

End-user Configuration

1. User installs WireGuard client & key
2. User configures 2FA via mamori web portal
3. User accesses resources as normal