DYOPATH: Managed Security

DYOPATH offers flexible, customizable Managed Security Services for organizations of all sizes that need protection from hackers, data breaches and more. We can help you identify and block cyber threats, respond to potential data breaches, protect intellectual property and keep your client and customer information secure.

Why Clients Choose DYOPATH For Managed Security Services

Integrated

We provide 24/7 protection and analysis with our Managed Security Services. Continuous, real-time monitoring and universal automatic policy enforcement begin with a technology assessment to evaluate your organization's systems and operations. Our integrated approach is based on a stack of tools backed by managed Security Information and Event Management (SIEM) with a 24/7 Security Operations Center (SOC).

Low Noise

Many SIEMS becomes worthless due an excessive amount of alarms. Our SIEM is continually tuned by professionals – our goal is to avoid unnecessary alarms and noise.

Adaptable

The SEIM and SOC can consume data from our existing stack or 200+ other 3rd party products. We work with our clients to integrate into their environment.

We Provide Strong Protection, Rapid Detection & Instant Responses

Focus on your core business while we keep it secure. Due to the ever-changing digital landscape with new threats arising continually, you need a security company that can adapt and react with those changes. That's what we do well and the Managed Security Services we offer give you unparalleled network protection.

Malware Protection for Endpoints

Fully managed next-gen AV/Malware platform that blocks malicious software or file-less malware before execution. Our 24/7 staffed SOC manages the fine-tuning of the application in the environment in which its deployed and then manages the reporting and tier 1/2 triage of alerts to ensure accuracy.
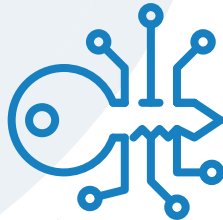
Encryption For Endpoints

Web-based console encryption management for File Vault on Mac OS, and BitLocker within Windows. We provide an audit trail of devices/drives being encrypted and can control access if a device is misplaced or stolen.

Endpoint Detection and Response

Our EDR solution provides detection, investigation and remediation. We can discover known and unknown elements of an attack through real-time threat hunting. Once a threat is detected and qualified, we can air gap the device and prevent it from being used for credential escalation or island hopping.

Contact DYOPATH Today for your Managed Security Questions