Linux support

General system maintenance:

- OS updates and patch management
- Configuration management (server settings, service tuning)
- Container and virtual machine basic operations (creation, monitoring, lifecycle tasks)
- Application installation and basic configuration support (common packages only; complex application deployments may require a project quote)
- Log management and rotation setup
- Package repository configuration and troubleshooting

Backup verification & maintenance:

- Backup strategy design and scheduling
- Verification of existing backup systems
- Restoration test assistance
- Storage solution integration (customer-provided storage)

Performance tuning and automation assistance:

- Basic performance tuning (CPU, memory, disk I/O tuning)
- Automation scripting (Bash, Python, etc.)
- Job scheduling and maintenance (cron, systemd timers)
- Monitoring integration (Netdata, Prometheus, etc.)

DevSecOps management:

- Version control system setup and management (Git, Gitea, etc.)
- Static code analysis pipeline integration
- Secrets management systems (Vault, sops, agenix, etc.)
- Infrastructure as Code support (Terraform, Ansible, Nix)
- CI/CD pipeline support (basic GitHub/GitLab CI config, runner deployment)

Security & Compliance:

- User and group management (access controls, sudo policies)

- Firewall and intrusion detection configuration (UFW, fail2ban, etc.)
- Patch audit and CVE tracking
- SSH hardening and key management

Networking & Connectivity:

- VPN and SSH bastion setup
- DNS, DHCP, and local resolver configuration
- Troubleshooting network-related outages or performance issues

---

Cybersecurity support

Vulnerability Management:

- Monthly perimeter vulnerability assessments (external-facing systems only)
- Internal network vulnerability scans (yearly or on request)
- CVE monitoring and proactive advisories (requires SBOM availability)
- Threat intelligence monitoring for exposed assets (optional add-on)

Security Audits & Assessments:

- Yearly security audit (included for annual retention customers, project-based for monthly customers):
  - Internal network vulnerability scans
  - External perimeter scans
  - Configuration baseline reviews
  - Remediation planning assistance
- Security posture evaluations based on NIST Cybersecurity Framework (CSF) and CIS Controls

Compliance & Standards Support:

- ISO 27001 awareness and implementation training (scheduled sessions)
- GDPR, HIPAA, and PCI-DSS readiness advisory
- Assistance preparing internal documentation and policies for audits

Incident Response & Recovery:

- Initial incident triage and advisory
- Post-incident analysis and reporting
- Assistance setting up incident detection and alerting systems (IDS/IPS/SIEM)

Security Engineering:

- Secure configuration of firewalls, VPNs, and endpoint protection tools
- Basic hardening of servers and workstations (Linux, Windows, MacOS)
- Secrets management setup and integration (Vault, SOPS, custom solutions)
- MFA implementation assistance (TOTP, WebAuthn, Passkeys, etc.)

Website management

CMS Operations:

- Support for major CMS platforms (WordPress, Joomla, Drupal, etc.)
- Core updates and security patching
- Plugin and module updates (Limited support custom codebases)
- CMS configuration troubleshooting and minor fixes

Monitoring & Maintenance:

- Uptime monitoring for HTTP/HTTPS availability
- Basic performance checks (page load time, resource usage alerts)
- SSL/TLS certificate monitoring (expiration alerts)
  Backup & Recovery:
- Scheduled database backups (to customer-provided storage)
- Scheduled file backups (site content, media libraries)
- Backup restoration support (upon request)

Security & Hardening:

- CMS security hardening (basic measures such as login protection, admin path obfuscation)
- Malware scanning and cleanup advisory
- Web Application Firewall (WAF) integration assistance (optional add-on)

Project services

> This is a non-exhaustive list, please contact us for queries

- Major application deployments or migrations
- Large-scale infrastructure overhauls
- Custom application support (bespoke code, custom stacks)

Cybersecurity

- Full NIST Cybersecurity Maturity Assessments
- Red Team / Purple Team exercises (lightweight engagements)
- Advanced phishing simulation campaigns and reporting
    - Tiered for spearphising / whaling / standard phishing
- Zero Trust architecture advisory and design
- Cloud security posture reviews (AWS, Azure, GCP)

Website Management

- Website migration services (between hosts or platforms)
- Major CMS version upgrades (including staging/testing environment setup)
- SEO health monitoring and basic recommendations

Clarifications and limitations

> "*System health monitoring tools are supported where installed, but installation/configuration of enterprise monitoring solutions (e.g., Zabbix, Prometheus, Netdata, Nagios) are considered project work.*"

> "*Support includes container operation support (starting/stopping/updating), but not DevOps-level orchestration (e.g., Kubernetes, Rancher) unless separately quoted.*"

> "*All services are provided on a best-effort basis within the limits of the agreed support tier and scope. No warranty or guarantee of outcome is implied unless explicitly stated in a project agreement.*"

> "*Customers are responsible for maintaining access credentials, licensing, hardware warranty, and any third-party service subscriptions necessary for environment operation unless specified otherwise.*)"

"*Requests falling outside the defined Support Scope may be deferred, require a project quote, or be declined based on feasibility or risk.*"

"*Support services may involve interaction with third-party vendors (e.g., cloud providers, software vendors). Delays or issues arising from third-party limitations are outside of our direct control.*"

"*Major configuration changes, critical system alterations, or security policy adjustments may require pre-approval or project scoping before execution.*"