

G-Cloud 15 Service Definition

NinjaOne - Unified IT Management Platform

Service Name	NinjaOne Unified IT Management Platform
Service Type	Software as a Service (SaaS)
Supplier	Howell Technology Group Limited
Framework	G-Cloud 15

Service Summary

NinjaOne provides a comprehensive unified endpoint management platform, delivering remote monitoring and management (RMM), patch management, remote access, and IT automation capabilities through a single consolidated console. The platform manages Windows, macOS, and Linux devices with automated maintenance, software deployment, and ITSM ticketing integration, streamlining IT operations through intelligent automation and centralised management whilst reducing tool sprawl and operational complexity.

Service Description

Modern IT organisations manage increasingly diverse device estates spanning multiple operating systems, locations, and ownership models, whilst being tasked with maintaining security, compliance, and user productivity with limited resources. Traditional approaches requiring multiple point solutions for monitoring, patching, remote access, and asset management create operational inefficiency, data silos, visibility gaps, and unnecessary complexity.

NinjaOne addresses these challenges by providing a unified platform that consolidates the core IT management capabilities organisations require into a single, intuitive solution. The platform eliminates tool sprawl by replacing multiple disparate systems with one comprehensive management console, accessible from anywhere via web browser or mobile application.

The service provides continuous monitoring of endpoint health, performance, and security posture, automatically detecting issues and resolving many without human intervention through sophisticated automation capabilities. IT teams gain complete visibility across their entire device estate regardless of location, with real-time insights into device status, software inventory, security compliance, and performance metrics.

Automated patch management ensures endpoints remain secure and compliant, with intelligent scheduling that minimises user disruption whilst maintaining security posture. Software deployment capabilities enable rapid distribution of applications, scripts, and configurations across large device estates with minimal administrative effort. Integrated remote access provides secure connectivity to managed devices for troubleshooting and support without requiring separate remote control tools.

NinjaOne integrates seamlessly with existing ITSM platforms, professional services automation (PSA) tools, and security solutions, creating a cohesive IT management ecosystem. The platform's automation engine enables organisations to standardise routine maintenance tasks, enforce configuration baselines, and respond proactively to issues before they impact users.

The solution scales efficiently from small organisations with dozens of devices through to large enterprises managing tens of thousands of endpoints across multiple geographies. Cloud-native architecture ensures consistent performance regardless of scale whilst eliminating infrastructure management overhead.

Service Benefits

Operational Efficiency

- Consolidate multiple IT management tools into single platform
- Reduce time spent on routine maintenance by 70% through automation
- Eliminate context-switching between disparate management consoles
- Streamline workflows through integrated capabilities
- Free IT resources for strategic initiatives

Enhanced Security and Compliance

- Automated patch management reduces vulnerability exposure
- Real-time compliance monitoring and reporting
- Proactive threat detection and remediation
- Consistent security baselines across all devices
- Audit-ready compliance documentation

Improved User Experience

- Faster issue resolution through proactive monitoring
- Reduced downtime through automated remediation
- Seamless remote support capabilities
- Minimal disruption from maintenance activities
- Improved device performance through optimisation

Cost Reduction

- Eliminate multiple tool subscriptions and licensing costs
- Reduce help desk ticket volume through proactive maintenance
- Lower IT staffing requirements through automation
- Predictable subscription-based pricing
- Reduce security incident costs through vulnerability management

Scalability and Flexibility

- Single platform manages Windows, macOS, and Linux devices
- Scale from tens to tens of thousands of devices seamlessly
- Support on-premises, cloud, and hybrid environments
- Remote workforce support without VPN requirements
- Multi-site and multi-tenant capabilities

Visibility and Control

- Real-time visibility across entire device estate
- Comprehensive reporting and analytics
- Customisable dashboards for different stakeholders
- Inventory management and asset tracking
- Software license optimisation insights

Service Features

Remote Monitoring and Management (RMM)

- Real-time device health monitoring
- Performance metrics tracking (CPU, memory, disk, network)
- Event log monitoring and alerting
- Service and process monitoring
- Hardware inventory and tracking

- Automated health checks and remediation
- Custom monitoring policies and thresholds

Patch Management

- Automated Windows Update management
- Third-party application patching
- macOS and Linux patch management
- Flexible scheduling and deployment rings
- Pre-approval workflows for critical patches
- Patch compliance reporting
- Rollback capabilities for problematic updates

Remote Access and Control

- Built-in remote desktop connectivity
- Remote command execution
- File transfer capabilities
- Multi-monitor support
- Session recording for compliance
- Wake-on-LAN integration
- Unattended access to servers and workstations

Software Deployment and Management

- Application installation and updates
- Script deployment and execution
- Configuration management
- Software inventory tracking
- License compliance monitoring
- Bulk deployment capabilities
- Application whitelisting and blacklisting

Automation Engine

- Custom script library (PowerShell, Bash, Apple Script)
- Scheduled automation tasks
- Event-triggered automation
- Policy-based automation
- Pre-built automation templates
- Drag-and-drop automation designer
- Conditional logic and workflow automation

Backup and Disaster Recovery Integration

- Backup monitoring and verification
- Integration with leading backup solutions
- Backup failure alerting
- Disaster recovery testing capabilities
- Image-based backup management
- Cloud backup integration

Security and Compliance

- Antivirus and security software monitoring
- Windows Defender management
- BitLocker encryption management
- Firewall configuration and monitoring
- Security baseline enforcement

- Compliance policy templates (CIS, NIST, Cyber Essentials)
- Vulnerability assessment and reporting

Mobile Device Management Integration

- iOS and Android device visibility
- Basic mobile device management capabilities
- Integration with Microsoft Intune and other MDM platforms
- Mobile device inventory
- Application deployment to mobile devices

Ticketing and ITSM Integration

- Built-in ticketing system
- Integration with ConnectWise, Autotask, Kaseya BMS, and other PSA platforms
- Ticket creation from monitoring alerts
- Ticket workflow automation
- SLA tracking and management
- Customer portal for ticket submission

Reporting and Analytics

- Pre-built report templates
- Custom report creation
- Scheduled report delivery
- Executive dashboards
- Compliance reporting
- Patch compliance reports
- Software inventory reports
- Hardware lifecycle reports

Network Discovery and Management

- Automatic network discovery
- SNMP monitoring
- Network device management
- Switch and router monitoring
- Printer management
- Network mapping
- IP address management

How the Service is Delivered

Initial Assessment and Planning

HTG conducts comprehensive discovery of your IT environment, understanding your device estate, current management tools, automation opportunities, integration requirements, and operational objectives. This assessment informs deployment strategy and configuration approach.

Platform Deployment

NinjaOne is delivered as a pure SaaS solution requiring no on-premises infrastructure:

1. **Tenant Provisioning:** HTG provisions your dedicated NinjaOne tenant with initial configuration aligned to your organisational structure and security requirements
2. **Integration Configuration:** Configuration of integrations with existing tools including ITSM platforms, Microsoft 365, Active Directory, PSA systems, and backup solutions

3. Policy Development: Creation of monitoring policies, patch management schedules, automation workflows, and security baselines customised to your requirements

Agent Deployment

NinjaOne agents are deployed to managed devices using appropriate deployment methods:

Domain-Joined Windows Devices: Deployment via Group Policy, SCCM, Intune, or existing RMM tool for migration scenarios

Non-Domain Windows Devices: Manual installation, email deployment links, or MDM deployment

macOS Devices: Deployment via MDM, Self-Service portal, or package installer

Linux Servers: Deployment via package managers or installation scripts

Typical deployment completes within 1-2 weeks for organisations up to 500 devices, with phased rollout approach for larger estates.

Configuration and Customisation

HTG configures NinjaOne to align with your operational requirements:

- Monitoring policies tailored to device types and roles
- Patch management schedules aligned with change windows
- Automation workflows for routine maintenance
- Alerting thresholds and escalation procedures
- Custom dashboards for different stakeholder groups
- ITSM ticketing workflow integration

Knowledge Transfer and Training

Comprehensive training is provided for IT administrators covering:

- Platform navigation and core functionality
- Policy and automation creation
- Remote access and control
- Reporting and analytics
- Troubleshooting and incident resolution
- Best practices for operational efficiency

Training is delivered remotely via Microsoft Teams with recorded sessions and comprehensive documentation.

Ongoing Management Options

Self-Managed with Support: Your IT team operates NinjaOne with HTG providing technical support, best practice guidance, platform optimisation recommendations, and escalation assistance.

Co-Managed Service: HTG provides active monitoring support, alert triage and response, automation development, regular platform optimisation, and strategic guidance whilst your team maintains day-to-day management.

Fully Managed Service: HTG assumes primary responsibility for endpoint management including monitoring and alerting, patch management, software deployment, automation development, incident response, and regular reporting. Your team receives comprehensive managed IT services with NinjaOne as the platform foundation.

Continuous Improvement

HTG provides ongoing service enhancement through quarterly platform reviews assessing automation opportunities, policy optimisation, integration enhancements, and operational efficiency improvements.

Service Management

Service Desk and Support

- UK-based service desk available during business hours (08:00-18:00 GMT)
- Email, telephone, and web portal support
- Ticket tracking through HTG's service management platform
- Dedicated account manager for service oversight
- Access to NinjaOne vendor support for platform issues
- Online knowledge base and documentation

Incident Management

- Priority-based incident classification and response
- P1 (Critical - platform unavailable): 1-hour response time
- P2 (High - major functionality impaired): 2-hour response time
- P3 (Medium - minor functionality impaired): 4-hour response time
- P4 (Low - information request): 1 business day response
- Proactive monitoring of platform health and performance

Change Management

- Formal change management process for production changes
- Testing environment available for policy and automation testing
- Scheduled maintenance windows for major changes
- Change advisory board for significant modifications
- Emergency change procedures for security updates

Service Reporting

- Monthly operational reports detailing device health, patch compliance, and incident summary
- Quarterly business reviews with strategic recommendations
- Annual service assessments and planning
- Real-time dashboard access for continuous visibility
- Custom reporting available on request

Onboarding and Offboarding

Onboarding Process

Typical onboarding completes within 2-4 weeks depending on estate size:

1. **Discovery and Planning (Week 1):** Environment assessment, device inventory, requirements gathering, integration planning, project scheduling
2. **Platform Configuration (Week 1-2):** Tenant provisioning, integration setup, policy development, automation creation, testing
3. **Agent Deployment (Week 2-3):** Phased agent rollout, monitoring verification, policy application, optimisation
4. **Training and Handover (Week 3-4):** Administrator training, documentation delivery, knowledge transfer, operational handover, go-live

Migration Support

For organisations migrating from existing RMM platforms, HTG provides:

- Migration planning and strategy
- Data export from legacy platform
- Agent replacement coordination
- Policy and automation migration
- Parallel operation period
- Legacy platform decommissioning support

Offboarding Process

Should you choose to discontinue the service:

1. **Notice Period:** 30 days' notice required for service termination
 2. **Data Export:** Complete export of device inventory, policies, automation scripts, and historical data
 3. **Knowledge Transfer:** Documentation of configurations and customisations
 4. **Agent Removal:** Coordinated uninstallation of NinjaOne agents
 5. **Migration Support:** Assistance with migration to alternative platform if required
- No penalties for service termination. Your device data and configurations are exported for your records.

Service Constraints and Dependencies

Prerequisites

- Windows 7 or later, Windows Server 2008 R2 or later
- macOS 10.12 Sierra or later
- Modern Linux distributions (Ubuntu, RHEL, CentOS, Debian)
- Internet connectivity for agent communication
- Administrative credentials for agent deployment
- Firewall rules allowing outbound HTTPS (TCP 443)

Technical Constraints

- Agent requires outbound internet connectivity (no inbound ports required)
- Minimum 50MB RAM per agent
- Minimum 200MB disk space per device
- Administrative/root access required for deployment
- Some automation requires local admin rights on endpoints
- Windows Server Core has limited functionality

Functional Limitations

- Physical hardware access requires on-site presence
- Some features specific to Windows environments
- macOS and Linux feature parity lower than Windows
- Mobile device management capabilities limited compared to dedicated MDM
- Network device monitoring limited to SNMP capabilities
- Application-layer monitoring requires additional tools

Scale Considerations

- Recommended maximum 50,000 devices per tenant
- Large file transfers may require bandwidth management

- Mass deployments should be scheduled appropriately
- Concurrent remote sessions limited by subscription tier
- API rate limits apply to high-frequency operations

Integration Dependencies

- ITSM integration requires compatible PSA platform
- Backup monitoring requires agent on backup server
- Active Directory integration requires domain connectivity
- Single sign-on requires Azure AD Premium
- Some integrations require API access and licensing

Supported Environments

- On-premises Windows domains
- Azure AD environments
- Hybrid identity configurations
- Cloud-hosted virtual machines (Azure, AWS, GCP)
- Physical servers and workstations
- Remote worker devices

Pricing Information

Licensing Model

NinjaOne is licensed on a per-device, per-month basis. Pricing includes:

- Complete platform access with all features
- Unlimited technician users
- Mobile application access
- Regular platform updates and new features
- Standard technical support during business hours
- Online knowledge base and documentation

Tiered Licensing Options

- Essential: Core RMM and monitoring capabilities
- Complete: Adds patch management and remote access
- Professional: Adds backup integration and ticketing
- Enterprise: Adds advanced automation and API access

HTG Professional Services

Implementation and ongoing management services are priced separately:

- Initial deployment and configuration
- Agent deployment assistance
- Policy and automation development
- Administrator training
- Migration from legacy RMM platforms
- Ongoing managed service options (co-managed or fully managed)

Pricing Transparency

Detailed pricing is available through HTG's G-Cloud 15 pricing document. Pricing is based on:

- Number of managed devices by type (workstation, server, network device)
- NinjaOne tier selected (Essential, Complete, Professional, Enterprise)
- HTG service level (self-managed, co-managed, fully managed)
- Professional services requirements

- Contract term and volume discounts

No Hidden Costs

- No per-technician licensing fees
- No additional charges for remote access sessions
- No fees for platform updates or new features
- No charges for standard technical support
- No termination or exit fees

Data Security and Protection

Data Location and Sovereignty

- NinjaOne platform hosted in Amazon AWS
- European customer data processed in EU-West (Ireland) region
- UK customer data can be segregated to UK-specific infrastructure
- Customer can specify preferred data processing region
- No data transfer outside designated region without consent

Data Collection and Processing

- Device telemetry: performance metrics, event logs, software inventory, hardware details
- No collection of user documents, email, or personal files
- No collection of web browsing history or keystroke logging
- Configuration data and scripts stored encrypted
- All data encrypted in transit and at rest

Data Security Measures

- TLS 1.3 encryption for all data transmission
- AES-256 encryption at rest
- Multi-factor authentication supported and recommended
- Role-based access control (RBAC)
- Comprehensive audit logging
- Regular security assessments and penetration testing
- SOC 2 Type II certified

Compliance and Certifications

- SOC 2 Type II certified
- ISO 27001 certified
- GDPR compliant data processing
- UK Data Protection Act 2018 compliance
- HIPAA compliance available
- HTG Cyber Essentials Plus certified

Privacy Protection

- Data Processing Agreement provided
- Privacy policy clearly defines data use
- No sale or sharing of customer data
- GDPR rights honoured
- Right to erasure upon service termination
- Data retention policies configurable

Access Control

- Granular RBAC with customisable roles

- Multi-factor authentication enforced
- SSO integration via SAML 2.0
- Session timeout and inactivity controls
- IP address restrictions available
- Comprehensive audit trail of all administrative actions

Service Level Agreement (SLA)

Platform Availability

- 99.99% uptime guarantee for NinjaOne platform
- Measured monthly excluding planned maintenance
- Service credits available for SLA breaches
- Planned maintenance communicated 7 days in advance
- Maintenance typically performed outside business hours

Performance Commitments

- Agent check-in frequency: every 60 seconds
- Alert notification within 2 minutes of detection
- Remote access connection establishment <5 seconds
- Platform API response time <500ms (95th percentile)
- Dashboard loading time <3 seconds

Agent Communication

- Real-time agent communication
- Automatic agent reconnection after connectivity loss
- Queued commands executed when agent reconnects
- Agent health monitoring and alerting
- Redundant infrastructure for agent communication

Support Response Times

- P1 (Critical): 1 hour, business hours
- P2 (High): 2 hours, business hours
- P3 (Medium): 4 hours, business hours
- P4 (Low): 1 business day

24/7 emergency support available for fully managed customers.

Business hours defined as 08:00-18:00 GMT, Monday-Friday, excluding UK public holidays.

Terms and Conditions

Service provision is governed by HTG's G-Cloud 15 Call-Off Terms and Conditions. Key terms include:

Contract Duration

- Minimum initial term: 12 months
- Monthly renewal thereafter
- 30 days' notice required for termination
- No penalties for termination after minimum term

Service Changes

- HTG reserves right to update service features
- Material changes communicated 30 days in advance
- Pricing changes on 90 days' notice

- Customer right to terminate if changes unacceptable
- Platform updates managed by NinjaOne with advance notification

Liability

- Liability terms as per G-Cloud framework
- Professional indemnity insurance: £5,000,000
- Public liability insurance: £5,000,000
- Cyber liability insurance: £5,000,000

Data Ownership

- Customer retains ownership of all data
- Customer data exportable at any time
- No vendor lock-in or proprietary data formats
- Configuration scripts and automation provided in standard formats

Additional Information

Environmental and Social Value

- Cloud-native platform eliminates hardware requirements
- Reduced travel through remote management capabilities
- Paperless operations and reporting
- Carbon-neutral operations commitment
- Apprenticeship programmes in IT support

Supplier Information

- Company Name: Howell Technology Group Limited
- Microsoft Solutions Partner status
- NinjaOne Certified Partner
- ISO 27001 certified
- Cyber Essentials Plus certified

Document Version: 1.0

Last Updated: January 2026

Framework: G-Cloud 15