Product Requirements Document (PRD)

Next-Generation Hosting Control Panel with Integrated Billing and Automation

Document Version: 1.0
Date: November 2, 2025
Project Owner: Romeo Alexandru Neacsu
Status: Draft

Executive Summary

This Product Requirements Document outlines the comprehensive feature set and functional requirements for developing a next-generation hosting control panel that combines the best capabilities of industry-leading solutions (Enhance Panel, CloudPanel, and WHMCS) with enhanced enterprise-grade security features. The platform aims to provide hosting providers with a complete, secure, and scalable solution for managing multi-server hosting infrastructure, automated billing, customer provisioning, and comprehensive support systems.

Primary Objectives:

- Create a unified platform combining hosting management, billing automation, and customer support
- Implement enterprise-grade security with PHP hardening, advanced WAF, and comprehensive threat protection
- Enable multi-server clustering with zero-configuration scaling
- Provide automated provisioning and billing workflows
- Deliver superior user experience for administrators, resellers, and end customers

1. Product Vision and Goals

1.1 Vision Statement

To build the most comprehensive, secure, and user-friendly hosting control panel that empowers hosting providers to scale from single-server operations to enterprise multi-server clusters while automating billing, provisioning, and security without complexity.

1.2 Primary Goals

1. **Unified Platform:** Single control panel for hosting management, billing, provisioning, and support
2. **Enterprise Security:** Industry-leading security with hardened PHP, advanced WAF, brute force protection, and antivirus scanning
3. **Scalability:** Support growth from 1 server to 10,000+ servers with zero per-server licensing costs
4. **Automation:** Fully automated billing, provisioning, domain management, and support workflows
5. **Performance:** Optimize website performance with integrated caching (Varnish, Redis, Opcode)
6. **User Experience:** Intuitive interface for all user types with mobile responsiveness and white-label branding

1.3 Success Metrics

- **Deployment Time:** < 30 minutes for initial server setup
- **Security:** Zero-day vulnerability protection with < 1 hour patch deployment
- **Performance:** Support 10,000+ websites per server cluster with 99.9% uptime
- **Automation:** 95% reduction in manual provisioning and billing tasks
- **Customer Satisfaction:** > 4.5/5.0 customer rating across all user types

2. User Personas

2.1 Hosting Provider Administrator (Primary)

Profile: IT professional managing hosting infrastructure for multiple customers
Goals:

- Efficiently manage multi-server hosting clusters
- Automate billing and provisioning workflows
- Monitor security threats and performance metrics
- Scale infrastructure without complexity
  Pain Points:
- Manual provisioning wastes time
- Multiple separate systems for hosting, billing, and support
- Security threats require constant vigilance
- Scaling is complex and expensive

2.2 Reseller (Secondary)

Profile: Business offering white-labeled hosting services
Goals:

- Manage multiple customer accounts under own brand
- Create and sell custom hosting packages
- Provide support to end customers
- Generate revenue from hosting services
  Pain Points:
- Limited branding capabilities
- Complex customer management
- Difficulty tracking profitability per customer

2.3 End Customer / Website Owner (Tertiary)

Profile: Individual or small business running websites
Goals:

- Easy website management without technical expertise
- Fast website performance
- Reliable email and domain services
- Quick support when needed
  Pain Points:
- Complex control panels
- Slow website loading times
- Security concerns about hacking
- Poor customer support

3. Core Feature Requirements

3.1 Security Features

3.1.1 PHP Hardening (CloudLinux-Inspired)

Requirement: Implement enterprise-grade PHP security hardening to protect against vulnerabilities in older PHP versions.

Detailed Specifications:

Multi-Version PHP Security Patching

- Backport security patches to unsupported PHP versions (5.4, 5.5, 5.6, 7.0, 7.1, 7.2)
- Maintain patch database covering 100+ known vulnerabilities
- Automatic security patch deployment within 24 hours of discovery
- Version-specific vulnerability tracking and remediation
- Security bulletin notifications for affected customers

PHP Selector

- Support PHP versions: 5.4, 5.5, 5.6, 7.0, 7.1, 7.2, 7.3, 7.4, 8.0, 8.1, 8.2, 8.3
- Per-website PHP version selection
- Support for 120+ PHP extensions
- Per-site extension enable/disable capability
- Extension compatibility validation per PHP version
- One-click PHP version switching with zero downtime

PHP Security Directives

- **disable_functions:** Restrict dangerous functions (exec, shell_exec, system, passthru, proc_open, popen, curl_exec, curl_multi_exec, parse_ini_file, show_source)
- **open_basedir:** Enforce per-domain file system restrictions preventing directory traversal
- **allow_url_fopen:** Disabled by default to prevent remote file inclusion
- **allow_url_include:** Disabled to prevent RFI attacks
- **expose_php:** Hidden to prevent version disclosure
- **register_globals:** Disabled to prevent variable injection
- **magic_quotes_gpc:** Disabled (deprecated security feature)
- **file_uploads:** Configurable per site with upload size limits
- **max_execution_time:** Adjustable per site (30-300 seconds)
- **memory_limit:** Configurable per site (64M-512M)

PHP Configuration Management

- Global configuration file: /etc/php/secure.conf
- Per-user PHP configuration overrides
- Per-site PHP.ini customization interface
- Real-time configuration updates without service restart
- PHP-FPM pool isolation per website with dedicated pool configurations
- Resource limits per PHP-FPM pool (memory, CPU, processes)

Extension Security Management

- Whitelist/blacklist PHP extensions per user or per site
- Automatic vulnerability scanning for installed extensions
- Extension version control with automatic security updates
- Incompatibility warnings when enabling risky extension combinations
- Custom extension upload and installation (with security scanning)

User Actions:

- Admins can enforce global PHP security policies
- Customers can select PHP version and enable/disable allowed extensions
- Admins receive alerts for sites using vulnerable PHP versions
- Automated migration tools to upgrade PHP versions with testing capability

3.1.2 Enterprise-Grade Web Application Firewall (WAF)

Requirement: Deploy comprehensive WAF system to protect against sophisticated web attacks, DDoS, and malicious traffic.

Detailed Specifications:

ModSecurity Integration

- Full ModSecurity v3.x engine integration
- OWASP Core Rule Set (CRS) 3.3+ with automatic updates
- Real-time rule updates from global threat intelligence feeds (multiple sources)
- Custom rule creation interface with regex pattern builder
- Rule testing sandbox environment
- Per-site WAF configuration (enable/disable, rule selection)
- Global WAF configuration with site overrides
- Rule tuning wizard to reduce false positives
- Performance mode settings (DetectionOnly, On, Off)

WAF Rule Categories with Detailed Protection

SQL Injection Protection:

- Detect SQL injection in GET/POST parameters, cookies, headers
- Protection against: UNION-based injection, Boolean-based blind injection, Time-based blind injection, Error-based injection, Stacked queries
- Database-specific protection (MySQL, PostgreSQL, MSSQL, Oracle)
- Encoded payload detection (Base64, Hex, URL encoding)

Cross-Site Scripting (XSS) Protection:

- Reflected XSS detection and blocking
- Stored XSS prevention through input sanitization
- DOM-based XSS protection
- JavaScript event handler injection blocking
- HTML tag injection prevention
- SVG-based XSS protection

Cross-Site Request Forgery (CSRF) Protection:

- Automatic CSRF token generation and validation
- Referer header validation
- Custom header requirement for state-changing operations
- Double-submit cookie pattern support

Remote File Inclusion (RFI) / Local File Inclusion (LFI) Protection:

- Block external URL inclusion attempts
- Prevent directory traversal attacks (../, .., etc.)
- Null byte injection protection

- PHP wrapper exploitation prevention

Command Injection Protection:

- Shell command injection detection (bash, sh, cmd)
- Code execution attempt blocking
- Environment variable manipulation prevention

Protocol Attack Protection:

- HTTP protocol violation detection
- Malformed request blocking
- HTTP method enforcement (whitelist GET, POST, HEAD, etc.)
- Header size limit enforcement
- Request size limit enforcement

Session Fixation Protection:

- Session ID randomization
- Session regeneration on authentication
- Cookie security flags enforcement (Secure, HttpOnly, SameSite)

DDoS Protection

Layer 7 DDoS Mitigation:

- Application-layer attack detection (SlowLoris, Slow POST, HTTP flood)
- Connection rate limiting per IP (configurable: 10-1000 req/min)
- Concurrent connection limiting per IP
- Request pattern analysis for attack detection
- Adaptive rate limiting based on server load

Challenge-Response System:

- JavaScript challenge for suspicious traffic
- CAPTCHA integration (reCAPTCHA v2, v3, hCaptcha, custom)
- Challenge difficulty adjustment based on threat level
- Automatic challenge triggering rules

Behavioral Analysis:

- Machine learning model for traffic pattern analysis
- Anomaly detection for unusual request patterns
- Session behavior tracking
- Request velocity monitoring

Geographic Blocking:

- Country-based traffic filtering (allow/block lists)
- Region-based restrictions
- City-level geo-blocking support
- Automatic blocking of high-risk countries

ASN Blocking:

- Autonomous System Number (ASN) blocking
- Block entire hosting providers known for abuse
- Datacenter IP range blocking
- Cloud provider IP filtering

Bot Protection

Good Bot Whitelist:

- Search engine crawlers (Google, Bing, Yahoo, Baidu, Yandex)
- Monitoring services (Pingdom, UptimeRobot, StatusCake)
- Social media crawlers (Facebook, Twitter, LinkedIn)
- Feed readers and aggregators
- Custom good bot additions

Bad Bot Blacklist:

- Known malicious bots database (10,000+ signatures)
- Content scrapers and harvesters
- Vulnerability scanners
- Spam bots and email harvesters
- SEO crawlers (aggressive)
- Automated testing tools
- Custom bad bot additions

Bot Signature Detection:

- User-Agent string analysis
- HTTP header pattern matching
- Request frequency analysis
- Mouse movement and keyboard tracking (JavaScript)

Honeypot Traps:

- Hidden form fields to catch automated submissions
- Hidden links invisible to humans
- Trap URLs that only bots would access
- Cookie validation for bot detection

JavaScript Challenge:

- Verify browser JavaScript execution capability
- Math problem solving challenges
- Timed challenges
- Invisible challenges for legitimate users

Browser Fingerprinting:

- Canvas fingerprinting
- WebGL fingerprinting
- Audio context fingerprinting
- Font fingerprinting
- Screen resolution and color depth tracking
- Plugin detection

IP Reputation & Threat Intelligence

Real-Time IP Reputation Database:

- Integrate with 5+ major IP reputation services
- Local reputation database with 100M+ IP records
- Reputation scoring (0-100 scale)

- Dynamic reputation updates every 5 minutes
- Historical attack data per IP

Global Threat Intelligence Integration:

- AlienVault OTX integration
- AbuseIPDB integration
- Spamhaus integration
- Emerging Threats ruleset
- Custom threat feed support via API

Automatic IP Blacklisting:

- Dynamic blacklist based on attack attempts
- Progressive penalty system (warning → temporary ban → permanent ban)
- Automatic blacklist duration: 1 hour to 30 days
- Global blacklist sharing across clustered servers

IP Whitelist Management:

- Admin IP whitelist (never block admins)
- Partner/API IP whitelist
- Network range whitelisting (CIDR notation)
- Time-based temporary whitelist
- Automatic whitelist for successful 2FA logins

Geolocation-Based Blocking:

- MaxMind GeoIP2 integration
- Country, region, city-level blocking
- Continent-level blocking
- Custom geo-fence creation
- Temporary geo-block during attacks

Tor Exit Node Blocking:

- Tor exit node IP database (updated hourly)
- Optional Tor access allowing
- Tor detection with challenge requirement
- VPN/Proxy detection and blocking

Advanced Threat Detection

Machine Learning-Based Anomaly Detection:

- Train ML models on normal traffic patterns per site
- Detect deviations from baseline behavior
- Adaptive learning from blocked attacks
- False positive feedback loop
- Per-site custom ML models

Zero-Day Attack Protection:

- Heuristic analysis of requests
- Behavior-based threat detection
- Signature-less malware detection
- Exploit attempt detection (buffer overflows, format strings)

- Unknown payload analysis

Malware Upload Prevention:

- Real-time file upload scanning
- Signature-based malware detection (ClamAV integration)
- Heuristic malware analysis
- Archive scanning (zip, tar, rar, 7z)
- Polymorphic malware detection
- File type validation (prevent executable disguised as image)
- Maximum upload size enforcement

Phishing Protection:

- Detect phishing pages by content analysis
- Domain typosquatting detection
- SSL certificate validation for external links
- Brand name hijacking detection
- Fake login page detection

API Abuse Protection:

- API rate limiting per API key
- OAuth token validation
- JWT token verification
- API authentication brute force protection
- API endpoint-specific rate limits
- GraphQL query complexity analysis

Credential Stuffing Protection:

- Detect automated login attempts using stolen credentials
- Password spray attack detection
- Multi-account login attempt correlation
- CAPTCHA requirement after X failed attempts
- Alert legitimate users of credential compromise

WAF Logging & Monitoring

Real-Time Attack Logging:

- Log all blocked requests with full details (IP, URL, payload, rule triggered)
- Log severity levels (Critical, High, Medium, Low, Info)
- Attack categorization (SQLi, XSS, RFI, etc.)
- Request and response headers
- Full request body for forensic analysis
- Geo-location data for each request

WAF Dashboard:

- Real-time attack visualization (attacks per second)
- Attack type distribution (pie chart, bar graph)
- Top attacking IPs (with WHOIS lookup)
- Top attacked URLs
- Geographic heat map of attacks

- Time-series graphs (hourly, daily, weekly, monthly)
- False positive rate tracking
- WAF effectiveness metrics

Alert Notifications:

- Email alerts for critical attacks
- SMS alerts for DDoS and major incidents
- Webhook integration for custom alerts
- Slack/Discord/Telegram integration
- Alert thresholds (trigger after X attacks in Y minutes)
- Alert aggregation to prevent spam
- Alert escalation rules

Log Retention:

- Configurable log retention (30 days to 1 year)
- Log compression for space efficiency
- Archive old logs to S3-compatible storage
- On-demand log export (CSV, JSON, syslog format)

SIEM Integration:

- Syslog export to external SIEM systems
- CEF (Common Event Format) support
- Integration with Splunk, ELK Stack, Graylog
- Real-time log streaming via API
- Pre-built SIEM dashboards and parsers

Forensic Analysis Tools:

- Request replay capability for testing
- Attack pattern visualization
- Attacker behavior timeline
- IP investigation tools (WHOIS, geolocation, reputation)
- Traffic comparison (before/during/after attack)
- Export investigation reports (PDF format)

Response Actions

Action Types:

- **Block:** Immediate request termination (403 Forbidden)
- **Challenge:** Present CAPTCHA or JavaScript challenge before allowing access
- **Tarpit:** Intentionally slow down suspicious requests (delay 5-30 seconds)
- **Log Only:** Monitor and log without blocking (testing mode)
- **Alert:** Log and send alert notification but allow request
- **Redirect:** Redirect to safe page or honeypot

Custom Error Pages:

- Branded error pages for blocked requests
- Customizable HTML templates
- Multi-language support
- Contact information display

- Appeal process information
- Unique incident ID for support reference

Automatic IP Banning:

- Progressive penalty system:
  - 1st violation: Log only
  - 2nd-3rd violations: CAPTCHA challenge
  - 4th-5th violations: 1-hour IP ban
  - 6+ violations: 24-hour IP ban
  - 10+ violations: Permanent ban (admin review required)
- Configurable penalty thresholds
- Automatic ban expiration
- Ban appeal process
- Whitelist bypass for penalties

User Actions:

- Admins configure global WAF rules and policies
- Per-site WAF customization by admins or site owners
- View real-time attack dashboard
- Investigate individual attacks
- Manually ban/unban IPs
- Create custom WAF rules
- Test WAF rules in sandbox mode
- Export attack reports
- Configure alert notifications

3.1.3 Brute Force Protection

Requirement: Implement multi-layered protection against brute force attacks across all authentication points.

Detailed Specifications:

Login Protection

Progressive Delay System:

- Exponential backoff algorithm for failed login attempts
- Delay formula: delay = 2^(failed_attempts) seconds
  - 1st failure: 2 seconds delay
  - 2nd failure: 4 seconds delay
  - 3rd failure: 8 seconds delay
  - 4th failure: 16 seconds delay
  - 5th+ failure: 25 seconds delay (maximum)
- Per-IP and per-account delay tracking
- Delay reset after successful login
- Bypass delay for whitelisted IPs

Maximum Attempt Threshold:

- Configurable maximum failed attempts (default: 5)
- Account lockout after threshold reached
- Lockout duration: 5 minutes to 24 hours (configurable)

- Progressive lockout: longer duration for repeat lockouts
- Unlock methods: time expiration, admin unlock, email verification link

Temporary IP Banning:

- Ban IPs with excessive failed login attempts across multiple accounts
- Ban duration: 30 minutes to 24 hours
- Threshold: 10 failed attempts in 10 minutes (configurable)
- Ban applies to all services (control panel, email, FTP, SSH)
- Automatic unban after duration expires

Permanent IP Blacklist:

- Manually add IPs to permanent blacklist
- Automatically add IPs with severe abuse (50+ failures in 1 hour)
- Blacklist applies cluster-wide across all servers
- Import/export blacklist functionality
- CIDR range support for network blocks

Account Lockout Duration:

- Short lockout: 5 minutes (for low-risk accounts)
- Medium lockout: 30 minutes (default)
- Long lockout: 24 hours (for high-risk accounts or admins)
- Permanent lockout: requires admin intervention
- Configurable per user role and account type

Two-Factor Authentication (2FA):

- Optional or mandatory 2FA per user role
- Supported methods: TOTP (Google Authenticator, Authy), SMS, Email, Hardware tokens (FIDO2/U2F)
- Backup codes for account recovery
- Trust device for X days option
- Force 2FA re-authentication for sensitive actions

Service-Level Protection

SSH Brute Force Protection:

- Monitor SSH login attempts via PAM integration
- Fail2Ban integration with custom SSH jail
- Ban after X failed attempts (default: 3)
- Ban duration: 1 hour to permanent
- Whitelist admin IPs from SSH bans
- Public key authentication enforcement option
- Disable password authentication option
- SSH port customization
- Log all SSH attempts (successful and failed)

FTP Brute Force Protection:

- Monitor FTP authentication attempts
- Ban IPs with failed FTP logins
- Threshold: 5 failures in 5 minutes
- Per-user FTP account lockout

- Enforce FTPS/SFTP over plain FTP
- IP whitelist for FTP access
- FTP access time restrictions (allow only during business hours)

Email Authentication Protection:

- SMTP authentication brute force detection
- POP3/IMAP authentication monitoring
- Ban IPs attempting email relay abuse
- Temporary suspension of email accounts under attack
- Alert users of suspicious email login attempts
- Require strong passwords for email accounts

Control Panel Login Protection:

- Separate brute force protection for admin panel
- More restrictive thresholds for admin accounts
- CAPTCHA after 3 failed admin login attempts
- IP whitelist for admin access
- Geolocation-based admin access restrictions
- Admin login notifications (email, SMS)
- Admin session timeout (15 minutes default)

API Authentication Protection:

- API key brute force protection
- Rate limiting per API key: 60 requests per minute (configurable)
- Temporary API key suspension after abuse
- OAuth token validation with rate limits
- API authentication attempt logging
- Alert on suspicious API usage patterns

Database Login Protection:

- Monitor database authentication attempts (MySQL, PostgreSQL)
- Restrict database access to localhost by default
- IP whitelist for remote database connections
- Database user account lockout
- Log all database connection attempts
- Alert on unauthorized database access attempts

CAPTCHA Integration

Automatic CAPTCHA Triggering:

- Show CAPTCHA after X failed login attempts (default: 3)
- CAPTCHA difficulty scales with threat level
- Time-based CAPTCHA expiration (5 minutes)
- Configurable CAPTCHA trigger thresholds per service

Multiple CAPTCHA Providers:

- reCAPTCHA v2 (I'm not a robot checkbox)
- reCAPTCHA v3 (invisible, score-based)
- hCaptcha (privacy-focused alternative)

- Custom CAPTCHA (math problems, image selection)
- Provider failover if primary is unavailable

Invisible CAPTCHA:

- reCAPTCHA v3 for transparent bot detection
- Score threshold: 0.5 (configurable 0.0-1.0)
- Challenge only low-scoring requests
- No user interaction for legitimate users

Audio CAPTCHA:

- Accessibility option for visually impaired users
- Audio puzzle with numbers and letters
- Background noise to prevent automated solving
- Option to refresh audio challenge

Custom CAPTCHA Difficulty:

- Easy: Simple checkbox or single image selection
- Medium: Multiple image selection or simple math
- Hard: Complex image puzzles or distorted text
- Difficulty auto-adjustment based on threat assessment

Whitelist Management

Trusted IP Whitelist:

- Never block whitelisted IPs
- Bypass all brute force protections
- Applies to all services
- Support for single IPs and CIDR ranges
- Comments/notes for each whitelisted IP

Admin IP Whitelist:

- Separate whitelist specifically for admin access
- Auto-whitelist on first successful admin login (optional)
- Two-factor authentication still required
- Admin IPs never subject to bans

Partner/API Whitelist:

- Permanent access for integrated systems and partners
- Whitelist for API keys and service accounts
- Separate rate limits for whitelisted partners
- Monitoring of whitelisted activity

Time-Based Whitelist:

- Temporary whitelist for specific duration (1 hour to 30 days)
- Use cases: maintenance, migrations, third-party audits
- Automatic removal after expiration
- Email notification before expiration

Network Range Whitelist:

- Allow entire office networks or data centers
- CIDR notation support (e.g., 192.168.1.0/24)

- IPv4 and IPv6 support
- Subnet calculator tool

Detection & Response

Real-Time Attack Detection:

- Monitor all authentication endpoints simultaneously
- Detect brute force attacks within seconds
- Correlation of attacks across multiple IPs
- Attack pattern recognition (sequential, distributed)
- Immediate blocking of detected attacks

Distributed Attack Protection:

- Detect coordinated attacks from multiple IPs
- Botnet detection via behavior correlation
- Automatic IP range blocking for distributed attacks
- Global threat sharing across clustered servers
- Machine learning for botnet pattern detection

Password Complexity Enforcement:

- Minimum password length: 8 characters (configurable 8-32)
- Require uppercase, lowercase, numbers, symbols
- Dictionary word prevention
- Common password blacklist (10,000+ passwords)
- Password strength meter (weak, medium, strong)
- Custom password policies per user role

Password History:

- Prevent password reuse for last X passwords (default: 5)
- Password expiration policy (30, 60, 90 days)
- Force password change on first login
- Password age tracking

Failed Attempt Notifications:

- Email users after failed login to their account
- Include IP address, location, timestamp
- "Was this you?" confirmation link
- Option to immediately change password
- Lock account if user reports unauthorized attempt

Geolocation-Based Alerts:

- Alert on logins from unusual countries/regions
- Whitelist common user locations
- Suspicious location triggers 2FA even if normally disabled
- Travel mode to temporarily allow global access
- Login location history visualization

Integration Features

Fail2Ban Integration:

- Native Fail2Ban jail configurations

- Custom filters for panel-specific logs
- Coordinated banning across all protected services
- Fail2Ban status monitoring in dashboard
- Manual ban/unban via control panel

PAM Module Integration:

- Linux Pluggable Authentication Modules (PAM) integration
- System-level authentication protection
- Applies to SSH, FTP, and local logins
- pam_faillock for account lockouts
- pam_pwquality for password policies

OSSEC Active Response:

- OSSEC integration for intrusion detection
- Automated response to brute force attacks
- Firewall rule updates via OSSEC
- Log correlation across services
- Custom OSSEC rules for panel-specific threats

Imunify360 Compatible:

- Works alongside Imunify360 if installed
- Share threat intelligence with Imunify
- Coordinated blocking decisions
- Avoid duplicate protections
- Unified security dashboard

Custom Scripts Support:

- Execute custom bash/python scripts on attack detection
- Webhook notifications for external integration
- Custom response actions (e.g., notify Slack, create ticket)
- Script execution with full context (IP, user, service, attempt count)
- Script library with community-contributed responses

User Actions:

- Admins configure brute force protection policies globally
- View real-time brute force attack dashboard
- Manually ban/unban IPs
- Review locked accounts and unlock if necessary
- Configure email notifications for brute force events
- Whitelist trusted IPs
- Export brute force logs
- Customers receive alerts of failed login attempts to their accounts
- Customers can enable/configure 2FA for their accounts

3.1.4 Antivirus & Malware Protection

Requirement: Deploy comprehensive malware detection, quarantine, and remediation system to protect websites and server infrastructure.

Detailed Specifications:

Real-Time Scanning

On-Access Scanning:

- Scan files as they are read, written, or executed
- Kernel-level integration for low latency
- Whitelist system files and trusted applications
- Configurable scan depth (full or quick)
- Automatic quarantine of infected files before access
- Performance-optimized scanning (< 100ms per file)

On-Upload Scanning:

- Intercept all file uploads (HTTP, FTP, WebDAV)
- Scan files before saving to disk
- Block malicious uploads immediately
- Support for all file types and archives
- Upload size limit: up to 1GB per file
- Progress indicator for large file scans

Email Attachment Scanning:

- Scan all incoming email attachments
- Scan outgoing attachments to prevent spreading
- Support for all email protocols (SMTP, POP3, IMAP)
- Archive scanning within attachments (zip, rar, 7z)
- Automatic quarantine of malicious attachments
- Email sender notification of blocked attachments

Background Scanning:

- Scheduled full system scans (daily, weekly, monthly)
- Incremental scans of changed files only
- Low-priority scanning to avoid performance impact
- Scan during off-peak hours (configurable schedule)
- Scan specific directories or entire server
- Report generation after each scan

Change Detection:

- File Integrity Monitoring (FIM) for critical files
- Detect unauthorized file modifications
- Baseline creation for clean file states
- Real-time alerts on file changes
- Scan modified files immediately
- Rollback capability for critical system files

Memory Scanning:

- Detect malware running in memory

- Rootkit detection in kernel space
- Process injection detection
- Scan running processes for malicious code
- Fileless malware detection
- Terminate malicious processes automatically

Malware Detection

Signature-Based Detection:

- Malware signature database: 10 million+ signatures
- Signatures updated hourly from ClamAV and commercial feeds
- Support for multiple signature formats (hash, bytecode, YARA)
- Regular expression signatures for polymorphic malware
- Signature-based scanning speed: 10MB/s per CPU core
- Database size: ~200MB compressed

Heuristic Analysis:

- Behavior-based detection for unknown malware
- Analyze file structure, code patterns, entropy
- Detect packing and obfuscation techniques
- Identify suspicious function calls
- File type mismatch detection (e.g., .jpg contains PHP)
- Heuristic sensitivity: low, medium, high (configurable)

AI-Powered Detection:

- Machine learning models trained on millions of malware samples
- Deep learning for zero-day threat detection
- Trained to detect: webshells, backdoors, trojans, ransomware, adware
- ML model updates weekly
- Local inference for privacy (no cloud upload)
- ML detection accuracy: >98% with <1% false positive rate

Exploit Detection:

- Identify exploit attempts in uploaded files
- Detect: buffer overflows, format string attacks, code injection
- Analyze shellcode patterns
- Detect exploit kits (RIG, Angler, Neutrino)
- Prevent privilege escalation exploits

Backdoor Detection:

- Detect hidden backdoors in PHP, Python, Perl, Ruby files
- Common backdoor signatures: c99, r57, WSO, b374k, etc.
- Encrypted backdoor detection via entropy analysis
- Base64-encoded backdoor detection
- Detect backdoor persistence mechanisms

Webshell Detection:

- Specialized detection for PHP, ASP, JSP, CGI webshells
- Pattern matching for common webshell functions (eval, exec, system)

- Detect obfuscated webshells (hex, base64, gzip)
- YARA rules for advanced webshell detection
- Database of 5,000+ known webshell variants

Ransomware Detection:

- Early detection of file encryption activity
- Monitor for rapid file modification patterns
- Detect ransom note files (README.txt, HOW_TO_DECRYPT.html)
- Known ransomware family signatures (WannaCry, Locky, Cryptolocker)
- Automatic file backup before encryption detected
- Kill ransomware processes immediately

Quarantine & Remediation

Automatic Quarantine:

- Isolate infected files immediately upon detection
- Move to secure quarantine directory (/var/quarantine)
- Encrypted storage for quarantined files
- Quarantine retention: 30 days (configurable)
- Prevent execution of quarantined files
- Automatic quarantine notifications to admins and users

Manual Review Interface:

- Admin dashboard for quarantine management
- List all quarantined files with metadata (path, date, threat type)
- View file contents safely (sandboxed preview)
- VirusTotal integration for second opinion
- False positive reporting mechanism
- Batch operations on multiple files

One-Click Cleanup:

- Remove all quarantined files with one click
- Smart cleanup: delete confirmed threats, preserve suspected files
- Cleanup confirmation prompts
- Post-cleanup verification scan
- Cleanup logs for audit trail

Backup Before Cleanup:

- Automatic backup of files before removal
- Backup retention: 7 days
- Compressed backups to save space
- Restore from backup option
- Backup verification checksums

Restore from Quarantine:

- Restore false positives to original location
- Whitelist restored files to prevent re-quarantine
- Restore permissions and ownership
- Verify file integrity after restore

- Log all restore operations

Infection Report:

- Detailed report after each scan
- Information included: total files scanned, infections found, threats by type, infected file paths, actions taken
- PDF report generation
- Email report to admins and affected users
- Historical report comparison
- Executive summary for non-technical users

Proactive Protection

File Integrity Monitoring (FIM):

- Monitor critical directories for unauthorized changes
- Monitored paths: /etc, /usr/bin, /var/www, WordPress core files
- Detect: file addition, deletion, modification, permission changes
- Real-time alerts on changes
- Baseline comparison
- Integration with malware scanner for changed files

Critical File Protection:

- Read-only protection for system files
- Immutable flags on critical binaries
- Prevent modification of: passwd, shadow, sudoers, cron files
- Require explicit admin unlock to modify protected files
- Audit log of protection override attempts

Upload Restrictions:

- Block dangerous file extensions: .exe, .dll, .bat, .cmd, .com, .pif, .scr, .vbs, .js
- Configurable extension blacklist per site
- MIME type validation (prevent disguised executables)
- File content inspection (ignore extension, check actual content)
- Archive inspection (scan inside zip, tar, rar)
- Maximum upload size enforcement

Script Injection Prevention:

- Detect malicious code injection in legitimate files
- Monitor PHP, JS, Python files for suspicious additions
- Base64-encoded injection detection
- Iframe injection detection
- Redirect injection detection (spam SEO)
- Automatic removal of injected code with file restoration

Database Malware Scanning:

- Scan MySQL and PostgreSQL databases for malicious content
- Detect: SQL injection payloads, spam links, phishing redirects
- Scan tables: posts, pages, options, users (WordPress)
- Clean database entries automatically or prompt admin
- Database backup before cleanup

- Schedule database scans weekly

Configuration File Monitoring:

- Monitor changes to: .htaccess, wp-config.php, config.php
- Alert on suspicious directives (auto_prepend_file, auto_append_file)
- Detect unauthorized user additions in CMS configs
- Backup configuration files on changes
- Revert unauthorized changes automatically

Scanning Configuration

Scheduled Scans:

- Daily quick scan: scan uploads and web directories only
- Weekly full scan: scan entire website directories
- Monthly deep scan: scan entire server including system files
- Custom scan schedules per site or server
- Staggered scan timing to balance load
- Pause/resume scan capability

Quick Scans:

- Rapid scan of high-risk areas
- Focus on: uploads, tmp, cache, plugins, themes
- Skip static files (images, videos, PDFs)
- Scan duration: 1-5 minutes per site
- On-demand quick scan button

Custom Scan Paths:

- Define specific directories to scan or exclude
- Per-site scan path configuration
- Regex pattern support for path matching
- Include/exclude rules
- Scan external mount points (NFS, CIFS)

Exclusion Lists:

- Skip known-good files from scanning (whitelist)
- Exclude by: file path, file name pattern, file hash
- Per-site exclusions
- Global exclusions for system files
- Trusted vendor exclusions (WordPress core, plugins from official repo)

Scan Depth Control:

- Configure maximum directory recursion depth
- Limit: 1-100 levels (default: unlimited)
- Skip deep nested directories to improve performance
- Symbolic link following: on/off

Performance Tuning:

- Adjust scan intensity: low, medium, high
- CPU priority: nice value adjustment (10-19)
- I/O priority: ionice class adjustment

- Concurrent scan threads: 1-8
- Scan rate limiting: max MB/s
- Adaptive scanning based on server load

Threat Intelligence

Automatic Signature Updates:

- Hourly updates from ClamAV
- Daily updates from commercial feeds
- Delta updates to minimize bandwidth
- Automatic retry on update failure
- Update verification via digital signatures
- Rollback to previous signatures if issues detected

Global Threat Feeds:

- Integration with multiple sources:
  - ClamAV official signatures
  - Malware Hash Registry (MHR)
  - VirusTotal API
  - AlienVault OTX
  - abuse.ch feeds (URLhaus, MalwareBazaar)
- Custom threat feed support via URL
- STIX/TAXII protocol support
- Threat feed priority and weighting

Reputation Scoring:

- File reputation based on global prevalence
- Domain reputation for external links
- IP reputation for connection sources
- Reputation score: 0-100 (0=malicious, 100=trusted)
- Whitelist high reputation files to reduce scans
- Alert on low reputation file execution

IOC Detection (Indicators of Compromise):

- Detect known malicious file hashes (MD5, SHA1, SHA256)
- Detect known malicious URLs and domains
- Detect known malicious IP addresses
- Detect known malicious email addresses
- YARA rule matching for complex IOCs
- Automatic IOC updates from threat feeds

Threat Correlation:

- Connect related security events across services
- Detect multi-stage attacks
- Timeline visualization of attack progression
- Attribution to known threat actors
- Kill chain analysis

Notifications & Reporting

Real-Time Alerts:

- Immediate notification on malware detection
- Alert methods: email, SMS, webhook, Slack, Telegram
- Alert priority levels: critical, high, medium, low
- Alert aggregation to prevent spam
- Per-site alert configuration
- Admin and customer alert separation

Email Reports:

- Daily security summary email
- Weekly comprehensive report
- Monthly executive report
- Customizable report content
- HTML and PDF report formats
- Scheduled report delivery

Dashboard Visualization:

- Real-time malware detection statistics
- Threat type distribution (pie chart)
- Infection timeline (line graph)
- Top infected sites/users
- Scan coverage percentage
- Clean vs infected file ratio
- Quarantine storage usage

Scan History:

- Complete audit trail of all scans
- Historical scan results comparison
- Trend analysis (improving or worsening)
- Exportable scan logs (CSV, JSON)
- Per-site scan history
- Filter by date range, scan type, result

Threat Timeline:

- Chronological view of all security events
- Event types: detection, quarantine, cleanup, restore
- Drill-down into individual events
- Export timeline for reporting
- Visual indicators for severity

Compliance Reports:

- PCI-DSS compliance report
- HIPAA compliance report
- GDPR data breach reporting
- SOC 2 security report
- ISO 27001 documentation
- Customizable compliance templates

Integration

ClamAV Integration:

- ClamAV 1.0+ as primary scanning engine
- Clamscan for on-demand scans
- Clamd daemon for real-time scanning
- Freshclam for signature updates
- Custom ClamAV signature support
- Clamonacc for on-access scanning (Linux 5.0+)

Imunify360 Compatible:

- Detect Imunify360 installation
- Coordinate scanning to avoid duplication
- Share malware findings between systems
- Unified security dashboard
- Single point of malware management

Custom Scanner API:

- RESTful API for third-party scanner integration
- API endpoints: scan file, get results, quarantine, restore
- API authentication via API keys
- Rate limiting on API calls
- Webhook callbacks for scan completion

Webhook Notifications:

- POST malware detection events to external URLs
- Configurable webhook payloads (JSON)
- Retry logic for failed webhooks
- Webhook signature verification
- Multiple webhook destinations

SIEM Export:

- Export security events to SIEM systems
- Formats: Syslog, CEF, JSON
- Supported SIEMs: Splunk, ELK, Graylog, QRadar
- Real-time event streaming
- Historical event export

User Actions:

- Admins configure global antivirus policies
- Schedule scans globally or per site
- View real-time malware dashboard
- Review quarantined files and take actions
- Manually scan specific files or directories
- Configure alert notifications
- Generate compliance reports
- Customers receive alerts when malware detected on their sites
- Customers view scan results and clean their sites
- Customers whitelist known-good files

3.1.5 Additional Enterprise Security Features

CageFS / User Isolation

Virtualized File System:

- Each user operates in isolated virtual file system
- Users cannot see files owned by other users
- Chroot-like environment per user
- Isolated /tmp, /var/tmp per user
- Prevent access to /etc/passwd, /etc/shadow
- Per-user /proc to hide other processes

Symlink Attack Prevention (SecureLinks):

- Kernel-level symbolic link protection
- Prevent symlink attacks in WebDAV, FTP, file managers
- Block symlink creation to files user doesn't own
- Block hardlink attacks
- Protect system files from symlink exploitation

Process Isolation:

- Users cannot see other users' processes via ps, top
- Prevent ptrace attacks between users
- Dedicated process namespace per user
- Kill all user processes on logout

Resource Visibility Isolation:

- Hide system-wide CPU, memory, load stats
- Users see only their own resource usage
- Prevent information leakage about server capacity
- Per-user /proc/cpuinfo, /proc/meminfo

Intrusion Detection System (IDS)

Host-Based Intrusion Detection (OSSEC Integration):

- Real-time log analysis and correlation
- File integrity monitoring
- Rootkit detection (rkhunter integration)
- Active response to threats
- Alerting and reporting
- Central management for clustered servers

File System Monitoring:

- Monitor file access patterns for suspicious activity
- Detect rapid file access (data exfiltration)
- Alert on access to sensitive files
- Monitor file creation in unusual locations
- Detect privilege escalation attempts

Log Analysis:

- Parse logs from all services (Apache, NGINX, MySQL, FTP, email)
- Correlate events across services

- Detect attack patterns (SQL injection, XSS, LFI, RFI)
- Anomaly detection based on baseline
- Custom log parsing rules

Rootkit Detection:

- Scan for rootkits daily
- Detect kernel-level rootkits
- Check for modified system binaries
- Verify checksums of critical files
- Network-level rootkit detection

System Integrity Verification:

- Verify integrity of system binaries
- Compare against known-good checksums
- Detect binary trojans
- Alert on unexpected binary modifications
- Automatic restoration from clean sources

SSL/TLS Security

Automatic SSL Provisioning:

- Free Let's Encrypt SSL certificates for all sites
- Automatic issuance within 5 minutes of site creation
- Support for domain and wildcard certificates
- Automatic renewal 30 days before expiration
- Multi-domain SAN certificates support

SSL Certificate Monitoring:

- Track expiration dates for all certificates
- Email alerts 30, 14, 7, 1 days before expiration
- Dashboard showing all certificate statuses
- Renewal failure alerts
- Certificate chain validation

Strong Cipher Enforcement:

- Disable SSLv2, SSLv3, TLS 1.0, TLS 1.1
- Enable only TLS 1.2 and TLS 1.3
- Configure strong cipher suites (ECDHE, AES-GCM)
- Disable weak ciphers (RC4, DES, MD5)
- Perfect Forward Secrecy (PFS) enforcement
- A+ rating on SSL Labs test

HSTS Support (HTTP Strict Transport Security):

- Force HTTPS for all site connections
- HSTS headers with max-age=31536000
- includeSubDomains directive
- preload directive for HSTS preload list
- Per-site HSTS configuration

TLS 1.3 Support:

- Enable latest TLS 1.3 protocol
- Faster handshake (1-RTT, 0-RTT)
- Improved security with modern ciphers
- Backward compatibility with TLS 1.2
- Configurable per site

Certificate Pinning:

- HTTP Public Key Pinning (HPKP)
- Pin certificates to prevent MITM attacks
- Backup pins for certificate rotation
- Report-only mode for testing
- Per-site pinning configuration

Security Hardening

Secure Hardened Kernel:

- Grsecurity-based kernel patches
- ASLR (Address Space Layout Randomization)
- Stack smashing protection
- Kernel module signing enforcement
- Disable unprivileged user namespaces

Disable Unnecessary Services:

- Audit running services on installation
- Stop and disable: telnet, rsh, rlogin, FTP (in favor of SFTP)
- Remove unnecessary packages
- Minimize attack surface
- Service dependency analysis

Secure Default Configurations:

- Security-first configuration templates
- Strong password policies by default
- Encrypted communication by default
- Minimal permissions by default
- Fail-safe defaults (deny-by-default)

Regular Security Updates:

- Automated security patch deployment
- Zero-day patch deployment within 24 hours
- Kernel live patching (no reboot required)
- Package verification before installation
- Rollback capability for problematic updates
- Maintenance window scheduling

Compliance Templates:

- PCI-DSS compliance configuration template
- HIPAA compliance configuration template
- GDPR compliance configuration template
- SOC 2 compliance configuration template

- ISO 27001 compliance configuration template
- One-click compliance profile activation

User Actions:

- Admins enable/configure all security features
- View comprehensive security dashboard
- Generate security audit reports
- Configure security policies and templates
- Review security logs and incidents
- Enable specific security features per site
- Customers benefit from automated security without configuration

3.2 Server & Infrastructure Management

3.2.1 Multi-Server Clustering

Requirement: Support horizontal scaling from single server to 10,000+ servers with zero-configuration clustering.

Detailed Specifications:

Server Roles:

- **Control Panel:** Centralized management interface for entire cluster
- **Application:** Web server role (NGINX, Apache, LiteSpeed, OpenLiteSpeed)
- **Database:** MySQL/MariaDB server role
- **Email:** Mail server role (Postfix, Dovecot)
- **DNS:** Name server role (BIND, PowerDNS)
- **Backup:** Dedicated backup storage and management

Features:

- Add server with single command: `panel-cli server add --ip=X.X.X.X --role=application`
- Automatic role configuration and deployment
- No per-server licensing costs
- Load balancing across application servers
- Automatic failover for high availability
- Health monitoring for all servers
- Geographical distribution support
- Move websites between servers with zero downtime
- Server provisioning time: < 5 minutes

User Actions:

- Admins add/remove servers from cluster via CLI or UI
- Assign roles to servers
- Monitor server health and performance
- Move sites between servers
- Configure load balancing rules

3.2.2 Web Server Support

Requirement: Support multiple web server technologies with per-site selection.

Specifications:

- **NGINX:** Default web server, reverse proxy, load balancer
- **Apache:** Alternative web server with .htaccess support
- **LiteSpeed:** High-performance commercial web server
- **OpenLiteSpeed:** Open-source LiteSpeed alternative
- Per-site web server selection
- Automatic configuration management
- Vhost template system
- SSL/TLS termination
- HTTP/2 and HTTP/3 support
- WebSocket support
- Reverse proxy configuration
- URL rewriting and redirects

3.2.3 Database Management

Requirement: Comprehensive database management with clustering support.

Specifications:

- MySQL 8.0+ support
- MariaDB 10.6+ support
- PostgreSQL 14+ support (future)
- Per-site database creation
- phpMyAdmin integration
- Database user management with granular permissions
- Database backup automation
- Point-in-time recovery
- Database replication support
- Read replica configuration
- Database clustering for high availability
- Query monitoring and optimization suggestions
- Slow query log analysis

User Actions:

- Admins create database servers and configure replication
- Users create databases via control panel
- Users manage database users and permissions
- Users access phpMyAdmin for database management
- Users download database backups

3.2.4 Server Monitoring & Statistics

Requirement: Real-time server monitoring with historical data and alerting.

Specifications:

- **Metrics Monitored:**
    - CPU usage (per core, average, load average)
    - Memory usage (used, free, cached, swap)
    - Disk usage (per partition, I/O statistics)
    - Network traffic (inbound, outbound, per interface)
    - Active connections
    - Process count
    - Service status (running, stopped, failed)
- **Monitoring Features:**
    - Real-time metrics (updated every 5 seconds)
    - Historical data retention (1 year)
    - Customizable dashboards
    - Graph visualization (line, bar, pie charts)
    - Comparison across servers
    - Trend analysis and forecasting
    - Capacity planning reports
- **Alerting:**
    - Threshold-based alerts (CPU > 80%, disk > 90%, etc.)
    - Alert methods: email, SMS, webhook, Slack, PagerDuty
    - Alert escalation rules
    - Maintenance window configuration
    - Alert acknowledgment and resolution tracking

User Actions:

- Admins view server metrics in real-time dashboard
- Configure alert thresholds and notification methods
- Generate capacity planning reports
- Compare performance across servers

3.2.5 Resource Limits & Isolation

Requirement: Enforce per-website resource limits to ensure fair usage and prevent resource abuse.

Specifications:

- **Resource Types:**
    - CPU: percentage of CPU cores (e.g., 25% = 1/4 core)
    - Memory: RAM limit (64MB - 4GB)
    - I/O Bandwidth: MB/s throughput
    - IOPS: I/O operations per second
    - Number of Processes (nproc)
    - Inodes: file count limit
    - Entry Processes: concurrent PHP processes
- **Enforcement:**

    - Linux Control Groups (cgroups) enforcement
    - Soft limits with burst allowance
    - Hard limits with throttling
    - Real-time resource usage tracking
    - Automatic limit enforcement
    - Resource usage alerts to admins and customers
- **Package-Based Limits:**
    - Define resource limits per hosting package
    - Bronze: 1 CPU, 512MB RAM, 10 processes
    - Silver: 2 CPU, 1GB RAM, 20 processes
    - Gold: 4 CPU, 2GB RAM, 40 processes
    - Custom limits per customer

User Actions:

- Admins set resource limits per package
- Admins view resource usage per site
- Admins receive alerts for sites exceeding limits
- Customers view their resource usage in real-time
- Customers upgrade package when nearing limits

3.3 Website Management Features

3.3.1 File Manager

Requirement: Full-featured, web-based file manager with comprehensive file operations.

Specifications:

Core Features:

- **Upload:** Drag-and-drop upload, multi-file upload, resumable upload
- **Download:** Single file download, bulk download as zip
- **Create:** Create new files and folders
- **Delete:** Delete files and folders (with confirmation)
- **Rename:** Rename files and folders
- **Move:** Move files/folders via drag-and-drop or cut/paste
- **Copy:** Copy files and folders
- **Permissions:** Change file/folder permissions (chmod)
- **Ownership:** Change file/folder ownership (chown) - admin only
- **Compress:** Create zip, tar, tar.gz, tar.bz2 archives
- **Extract:** Extract zip, tar, rar, 7z, gz, bz2 archives
- **Search:** Search files by name, content, date, size
- **Preview:** Preview images, text files, PDFs in browser

File Editor:

- Syntax-highlighted code editor (Monaco Editor / CodeMirror)
- Support for 100+ languages (PHP, HTML, CSS, JS, Python, Ruby, etc.)
- Line numbers
- Code folding

- Auto-completion
- Find and replace
- Multiple file tabs
- Auto-save drafts
- Revision history

Additional Features:

- Right-click context menu
- Keyboard shortcuts
- Breadcrumb navigation
- Dual-pane view (like FTP client)
- Thumbnail view for images
- File type icons
- Sort by name, size, date, type
- Hidden file toggle (.htaccess, .git)
- Symbolic link support
- Disk usage visualization
- Mobile-responsive interface

Supported File Formats for Upload:

- Images: jpg, jpeg, png, gif, svg, webp, bmp, ico
- Documents: pdf, doc, docx, xls, xlsx, ppt, pptx, txt, rtf
- Web files: html, htm, css, js, php, xml, json
- Archives: zip, tar, gz, bz2, rar, 7z
- Media: mp3, mp4, avi, mov, flv, webm
- Code: py, rb, java, c, cpp, sh, sql
- Config: conf, ini, yaml, yml, env
- And all other text-based formats

Security:

- File upload size limit (configurable: 100MB - 10GB)
- Dangerous file type blocking (.exe, .dll, .sh execution)
- Malware scanning on upload
- Path traversal prevention
- Restrict access to sensitive directories (/etc, /var)
- Activity logging (all file operations)

User Actions:

- Users upload, manage, edit files via browser
- Users create and extract archives
- Users edit code with syntax highlighting
- Users search for files
- Admins control file manager permissions per user

3.3.2 FTP/SFTP Access

Requirement: Secure file transfer with multiple protocols and user management.

Specifications:

Supported Protocols:

- FTP: Standard File Transfer Protocol (port 21)
- FTPS: FTP over SSL/TLS (port 21, implicit port 990)
- SFTP: SSH File Transfer Protocol (port 22)

Features:

- Create FTP/SFTP user accounts
- Per-user home directory restriction (chroot)
- Per-user bandwidth limits
- Per-user IP whitelist/blacklist
- Passive mode configuration
- Active mode configuration
- TLS certificate for FTPS
- SSH key authentication for SFTP
- Password authentication
- Two-factor authentication for FTP (optional)
- Connection logging
- Transfer logging
- Session timeout configuration
- Maximum concurrent connections per user
- Idle timeout

Management:

- Add/edit/delete FTP users via control panel
- Assign users to specific directories
- Set quotas per FTP user
- Temporary FTP access (expiration date)
- Suspend/unsuspend FTP accounts
- View active FTP connections
- Terminate FTP sessions

Security:

- Brute force protection for FTP logins
- Rate limiting
- GeoIP blocking
- Deny anonymous FTP access
- Force FTPS/SFTP over plain FTP option
- TLS 1.2+ enforcement
- Strong cipher enforcement

User Actions:

- Users create FTP accounts for themselves or subusers
- Users connect via FTP client (FileZilla, WinSCP, Cyberduck)

- Users manage files via FTP
- Admins monitor FTP usage and connections

3.3.3 SSH Access

Requirement: Secure shell access for advanced users with security controls.

Specifications:

Features:

- Per-user SSH access control
- Jailed SSH environment (prevent access to other users)
- SSH key authentication (recommended)
- Password authentication (optional)
- Two-factor authentication for SSH (TOTP)
- Custom SSH port per server
- SSH session timeout
- Idle session termination
- Command logging
- Restricted shell (limit available commands) - optional

SSH Key Management:

- Upload public SSH keys via control panel
- Generate SSH key pairs in panel
- Support for RSA, ECDSA, Ed25519 keys
- Key fingerprint display
- Multiple keys per user
- Key expiration dates
- Revoke keys

Terminal Access:

- Web-based SSH terminal (WebSocket-based)
- No client software required
- Copy/paste support
- Configurable terminal size
- Session recording for auditing (optional)

Security:

- Brute force protection via Fail2Ban
- IP whitelist for SSH access
- Disable root login
- Disable password authentication (key-only mode)
- GeoIP restriction
- SSH session alerts (email on login)

User Actions:

- Users enable SSH access for their account
- Users upload SSH keys
- Users connect via SSH client or web terminal
- Users execute commands, run scripts, debug applications

- Admins control SSH access globally and per user

3.3.4 Domain & DNS Management

Requirement: Comprehensive domain and DNS management with automation.

Specifications:

Domain Management:

- Add primary domains
- Add addon domains (park additional domains)
- Add subdomains (unlimited)
- Add domain aliases (point to existing domain)
- Change primary domain of a site
- 301/302 redirects management
- Wildcard subdomains
- Domain verification (TXT record, file upload)

DNS Management:

- Full DNS zone editor
- DNS record types: A, AAAA, CNAME, MX, TXT, SPF, DKIM, DMARC, SRV, CAA, NS
- TTL configuration per record
- Bulk DNS operations
- Import/export DNS zones (BIND format)
- DNS templates for common configurations
- Preview DNS changes before applying
- DNS propagation checker
- DNSSEC support (enable/disable per domain)
- DNSSEC key management

DNS Clustering:

- Synchronize DNS across multiple DNS servers
- Primary/secondary DNS server configuration
- DNS zone transfer (AXFR/IXFR)
- Automatic DNS failover
- GeoDNS support (route based on visitor location)

Cloudflare Integration:

- One-click Cloudflare activation
- Import existing Cloudflare zones
- Sync DNS records with Cloudflare
- Manage Cloudflare proxy status (orange/gray cloud)
- Configure Cloudflare settings (SSL, caching, firewall)
- Purge Cloudflare cache
- View Cloudflare analytics

User Actions:

- Users add domains, subdomains, aliases
- Users manage DNS records for their domains
- Users configure email DNS (MX, SPF, DKIM, DMARC)

- Users add redirects
- Users enable DNSSEC
- Users activate Cloudflare integration
- Admins manage nameserver configuration

3.3.5 SSL/TLS Certificate Management

Requirement: Automated SSL certificate provisioning and management.

Specifications:

Let's Encrypt Integration:

- Automatic SSL certificate issuance
- Issuance time: < 5 minutes
- Domain validation via HTTP-01 challenge
- DNS-01 challenge support (for wildcard certs)
- Automatic renewal 30 days before expiration
- Renewal retry on failure
- Support for up to 100 domains per certificate (SAN)
- Wildcard certificate support (*.domain.com)

Certificate Types:

- Single domain certificate
- Multi-domain (SAN) certificate
- Wildcard certificate
- Organization Validation (OV) certificate - via upload
- Extended Validation (EV) certificate - via upload

Custom SSL Certificates:

- Upload custom SSL certificate
- Upload private key
- Upload certificate chain (intermediate certificates)
- Support for self-signed certificates
- PFX/PKCS12 format support
- Certificate format validation

Certificate Management:

- List all SSL certificates
- View certificate details (issuer, expiration, domains, fingerprint)
- Download certificate and private key
- Delete certificate
- Force HTTPS redirect per site
- Mixed content warnings
- SSL/TLS protocol selection (TLS 1.2, TLS 1.3)
- Cipher suite configuration

Monitoring:

- Certificate expiration monitoring
- Alert 30, 14, 7, 1 days before expiration
- Renewal failure alerts

- Certificate revocation checking
- SSL Labs integration for security grading

User Actions:

- Users request Let's Encrypt certificate (one click)
- Users upload custom SSL certificates
- Users configure HTTPS redirect
- Users view certificate status and expiration
- Admins receive renewal failure alerts

3.3.6 Website Applications & CMS Support

Requirement: One-click installation and management of popular web applications.

Specifications:

Supported Applications:

- **WordPress:** Latest version, auto-install with admin user setup
- **Joomla:** Latest version
- **Drupal:** Latest version
- **Magento:** E-commerce platform
- **PrestaShop:** E-commerce platform
- **OpenCart:** E-commerce platform
- **phpBB:** Forum software
- **MyBB:** Forum software
- **MediaWiki:** Wiki software
- **Moodle:** Learning management system
- **NextCloud:** Cloud storage and collaboration
- **Laravel:** PHP framework (install composer, setup .env)
- **Symfony:** PHP framework
- **Django:** Python framework
- **Ruby on Rails:** Ruby framework
- **Node.js applications:** Express, Next.js, Nuxt.js
- **Static HTML sites**
- **Custom PHP applications**

Installation Wizard:

- Select application from list
- Choose domain/subdomain for installation
- Specify install directory (public_html or subdirectory)
- Select PHP version
- Create database automatically
- Configure admin username and password
- Install sample data (optional)
- Installation time: 1-3 minutes

Application Management (WordPress Focus):

- One-click WordPress updates (core, themes, plugins)
- Automatic background updates (configurable)

- Staging environment creation
- Clone WordPress site
- Database search and replace (for migration)
- WordPress user management from panel
- Plugin installation from panel
- Theme installation from panel
- WP-CLI integration
- WordPress security hardening
- Disable file editing from WordPress
- Debug mode toggle
- Multisite support

User Actions:

- Users install applications with one-click installer
- Users manage WordPress sites from control panel
- Users create staging environments
- Users clone sites for testing
- Admins control available applications and versions

3.3.7 Cron Job Management

Requirement: Easy scheduling of automated tasks with flexible timing options.

Specifications:

Features:

- Web-based cron job interface
- Template-based scheduling (common intervals)
- Custom schedule configuration
- Execute shell commands, PHP scripts, URLs
- Per-site cron job management
- Email output of cron jobs (optional)
- Log cron job execution history
- Enable/disable cron jobs without deleting

Templates:

- Every minute: `* * * * *`
- Every 5 minutes: `*/5 * * * *`
- Every 15 minutes: `*/15 * * * *`
- Every 30 minutes: `*/30 * * * *`
- Every hour: `0 * * * *`
- Every 6 hours: `0 */6 * * *`
- Every 12 hours: `0 */12 * * *`
- Daily at midnight: `0 0 * * *`
- Daily at specific time: `0 2 * * *` (2 AM)
- Weekly on Sunday: `0 0 * * 0`
- Monthly on 1st: `0 0 1 * *`
- Yearly on Jan 1st: `0 0 1 1 *`

- Custom schedule

Command Types:

- Shell command: `/usr/bin/php /path/to/script.php`
- URL execution: `wget -O - -q https://example.com/cron.php`
- PHP script: `php /home/user/script.php`
- Custom with parameters

Advanced Options:

- Run as specific user
- Set environment variables
- Redirect output to log file
- Timeout for long-running jobs
- Retry on failure
- Concurrent job prevention (prevent overlap)
- Lock file mechanism

Monitoring:

- Cron execution history (last 100 runs)
- Execution status (success, failed, timeout)
- Execution duration
- Output log for each run
- Failure alerts

User Actions:

- Users create cron jobs via templates or custom schedule
- Users view cron execution history and logs
- Users enable/disable/delete cron jobs
- Users receive email output from cron jobs
- Admins set global cron job limits (max 100 per user)

3.3.8 Email Management

Requirement: Comprehensive email hosting with spam filtering and account management.

Specifications:

Email Accounts:

- Create unlimited email accounts
- Mailbox quota configuration per account (100MB - 10GB)
- Password management
- POP3, IMAP, SMTP access
- Webmail access (Roundcube, Rainloop, or custom)
- Email forwarding
- Email aliases
- Catch-all address

Email Protocols:

- SMTP: Port 25, 587 (submission), 465 (SMTPS)
- POP3: Port 110, 995 (POP3S)

- IMAP: Port 143, 993 (IMAPS)
- Enforce SSL/TLS encryption
- STARTTLS support

Auto-Responders:

- Enable auto-reply for email account
- Custom auto-reply message
- Subject line customization
- Start/end date for auto-reply
- Frequency limit (respond once per X hours)

Email Filtering:

- Spam filtering (SpamAssassin, Rspamd)
- Configurable spam score threshold
- Spam tag vs delete options
- Whitelist/blacklist email addresses
- Whitelist/blacklist domains
- Content-based filters (keywords)
- Attachment filtering (block .exe, .zip, etc.)
- SPF, DKIM, DMARC validation

SPF, DKIM, DMARC:

- Automatic SPF record creation
- DKIM key generation and DNS record creation
- DMARC policy configuration (none, quarantine, reject)
- DMARC reporting email configuration
- Verification status display for SPF, DKIM, DMARC
- Email authentication testing tool

Mailing Lists:

- Create mailing lists
- Subscriber management
- Mailman integration
- Announcement-only lists
- Discussion lists
- Moderation options

Email Storage & Backup:

- Mailbox backup and restore
- Email archiving
- Search archived emails
- Export mailboxes (mbox, Maildir format)

Email Limits:

- Outgoing email rate limit (anti-spam)
- Hourly email sending limit (e.g., 100 emails/hour)
- Daily email sending limit
- Attachment size limit
- Mailbox size limit

- Concurrent connection limit

User Actions:

- Users create and manage email accounts
- Users configure email forwarding and auto-responders
- Users configure spam filtering settings
- Users set up SPF, DKIM, DMARC records
- Users access webmail
- Users configure email clients (Outlook, Thunderbird, Apple Mail)
- Admins monitor email usage and enforce limits

3.3.9 Performance Optimization

Requirement: Integrated caching and optimization tools for maximum website performance.

Specifications:

Varnish Cache:

- HTTP reverse proxy cache
- Enable/disable per site
- Cache lifetime configuration (TTL: 1 hour to 7 days)
- Excluded parameters (URLs with query params to skip cache)
- Excluded paths (regex patterns for non-cached pages: ^/cart/, ^/checkout/, wp-admin)
- Cache tag prefix for multi-site management
- Purge entire cache for site
- Purge specific URL or cache tags
- Cache hit ratio statistics
- Performance: up to 250x faster page loads
- Backend connection: port 6081
- Automatic cache purge on content updates (WordPress, Joomla)
- Grace mode: serve stale cache if backend is down

Redis Cache:

- In-memory object cache
- Enable/disable per site
- Runs in website container (isolated)
- Persistent storage option
- Memory limit configuration (64MB - 512MB)
- Eviction policies (LRU, LFU, random)
- WordPress object cache plugin auto-activation
- Cache statistics (keys, hit rate, memory usage)

Opcode Caching:

- PHP opcode caching via OPcache
- Enable/disable per site
- Preload frequently used files
- Validate timestamps (check for file changes)
- Revalidate frequency configuration
- Memory consumption limit

- Maximum accelerated files
- Statistics (opcache usage, hit rate)

Other Optimization:

- Gzip/Brotli compression
- Image optimization on upload (lossy/lossless)
- CSS/JS minification
- HTML minification
- Browser caching headers
- CDN integration (Cloudflare, Amazon CloudFront)
- HTTP/2 and HTTP/3 support
- Keep-Alive connections
- Lazy loading for images

User Actions:

- Users enable caching features for their sites
- Users configure cache settings (TTL, exclusions)
- Users purge cache on demand
- Users view cache statistics
- Admins enable optimization globally

3.3.10 Staging & Cloning

Requirement: Create staging environments and clone websites for testing.

Specifications:

Staging Environment:

- One-click staging site creation
- Clone production to staging subdomain (staging.example.com)
- Duplicate files, database, email accounts
- Automatic database search/replace for URLs
- Isolated staging environment
- Push staging to production with one click
- Sync production to staging (overwrite)
- Delete staging environment
- Password-protect staging site (HTTP Basic Auth)
- Prevent search engine indexing (robots.txt, X-Robots-Tag)

Website Cloning:

- Clone existing website to new domain or subdomain
- Clone files and database
- Update database URLs and paths automatically
- Clone email accounts (optional)
- Clone SSL certificate (optional)
- Clone cron jobs (optional)
- Clone FTP users (optional)
- Clone to same server or different server in cluster
- Cloning time: 1-10 minutes depending on size

User Actions:

- Users create staging environment for testing
- Users make changes to staging without affecting production
- Users push staging to production when ready
- Users clone websites for new projects or clients
- Admins facilitate site migrations via cloning

3.4 Billing & Automation

3.4.1 Billing Automation

Requirement: Fully automated recurring billing and invoicing system.

Specifications:

Invoice Generation:

- Automatic recurring invoice generation
- One-time invoices
- Configurable billing cycles: monthly, quarterly, semi-annually, annually, biennially, triennially
- Pro-rata billing for mid-cycle changes
- Invoice generation X days before due date (configurable: 7-30 days)
- PDF invoice generation
- Customizable invoice templates
- Invoice numbering format customization
- Include company logo and branding

Payment Processing:

- Support for 50+ payment gateways
- **Credit Card:** Stripe, Authorize.net, Braintree, Square
- **PayPal:** PayPal Express, PayPal Standard, PayPal Payflow
- **Cryptocurrency:** Coinbase Commerce, BitPay
- **Bank Transfer:** Manual bank transfer, SEPA, ACH
- **E-wallets:** Skrill, Alipay, WeChat Pay
- **Regional:** Razorpay (India), Paytm (India), 2Checkout (global)
- Automatic payment collection for recurring invoices
- Payment failure handling and retry logic
- Email notifications for successful payments
- Email notifications for failed payments
- Receipt generation and email delivery

Subscription Management:

- Recurring subscription creation
- Automatic renewal on expiration
- Renewal reminder emails (7, 3, 1 days before due)
- Subscription cancellation (immediate or end of term)
- Subscription upgrade/downgrade
- Pro-rata credit calculation on downgrades

- Subscription suspension on non-payment
- Automatic service termination after X days overdue (configurable)

Payment Reminders:

- Overdue invoice reminders
- Escalating reminder schedule: 1 day overdue, 3 days overdue, 7 days overdue, 14 days overdue
- Customizable reminder email templates
- Final notice before suspension
- Late payment fees (optional)

Tax Management:

- Multiple tax rules support
- Tax rates by country, state/province, city
- VAT/GST support with tax ID validation
- Tax exemption for specific customers
- Compound tax support
- Tax reporting

Multi-Currency:

- Support for 150+ currencies
- Real-time exchange rate updates
- Display prices in customer's currency
- Base currency for accounting
- Currency conversion on invoices
- Multi-currency reporting

Credit System:

- Account credit/wallet
- Apply credit to invoices automatically
- Manual credit addition by admin
- Credit transactions log
- Refund to credit option

User Actions:

- Customers view invoices in client area
- Customers pay invoices online
- Customers download invoice PDFs
- Customers view payment history
- Customers update payment methods
- Admins create manual invoices
- Admins apply credits and refunds
- Admins configure tax rates and billing settings

3.4.2 Automated Provisioning

Requirement: Instant or scheduled service provisioning without manual intervention.

Specifications:

Provisioning Triggers:

- Automatic provisioning on payment receipt
- Automatic provisioning on order placement (free services)
- Manual admin approval required (optional per product)
- Delayed provisioning (schedule for later)

Provisioning Actions:

- Create hosting account automatically
- Create cPanel/Plesk/DirectAdmin account (if using external panel)
- Create databases
- Create email accounts
- Register domain (via registrar API)
- Issue SSL certificate
- Configure DNS
- Send welcome email with login details
- Log provisioning actions

Server Assignment:

- Automatic server selection based on:
    - Server load (CPU, memory, disk)
    - Geographic location
    - Server capacity (sites hosted, resources)
    - Round-robin distribution
    - Manual server assignment override

Account Lifecycle Management:

- Automatic suspension on non-payment (after X days overdue)
- Suspension actions: disable website, disable email, disable FTP, disable SSH
- Automatic unsuspension on payment
- Automatic termination after prolonged non-payment (after X days suspended)
- Termination actions: backup account, delete files, delete database, delete email, delete DNS
- Grace period before permanent deletion (7-30 days)

Module Integration:

- Integration with external control panels (cPanel, Plesk, DirectAdmin)
- Integration with virtualization platforms (SolusVM, Virtualizor, Proxmox)
- Integration with dedicated server management (WHMCS modules, custom APIs)
- Custom provisioning scripts support
- API-based provisioning for external services

User Actions:

- Customers receive instant service activation after payment
- Customers receive welcome email with credentials
- Admins configure provisioning rules per product
- Admins manually provision orders if needed
- Admins suspend/unsuspend/terminate services

3.4.3 Domain Management & Automation

Requirement: Complete domain lifecycle management with registrar integration.

Specifications:

Registrar Integration:

- Support for 20+ major domain registrars
- **Supported Registrars:** Enom, Namecheap, ResellerClub, OpenSRS, Tucows, GoDaddy, 101Domain, Internet.bs, OnlineNIC, CentralNic, LogicBoxes, Resellia, etc.
- API-based domain operations
- Real-time domain availability checking
- Domain registration
- Domain transfers
- Domain renewals

Domain Operations:

- **Registration:** Check availability, register domain, configure nameservers, configure contacts (registrant, admin, tech, billing)
- **Transfer:** Initiate transfer, automatic EPP code request, transfer status polling, automatic completion on success
- **Renewal:** Automatic renewal X days before expiration (configurable), manual renewal, renewal reminders
- **Management:** Update nameservers, update contact details (WHOIS), domain lock/unlock, enable/disable auto-renew, DNS management (if supported by registrar)

Domain Suggestions (Namespinning):

- Intelligent domain suggestions for unavailable domains
- Alternative TLDs suggestion (.com, .net, .org, .io, .co)
- Similar domain names (hyphens, numbers, prefixes/suffixes)
- Premium domain suggestions
- New TLD promotions

Domain Pricing:

- Per-TLD pricing configuration
- Registration, transfer, renewal pricing
- Promo pricing for first year
- Markup over registrar cost
- Bulk pricing management
- Registrar cost synchronization

Domain Addons:

- ID Protection (WHOIS privacy)
- DNS management service
- Email forwarding service
- Domain forwarding
- Premium DNS
- SSL certificates (sold as domain addon)

Domain Reminders:

- Renewal reminders: 60, 30, 14, 7, 1 days before expiration
- Transfer expiration reminders
- Domain expiration notifications

Bulk Operations:

- Bulk domain registration
- Bulk domain transfer
- Bulk renewal
- Bulk nameserver updates
- Bulk contact updates
- Bulk lock/unlock

User Actions:

- Customers search for domain availability
- Customers register domains via client area
- Customers transfer domains in
- Customers manage domain settings (nameservers, contacts, lock)
- Customers receive renewal reminders and renew domains
- Admins configure registrar APIs
- Admins set domain pricing
- Admins manage customer domains

3.4.4 Package & Product Management

Requirement: Flexible product configuration for hosting packages, addons, and services.

Specifications:

Product Types:

- Shared hosting packages
- Reseller hosting packages
- VPS hosting packages
- Dedicated server packages
- Domain registration
- SSL certificates
- Email hosting
- Website builder
- Marketing services
- Custom products/services

Package Configuration:

- **Name & Description:** Product name, marketing description, feature list
- **Pricing:** Setup fee, recurring price, billing cycles (monthly, quarterly, annually, etc.)
- **Resources:** Disk space, bandwidth, email accounts, databases, FTP accounts, subdomains, addon domains
- **Features:** Control panel, software installer, SSL certificate, staging, backups, etc.
- **Add-ons:** Optional add-ons (extra disk, extra bandwidth, dedicated IP, etc.)
- **Upgrade/Downgrade Paths:** Define which packages customers can upgrade/downgrade to
- **Server Assignment:** Assign product to specific server or server group
- **Provisioning Module:** Select control panel module for provisioning

Product Groups:

- Organize products into groups (Shared Hosting, VPS, Domains, etc.)
- Display groups in client area ordering

- Featured products

Promotional Pricing:

- First billing cycle discount
- Coupon code discounts
- Bundle pricing (hosting + domain discount)
- Limited-time offers
- Free trial periods

Product Addons:

- Configurable addons per product
- Addon types: one-time, recurring
- Addon dependencies (require another addon)
- Quantity-based addons (extra 10GB disk = $5/month)

Configurable Options:

- Dropdown selections (e.g., RAM size: 1GB, 2GB, 4GB)
- Checkbox options (e.g., automatic backups: yes/no)
- Quantity inputs (e.g., additional IP addresses)
- Price modifiers per option

User Actions:

- Customers browse hosting packages
- Customers select package and order
- Customers customize package with addons and options
- Customers upgrade/downgrade package
- Admins create and manage products
- Admins set pricing and promotions

3.5 Customer Management & Support

3.5.1 Customer Portal

Requirement: Self-service client area for customers to manage services and support.

Specifications:

Dashboard:

- Account overview
- Active services list with status
- Recent invoices and payments
- Open support tickets
- System announcements
- Service usage statistics
- Quick actions (pay invoice, open ticket, manage domain)

Service Management:

- View all services
- Service details (package, resources, expiration)
- Upgrade/downgrade service

- Cancel service
- Service-specific management (access control panel, view credentials)
- Addon management

Billing:

- View all invoices (paid, unpaid, overdue)
- Pay invoices online
- Download invoice PDFs
- View payment history
- Add/update payment methods
- Manage subscriptions
- View account credit balance

Domain Management:

- View all domains
- Manage nameservers
- Update domain contacts
- Transfer domain
- Renew domain
- Enable/disable auto-renew
- Manage domain addons (privacy, DNS)

Support:

- Open new support tickets
- View open and closed tickets
- Reply to tickets
- Ticket attachments
- Ticket priority selection
- Ticket department selection
- View knowledgebase articles
- View announcements
- View network status

Account Settings:

- Update profile information
- Change password
- Enable two-factor authentication
- Email notification preferences
- Security settings
- Security questions

User Actions:

- Customers log into client portal
- Customers manage all services
- Customers pay invoices
- Customers open and manage support tickets
- Customers update account information

3.5.2 Support Ticket System

Requirement: Comprehensive support desk for managing customer inquiries and issues.

Specifications:

Ticket Submission:

- Customers submit tickets via client area
- Customers submit tickets via email
- Unregistered visitors can submit tickets (optional)
- Admins create tickets on behalf of customers
- Ticket fields: department, subject, priority, service association

Ticket Departments:

- Configurable departments (Sales, Technical, Billing, Abuse, etc.)
- Department-specific email addresses
- Assign admin staff to departments
- Department permissions
- Auto-assign tickets to departments based on keywords

Ticket Priorities:

- Priority levels: Low, Medium, High, Critical
- Color-coding by priority
- Sort and filter by priority
- SLA timers per priority

Ticket Statuses:

- **Open:** New ticket awaiting first response
- **Answered:** Admin replied, awaiting customer response
- **Customer-Reply:** Customer replied, awaiting admin response
- **On Hold:** Ticket paused, waiting for external factor
- **In Progress:** Actively being worked on
- **Closed:** Ticket resolved

Ticket Features:

- **Threaded Discussion:** Conversation-style ticket view
- **File Attachments:** Attach images, logs, screenshots (max 10MB)
- **Ticket Flags:** Flag tickets for follow-up or escalation
- **Ticket Tags:** Categorize tickets with custom tags
- **Admin Notes:** Private internal notes not visible to customer
- **Predefined Replies:** Save common responses for quick replies
- **CC Recipients:** Add additional email addresses to ticket
- **Ticket Watchers:** Admins can watch tickets for notifications
- **Merge Tickets:** Combine duplicate tickets
- **Split Tickets:** Split single ticket into multiple tickets
- **Transfer Tickets:** Move ticket to different department
- **Assign Tickets:** Assign to specific admin
- **Ticket Linking:** Link related tickets together

Automated Actions:

- Auto-close tickets after X days of inactivity
- Auto-response on ticket submission
- Scheduled ticket actions (escalate, change priority, add note)
- Escalation rules (escalate to supervisor after X hours)
- SLA-based auto-assignment

Notifications:

- Email notifications to customer on admin reply
- Email notifications to admin on customer reply
- Email notifications to flagged admin on assignment
- Email notifications to watchers on updates
- Email notifications to department members on new ticket
- Notification preferences per admin

Ticket Feedback:

- Customer satisfaction rating after ticket closure (1-5 stars)
- Optional feedback comment
- Aggregate ratings per admin
- Feedback reports

User Actions:

- Customers submit and manage support tickets
- Customers attach files and reply to tickets
- Customers rate support quality
- Admins view, assign, and respond to tickets
- Admins use predefined replies for efficiency
- Admins add private notes for internal communication
- Admins close, merge, split, transfer tickets

3.5.3 Knowledgebase

Requirement: Self-help documentation to reduce support tickets and empower customers.

Specifications:

Features:

- Create knowledgebase articles
- Organize articles into categories and subcategories
- Article search functionality (full-text search)
- Article ratings (helpful/not helpful)
- Most popular articles display
- Recent articles display
- Related articles suggestions
- Rich text editor for articles (formatting, images, videos, code blocks)
- Article revisions and version history
- Draft articles (not publicly visible)

Organization:

- Hierarchical categories (parent and child categories)
- Tags for articles

- Multiple categories per article
- Featured articles

Public vs Private:

- Public knowledgebase accessible to everyone
- Private articles accessible only to logged-in customers
- Admin-only articles for internal documentation

Intelligent Suggestions:

- Suggest relevant knowledgebase articles when customer opens ticket
- Search knowledgebase as customer types ticket subject
- Reduce ticket submissions by providing self-help

User Actions:

- Customers search and browse knowledgebase
- Customers find solutions without opening tickets
- Admins create and manage knowledgebase articles
- Admins review article ratings and improve content

3.5.4 Announcements

Requirement: Communicate news, maintenance, and updates to customers.

Specifications:

Features:

- Create announcements
- Title, date, and content
- Rich text formatting
- Publish immediately or schedule for future
- Display on client area dashboard
- Display on dedicated announcements page
- Email announcements to customers (optional)
- Mark announcements as important (highlight)
- Announcement categories (maintenance, news, feature, promotion)

Social Sharing:

- Share announcements on social media (Facebook, Twitter, LinkedIn)
- Social share buttons on announcement page

User Actions:

- Customers view announcements in client area
- Customers receive email notifications for important announcements
- Admins create and publish announcements

3.5.5 Network Status

Requirement: Transparent communication about server issues and maintenance.

Specifications:

Features:

- Create server network status

- List all servers in network
- Server status: Operational, Degraded Performance, Partial Outage, Major Outage, Maintenance
- Color-coded status indicators (green, yellow, orange, red, blue)
- Add maintenance schedules
- Add incident reports
- Incident timeline (detected, investigating, identified, monitoring, resolved)
- Automatic customer notification for servers they use
- Historical uptime percentage per server
- Subscribe to status updates (email, SMS, RSS)

User Actions:

- Customers view server status
- Customers subscribe to status updates for their servers
- Customers view incident history
- Admins update server status
- Admins create maintenance schedules
- Admins post incident updates

3.6 User Interface & Experience

3.6.1 Design & Responsiveness

Requirement: Modern, intuitive interface that works on all devices.

Specifications:

Design Principles:

- Clean, minimal interface
- Consistent design language
- Intuitive navigation
- Reduced cognitive load
- Accessibility (WCAG 2.1 AA compliance)
- Fast loading times
- Progressive web app (PWA) capabilities

Responsive Design:

- Fully responsive layout for desktop, tablet, mobile
- Mobile-first design approach
- Optimized touch interactions for mobile
- Adaptive layouts based on screen size
- No feature limitations on mobile devices
- Mobile-specific navigation (hamburger menu)

Dashboard:

- Widget-based dashboard
- Customizable widget placement
- Drag-and-drop widget arrangement
- Collapsible widgets

- Real-time data updates
- Overview metrics (servers, sites, customers, revenue)

Navigation:

- Sidebar navigation (collapsible)
- Top navigation bar
- Breadcrumb navigation
- Global search (search servers, sites, customers, tickets)
- Quick actions menu
- Keyboard shortcuts

User Actions:

- Users access panel from any device
- Users customize dashboard layout
- Users navigate intuitively without training

3.6.2 White-Label Branding

Requirement: Complete customization for hosting providers to brand as their own.

Specifications:

Branding Options:

- Company logo upload (header, email, invoice, login page)
- Favicon customization
- Color scheme customization (primary, secondary, accent colors)
- Font selection (Google Fonts integration)
- Custom CSS injection for advanced styling
- Email template branding (logo, colors, footer)
- Invoice template branding
- Terms of Service and Privacy Policy links
- Custom copyright text

Domain Customization:

- Custom control panel domain (panel.yourdomain.com)
- Custom client area domain (clients.yourdomain.com)
- SSL certificate for custom domains

White-Label Options:

- Hide/show panel branding
- Custom welcome message
- Custom login page background image
- Custom admin email address
- Custom sender name for emails

User Actions:

- Admins upload logo and customize colors
- Admins set custom domain for control panel
- Admins preview branding before applying
- Customers see hosting provider's brand, not panel brand

3.6.3 Multi-Language Support

Requirement: Support for multiple languages to serve global customers.

Specifications:

Supported Languages:

- English (US, UK)
- Spanish (Spain, Latin America)
- French
- German
- Italian
- Portuguese (Brazil, Portugal)
- Russian
- Chinese (Simplified, Traditional)
- Japanese
- Korean
- Arabic
- Turkish
- Dutch
- Polish
- Swedish
- Danish
- Norwegian
- Finnish
- And 30+ additional languages

Language Features:

- Per-user language selection
- Automatic language detection based on browser
- Language switcher in header
- Admin interface translation
- Client area translation
- Email template translation
- Invoice translation
- Date/time format localization
- Currency symbol localization
- Number format localization (comma vs period)

Translation Management:

- Built-in translation editor
- Import/export language files (JSON, PO, CSV)
- Community translation contributions
- Translation completion percentage per language
- Override default translations

User Actions:

- Users select preferred language in profile

- Users view interface in their language
- Users receive emails in their language
- Admins add or edit translations

3.6.4 Dark Mode

Requirement: Dark theme option to reduce eye strain and save power.

Specifications:

Features:

- Dark mode toggle in user settings
- System theme detection (auto dark mode based on OS)
- Smooth transition between light and dark modes
- Dark mode for all interface sections
- High contrast for readability
- Optimized colors for dark mode (not just inverted colors)
- Remember user preference

User Actions:

- Users enable dark mode in settings
- Users enjoy reduced eye strain at night

3.7 Reporting & Analytics

3.7.1 Usage Reports

Requirement: Detailed reports on resource usage, billing, and system health.

Specifications:

Report Types:

- **Disk Usage Report:** Total disk used, per site, per customer, growth trends
- **Bandwidth Report:** Total bandwidth, per site, top consumers, trends
- **Email Usage Report:** Email accounts, mailbox sizes, email sent, spam blocked
- **Database Report:** Database count, database sizes, top databases
- **Server Load Report:** CPU, memory, disk I/O, network, over time
- **Security Report:** Attacks blocked, malware detected, brute force attempts
- **Customer Report:** New customers, churned customers, active services
- **Revenue Report:** Total revenue, revenue per product, revenue trends
- **Invoice Report:** Invoices generated, paid, unpaid, overdue

Report Features:

- Date range selection (last 7 days, last 30 days, last 12 months, custom)
- Export to PDF, CSV, Excel
- Schedule automatic email reports (daily, weekly, monthly)
- Graphical visualizations (line charts, bar charts, pie charts)
- Comparison view (compare current period to previous period)

User Actions:

- Admins generate reports for analysis

- Admins export reports for accounting
- Admins schedule reports for automatic delivery
- Customers view their own usage reports

3.7.2 Analytics Dashboard

Requirement: Real-time analytics and key performance indicators (KPIs).

Specifications:

KPIs:

- Total websites hosted
- Total customers
- Active services
- Monthly recurring revenue (MRR)
- Annual recurring revenue (ARR)
- Churn rate
- Average revenue per user (ARPU)
- Customer lifetime value (CLV)
- New orders today/this week/this month
- Server capacity utilization
- Support ticket volume and average response time
- System uptime percentage

Visualizations:

- Time-series graphs for trends
- Gauge charts for capacity
- Funnel charts for conversion
- Heat maps for geographic distribution
- Top 10 lists (customers, sites, products)

User Actions:

- Admins view real-time KPIs
- Admins identify trends and make decisions
- Admins monitor system health

4. Technical Architecture

4.1 Technology Stack

Backend:

- **Language:** Rust (primary), Python (automation scripts)
- **Web Framework:** Actix-web (Rust), async/await for performance
- **Database:** PostgreSQL 14+ (primary), Redis (caching, sessions)
- **ORM:** Diesel (Rust SQL toolkit)
- **Task Queue:** Celery with Redis backend (for async jobs)
- **API:** RESTful API with OpenAPI 3.0 specification, GraphQL (optional)

Frontend:

- **Framework:** React 18+ with TypeScript

- **UI Library:** Material-UI, Tailwind CSS
- **State Management:** Redux Toolkit
- **Build Tool:** Vite
- **Testing:** Jest, React Testing Library

Web Servers:

- NGINX (default, reverse proxy, load balancer)
- Apache (optional, via modules)
- LiteSpeed (optional, commercial)
- OpenLiteSpeed (optional, open-source)

Caching:

- Varnish Cache 7+ (HTTP cache)
- Redis 6+ (object cache, sessions)
- OPcache (PHP opcode cache)

Security:

- ModSecurity 3+ (WAF engine)
- ClamAV (antivirus)
- Fail2Ban (brute force protection)
- OSSEC (intrusion detection)
- Custom security modules in Rust

Infrastructure:

- **Containerization:** Docker for service isolation
- **Orchestration:** Kubernetes (optional for large deployments)
- **Clustering:** Custom clustering protocol over secure WebSocket
- **Load Balancing:** NGINX, HAProxy
- **Monitoring:** Prometheus (metrics), Grafana (visualization), ELK Stack (logging)

Deployment:

- **Supported OS:** Ubuntu 22.04 LTS (primary), Debian 11+, CentOS 8 Stream, Rocky Linux 8+
- **Architecture:** x86_64/amd64 (ARM support planned)
- **Minimum Requirements:** 4GB RAM, 40GB storage, 2 CPU cores
- **Recommended:** 8GB+ RAM, 100GB+ SSD, 4+ CPU cores

4.2 Scalability & Performance

Horizontal Scaling:

- Add unlimited servers to cluster
- Automatic load distribution
- No single point of failure
- Database read replicas for scaling
- Shared nothing architecture (stateless application servers)

Performance Targets:

- Page load time: < 200ms (control panel)
- API response time: < 100ms (95th percentile)
- Database query time: < 50ms (average)
- Support 10,000+ concurrent users

- Support 100,000+ websites per cluster
- Handle 10,000+ API requests per second

Caching Strategy:

- Application-level caching (Redis)
- Database query caching
- HTTP caching (Varnish)
- Opcode caching (OPcache)
- CDN integration for static assets

4.3 Security Architecture

Defense in Depth:

- Network layer: Firewall, DDoS protection
- Application layer: WAF, input validation
- Authentication: 2FA, strong passwords, rate limiting
- Authorization: Role-based access control (RBAC)
- Encryption: TLS 1.3, encrypted database connections, encrypted backups
- Monitoring: Intrusion detection, anomaly detection, security logging

Data Protection:

- Encryption at rest (database, backups)
- Encryption in transit (TLS 1.3)
- Secure key management
- Regular security audits
- Penetration testing
- Vulnerability scanning
- Compliance: PCI-DSS, GDPR, HIPAA

4.4 API & Integrations

RESTful API:

- Complete API coverage for all panel functions
- API authentication via API keys and OAuth 2.0
- Rate limiting: 60 requests/minute (default, configurable)
- Versioned API (v1, v2, etc.)
- Comprehensive API documentation (OpenAPI/Swagger)
- API playground for testing
- Webhooks for event notifications
- API client libraries (PHP, Python, JavaScript, Ruby)

Third-Party Integrations:

- Payment gateways (50+)
- Domain registrars (20+)
- DNS providers (Cloudflare, Route 53, etc.)
- Email services (SendGrid, Mailgun, Amazon SES)
- SMS providers (Twilio, Nexmo, MessageBird)
- Monitoring services (Pingdom, UptimeRobot)

- Analytics (Google Analytics, Matomo)
- CRM (Salesforce, HubSpot)
- Helpdesk (Zendesk, Freshdesk)

5. Implementation Roadmap

Phase 1: Foundation (Months 1-4)

Objective: Build core infrastructure and security foundation

Deliverables:

- Server management (add, remove, monitor servers)
- Multi-server clustering
- User management with RBAC
- PHP hardening implementation
- Basic WAF with ModSecurity
- Brute force protection (Fail2Ban integration)
- Database management
- Basic web server support (NGINX)
- Admin panel interface
- API foundation

Phase 2: Security & Protection (Months 4-6)

Objective: Implement advanced security features

Deliverables:

- Advanced WAF with custom rules and ML detection
- Antivirus and malware scanning (ClamAV integration)
- Intrusion detection system (OSSEC)
- CageFS / user isolation
- Complete brute force protection across all services
- Security monitoring dashboard
- Threat intelligence integration
- SSL/TLS management with Let's Encrypt

Phase 3: Website Management (Months 6-9)

Objective: Build comprehensive website management tools

Deliverables:

- File manager with editor
- FTP/SFTP access
- SSH access with web terminal
- Domain and DNS management
- Application installer (WordPress, etc.)
- Email management system
- Cron job manager
- Performance optimization (Varnish, Redis, OPcache)

- Staging and cloning features
- Customer portal (basic)

Phase 4: Billing & Automation (Months 9-12)

Objective: Implement billing and provisioning automation

Deliverables:

- Billing automation system
- Payment gateway integrations
- Invoice generation and management
- Automated provisioning
- Domain registrar integrations
- Package and product management
- Customer portal (complete)
- Support ticket system
- Knowledgebase
- Announcements and network status

Phase 5: Polish & Scale (Months 12-15)

Objective: Optimize, scale, and refine features

Deliverables:

- Performance optimization
- White-label branding system
- Multi-language support
- Dark mode
- Reporting and analytics dashboard
- Mobile app (iOS, Android)
- Migration tools (cPanel, Plesk, WHMCS)
- Advanced API features
- Documentation and training materials
- Beta testing with select hosting providers

Phase 6: Launch (Month 15+)

Objective: Public launch and continuous improvement

Deliverables:

- Public release (v1.0)
- Marketing and sales materials
- Licensing system
- Customer support infrastructure
- Community forums
- Regular updates and feature releases
- Security patches and maintenance

6. Non-Functional Requirements

6.1 Performance Requirements

- Control panel page load time: < 200ms
- API response time: < 100ms (95th percentile)
- Support 10,000+ concurrent users
- Database query time: < 50ms
- File manager operations: < 1 second
- Website provisioning: < 2 minutes

6.2 Security Requirements

- All communications encrypted with TLS 1.3
- Database encryption at rest
- Password hashing with bcrypt or Argon2
- Two-factor authentication support
- Regular security audits and penetration testing
- Compliance with PCI-DSS, GDPR, HIPAA
- Vulnerability disclosure program
- Security patch deployment within 24 hours of discovery

6.3 Reliability Requirements

- System uptime: 99.9% (excluding planned maintenance)
- Automatic failover for critical services
- Database replication for data redundancy
- Automated backups (daily, weekly, monthly)
- Disaster recovery plan
- Maximum 1 hour recovery time objective (RTO)
- Maximum 15 minutes recovery point objective (RPO)

6.4 Usability Requirements

- Intuitive interface requiring minimal training
- Consistent UI/UX across all modules
- Mobile-responsive design
- Accessibility compliance (WCAG 2.1 AA)
- Comprehensive documentation
- Video tutorials
- Contextual help system
- Maximum 3 clicks to reach any feature

6.5 Maintainability Requirements

- Modular architecture for easy updates
- Automated testing (unit, integration, E2E)
- CI/CD pipeline for deployment
- Code coverage > 80%
- Comprehensive logging and monitoring

- Database migration system
- Backward compatibility for API versions
- Regular refactoring and technical debt management

6.6 Compliance Requirements

- **GDPR:** Data protection, right to erasure, data portability, consent management
- **PCI-DSS:** Secure payment processing, cardholder data protection
- **HIPAA:** Healthcare data protection (if applicable)
- **SOC 2:** Security, availability, confidentiality, processing integrity, privacy
- **ISO 27001:** Information security management system

7. Success Criteria & KPIs

7.1 Technical KPIs

- System uptime: ≥ 99.9%
- API response time: < 100ms (95th percentile)
- Page load time: < 200ms
- Security incidents: 0 critical vulnerabilities unpatched > 24 hours
- Code test coverage: ≥ 80%

7.2 Business KPIs

- User adoption: 100+ hosting providers in first year
- Customer satisfaction: ≥ 4.5/5.0 rating
- Support ticket resolution: < 24 hours average response time
- Churn rate: < 5% monthly
- Net Promoter Score (NPS): ≥ 50

7.3 User Experience KPIs

- Time to provision new hosting account: < 2 minutes
- Setup complexity: Complete server setup in < 30 minutes
- Feature discoverability: Users find features without documentation ≥ 80%
- Mobile usability: Full feature parity on mobile devices
- Accessibility: WCAG 2.1 AA compliance 100%

8. Dependencies & Constraints

8.1 External Dependencies

- Domain registrar APIs (Enom, Namecheap, etc.)
- Payment gateway APIs (Stripe, PayPal, etc.)
- SSL certificate providers (Let's Encrypt, commercial CAs)
- Threat intelligence feeds
- Email delivery services
- SMS providers
- Cloud infrastructure providers

8.2 Technical Constraints

- Linux-based servers only (no Windows support initially)
- x86_64/amd64 architecture (ARM support planned)
- Minimum 4GB RAM per server
- PostgreSQL as primary database (no MySQL/MariaDB for panel database)
- Modern web browsers (Chrome 90+, Firefox 88+, Safari 14+, Edge 90+)

8.3 Regulatory Constraints

- GDPR compliance for European customers
- PCI-DSS compliance for payment processing
- DMCA compliance for copyright infringement
- CAN-SPAM compliance for email sending
- Regional data residency requirements

8.4 Risks & Mitigation

Risk: Security vulnerabilities

- Mitigation: Regular security audits, bug bounty program, rapid patching

Risk: Performance degradation at scale

- Mitigation: Load testing, horizontal scaling, performance monitoring

Risk: Third-party API changes

- Mitigation: API version pinning, regular integration testing, fallback options

Risk: Competitive market

- Mitigation: Unique features (security focus), competitive pricing, excellent support

Risk: Adoption challenges

- Mitigation: Migration tools, comprehensive documentation, onboarding support

9. Glossary

Control Panel: Web-based interface for managing hosting services, servers, and customers

Cluster: Group of servers working together as a single system

Provisioning: Automated setup of hosting accounts, databases, and services

WAF (Web Application Firewall): Security system that monitors and filters HTTP traffic

RBAC (Role-Based Access Control): Security model restricting access based on user roles

Varnish Cache: HTTP reverse proxy for caching web content

Redis: In-memory data store used for caching and sessions

OPcache: PHP extension for opcode caching

CageFS: Virtualized file system for user isolation

ModSecurity: Open-source web application firewall

SPF (Sender Policy Framework): Email authentication method

DKIM (DomainKeys Identified Mail): Email authentication method

DMARC (Domain-based Message Authentication): Email authentication method

Let's Encrypt: Free SSL certificate authority

Two-Factor Authentication (2FA): Additional security layer requiring second verification

API (Application Programming Interface): Interface for programmatic access to panel functions

CLI (Command Line Interface): Text-based interface for server management

WHOIS: Protocol for querying domain registration information

DNS (Domain Name System): System for translating domain names to IP addresses

DNSSEC (DNS Security Extensions): Security extension for DNS

SSL/TLS: Cryptographic protocols for secure communication

10. Appendices

Appendix A: Feature Priority Matrix

Feature Category	Priority	Phase
Multi-Server Clustering	Critical	Phase 1
PHP Hardening	Critical	Phase 1
Basic WAF	Critical	Phase 1
Brute Force Protection	Critical	Phase 1
Advanced WAF	High	Phase 2
Antivirus Scanning	High	Phase 2
File Manager	High	Phase 3
Email Management	High	Phase 3
Billing Automation	Critical	Phase 4
Automated Provisioning	Critical	Phase 4
Domain Management	High	Phase 4
White-Label Branding	Medium	Phase 5
Multi-Language	Medium	Phase 5
Mobile App	Low	Phase 5

Appendix B: API Endpoint Examples

Authentication:

- `POST /api/v1/auth/login` - Authenticate user
- `POST /api/v1/auth/logout` - Logout user
- `POST /api/v1/auth/refresh` - Refresh access token

Servers:

- `GET /api/v1/servers` - List all servers
- `POST /api/v1/servers` - Add new server
- `GET /api/v1/servers/{id}` - Get server details

- `PUT /api/v1/servers/{id}` - Update server
- `DELETE /api/v1/servers/{id}` - Remove server

Websites:

- `GET /api/v1/websites` - List all websites
- `POST /api/v1/websites` - Create new website
- `GET /api/v1/websites/{id}` - Get website details
- `PUT /api/v1/websites/{id}` - Update website
- `DELETE /api/v1/websites/{id}` - Delete website

Customers:

- `GET /api/v1/customers` - List all customers
- `POST /api/v1/customers` - Create new customer
- `GET /api/v1/customers/{id}` - Get customer details
- `PUT /api/v1/customers/{id}` - Update customer
- `DELETE /api/v1/customers/{id}` - Delete customer

Billing:

- `GET /api/v1/invoices` - List invoices
- `POST /api/v1/invoices` - Create invoice
- `GET /api/v1/invoices/{id}` - Get invoice details
- `POST /api/v1/invoices/{id}/pay` - Process payment

Appendix C: Database Schema Overview

Core Tables:

- users (authentication, roles, permissions)
- servers (server inventory, roles, status)
- websites (website data, configurations)
- customers (customer accounts, billing info)
- domains (domain registrations, DNS zones)
- invoices (billing data, payments)
- tickets (support tickets, replies)
- services (customer services, subscriptions)
- packages (hosting packages, pricing)

Security Tables:

- waf_logs (WAF attack logs)
- malware_scans (antivirus scan results)
- brute_force_attempts (failed login attempts)
- ip_blacklist (banned IPs)
- security_alerts (security events)

Configuration Tables:

- settings (global settings)
- email_templates (email content)
- payment_gateways (payment provider configs)
- registrars (domain registrar configs)

Appendix D: Security Checklist

Pre-Launch Security Audit:

- [ ] Penetration testing completed
- [ ] Vulnerability scanning completed
- [ ] Code security audit completed
- [ ] Dependency security audit completed
- [ ] SSL/TLS configuration validated (A+ rating)
- [ ] WAF rules tested and tuned
- [ ] Brute force protection tested
- [ ] DDoS protection tested
- [ ] Database encryption verified
- [ ] Backup encryption verified
- [ ] Password policies enforced
- [ ] Two-factor authentication functional
- [ ] API rate limiting tested
- [ ] GDPR compliance verified
- [ ] PCI-DSS compliance verified (if processing payments)
- [ ] Security documentation complete
- [ ] Incident response plan documented
- [ ] Security training for staff complete

Document Approval

Prepared By: Romeo Alexandru Neacsu
Date: November 2, 2025

Approved By: [Project Stakeholders]
Date: [Approval Date]

Next Review Date: [Date]

End of Product Requirements Document