COMPARATIVE ANALYSIS MATRIX

	Imunify360	BitNinja	Drawback of BitNinja
General comparison	**A Comprehensive Security Suite with File Antivirus, IDS/IP, Web Application Firewall, Network Firewall, Domain Reputation and Incident Management**	**IP Reputation, HoneyPot, WAF, Log review, DDOS protection, Malware Detection**	**It's just a firewall, a very good firewall.**
PROBLEMS ADDRESSED			
Malware on the server	• File Antivirus with Safe Malware Clean-up • Instant real-time Malware Scanner • Database scan and clean-up • Automatic clean-up after the 3rd day	• File Antivirus with Cleanup • Changed files detection • Local scanning only • Quick-Scans for new virus definitions • Last on their list of features	• No support for malware stored inside of databases • Detects significantly less malware than Imunify360 • Infections are quarantine instead of repaired which breaks websites • Quick Scans must be initiated by the server admin and only help once you have a problem • Cannot cleanup injections, most cleanups are just about removing files • Admins are forced to write rules to detect infections missed by BitNinja
Too much care regarding security	• Plugins for cPanel, Plesk, DirectAdmin • Integrated with cPanel File Manager • Easy installation on server • Command-line interface and REST API for remote management and incident processing • Hooks/callbacks for asynchronous notification	• Plugins for cPanel, Plesk, DirectAdmin • Customer notification on vulnerability detection • SOS service	• Requires configuration for hosting • Common ports are blocked on cPanel

PROBLEMS ADDRESSED	Imunify360	BitNinja	Drawback of BitNinja
Outdated server software and web apps	• Real-time virtual defense of ALL web-applications (WordPress, Joomla, Drupal, etc) using a proactive defence WaF • HardenedPHP: PHP with the latest fixed vulnerabilities • KernelCare - Rebootless kernel patching included • Wordpress/Joomla/Drupal specific WAF rulesets only enabled as needed per VirtualHost	• WAF rules only	• Does not patch kernel and PHP interpreter • No proactive defense for real time application self protection • No kernel patches • System reboots will be needed to keep servers secure
Security is complicated	• Simple Web-based UI • Fully-automated security solution • 24/7 live support ready to help	• No Control Panel UI by default	• UI can not be enabled on the server, but only via BitNinja's portal
Web-spam and bad bots	• **Cloud-based heuristics and WAF** • WordPress/other popular CMS brute-force attack detection and blocking • Anti-bot protection • Vulnerability scanner blocking • Exploit scanners blocking • Zero-days exploiters blocking	• OWASPv3 rules • NGNIX WAF Firewall	• Transparent proxy does not support CL 5/6/7 • OWASP Rules have a high rate of false positives

PROBLEMS ADDRESSED	Imunify360	BitNinja	Drawback of BitNinja
Blacklisted Server IP	• Two-mode port firewall • SMTP Traffic Management • File Antivirus • Advanced IP/login pair protection	• IP Reputation is their strongest feature • A curated list of bad ips • Greylists	• Blocking at the IP level can lock out a large number of website visitors behind a single NAT IP Address and IPv6 to IPv4 bridges. • Blocking IP and Login pairs only blocks attackers. • IP Based blocking locks users out of all services for triggering IMAP or SMTP block
Excessive server resource usage	• Advanced Web Application Firewall • Network Firewall • Real-time malware detection and execution blocking • Automated malware script detection and clean-up with trimming instead of removal	• No protection	