Manage
Protect.

The Ultimate Cybersecurity Plan for MSPs.

SMBs are the #1 target for cyberattacks — but most don't have the protection they need. With Guardz, you can deliver enterprise-grade security at a price your clients can afford.

Guardz.

Simplifying cybersecurity

Guardz is a cost-effective, hassle-free detection and response platform, allowing MSPs to deliver comprehensive cybersecurity to SMB customers.

Incorporating advanced EDR protection from SentinelOne™ - named a Leader in the Gartner® Magic Quadrant™ for Endpoint Protection Platforms four years running.

Manage Protect offer this leading global cybersecurity platform with local billing and support, as well as access to certification and training.

Managed Detection and Response

Unified, AI-powered security monitoring. Detect and resolve incidents from a single interface, minimising response times and reducing complexity.

User centric threat management

Surveillance across identities, endpoints, email, cloud and data, to support proactive threat monitoring and effective BYOD policies.

Simplifying endpoint protection

Deploy and manage SentinelOne agents directly through the Guardz platform, simplifying the provisioning, deployment and management of endpoint security.

Local support and remediation

Discover first class local support and enablement with Guardz-certified engineers based in Melbourne, Sydney and Auckland

Secure your clients.
Simplify your operations.
Scale your business.

Guardz. Manage Protect.

The MDR Experience

The Guardz Ultimate Plan helps MSPs scale protection across clients without added complexity or cost. How will it work for you?

1 Onboarding

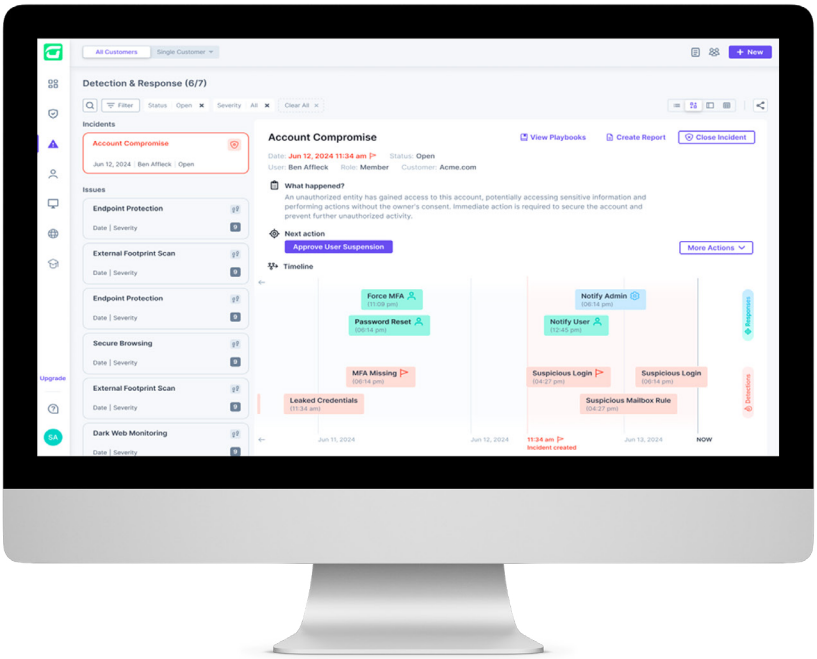
SentinelOne is embedded into the Guardz platform and managed by the Guardz MDR. Provisioning, deployment, and policy management is handled directly in Guardz.

2 Monitoring

Guardz MDR delivers continuous monitoring, incident triage, and rapid response via a fully managed 24/7 SOC. Guardz automatically pulls in every SentinelOne alert via API and enriches each one with user, device, and historical context. It then categorises threats, suppressing false positives and escalating verified alerts.

3 Threat Response

From a single console, analysts can kill malicious processes, quarantine infected files, or isolate compromised devices, and administrators rely on predefined SOPs to route any escalated incidents to their MSP by phone, chat, or email. Critical updates are pushed to Guardz console with optional escalation via chat or phone.



Get in touch.

1300 657 500 (AU)
0800 141 481 (NZ)
manageprotect.com

getguardz.com

Manage Protect.