Guardz Ultimate Plan

Unified AI-Powered Cybersecurity for MSPs

The Guardz Ultimate Plan combines advanced endpoint protection, identity-centric threat detection, and fully managed response, all in a unified platform designed for MSPs. With native ITDR, embedded SentinelOne EDR and Checkpoint Harmony email security, along with integrated MDR; MSPs can scale protection across clients without added complexity or cost.

Platform Security Controls

Comprehensive, multi-layered protection across all critical attack surfaces:

ITDR:

Identity Threat Detection and Response actively benchmarks and analyzes user behavior as well as attack patterns.

Email Security:

Embedded Check Point Harmony email security with in-line API for phishing, zero-day malware, URLs and internal email scanning.

Endpoint Security:

Embedded SentinelOne EDR with AI-native malware and ransomware detection and real-time response.

Cloud Data Protection:

Identifies unauthorized access and protects business data in cloud drives.

Security Awareness Training:

Contextual training to improve employee cyber hygiene and reduce human error.

Phishing Simulation:

AI-powered & templated simulations to test user resilience and identify gaps in awareness.

Dark Web Monitoring:

Continuously scans dark web for leaked credentials and sensitive data.

External Footprint Monitoring:

Detects exposed digital assets like domains, IPs, and cloud resources to reduce attack surface.

Managed Detection & Response (MDR)

Guardz MDR delivers continuous threat hunting, monitoring, incident triage and rapid response for all identity (ITDR), SentinelOne (EDR) and Checkpoint (email) events via a fully managed 24/7 SOC.

Alert Ingestion:

Ingests and classifies abnormal user behavior in the cloud and S1 alerts via API (no extra agent).

Classification & Triage:

Uses Agentic AI to triage and enrich raw findings, categorize threats, suppress benign detections, and escalate verified ones.

Response Actions:

User suspension and device isolation according to MSP approvals, while playbooks and incident reports steer further mitigation.

Service-Level Commitments:

24/7/365 expert managed SOC with 60-minute SLA for critical alerts and reported incidents.

Communication Channels:

Real-time incident communication via phone, email, chat, and platform notifications, with full audit trail per incident.

Integration Scope:

MDR actively covers SentinelOne EDR and Cloud ITDR with additional user posture and enriched data points as needed.

Identity Threat Detection & Response = Managed ITDR

Microsoft 365 & Google Workspace

Guardz ITDR continuously monitors user behavior to flag abnormal patterns in cloud logs, preventing account takeover by suspending users before damage occurs.

Cloud-Native Coverage:

Natively integrates with M365 and Google Workspace to run analysis across the most critical cloud logs without complex integrations or service accounts.

Behavioral Analytics & Baselining:

Monitors user behavior to build benchmarks over time and detect deviations from these normal patterns, spotting threats like credential abuse and privilege misuse.

Automated Threat Response:

One-click remediations like account suspension and user isolation are essential responses to minimize time to containment and prevent lateral movement.

Incident Timeline & Forensics :

Visualizes the full attack path across identity findings to help admins understand the who, what, when, and how, making incident investigation fast and actionable.

Cross Signal Mapping:

Correlates diverse findings from configurations, logins, mailboxes, and other log activity to expose complex identity attacks that would otherwise evade detection.

Built-In Use Cases & Playbooks:

Attack scenarios like BEC, ATO, and Data Exfiltration, are formulated by expert researchers and threat hunters who also define playbooks to guide MSPs through incident response.

ITDR Technical Requirements & Deployment

Supported Integrations:

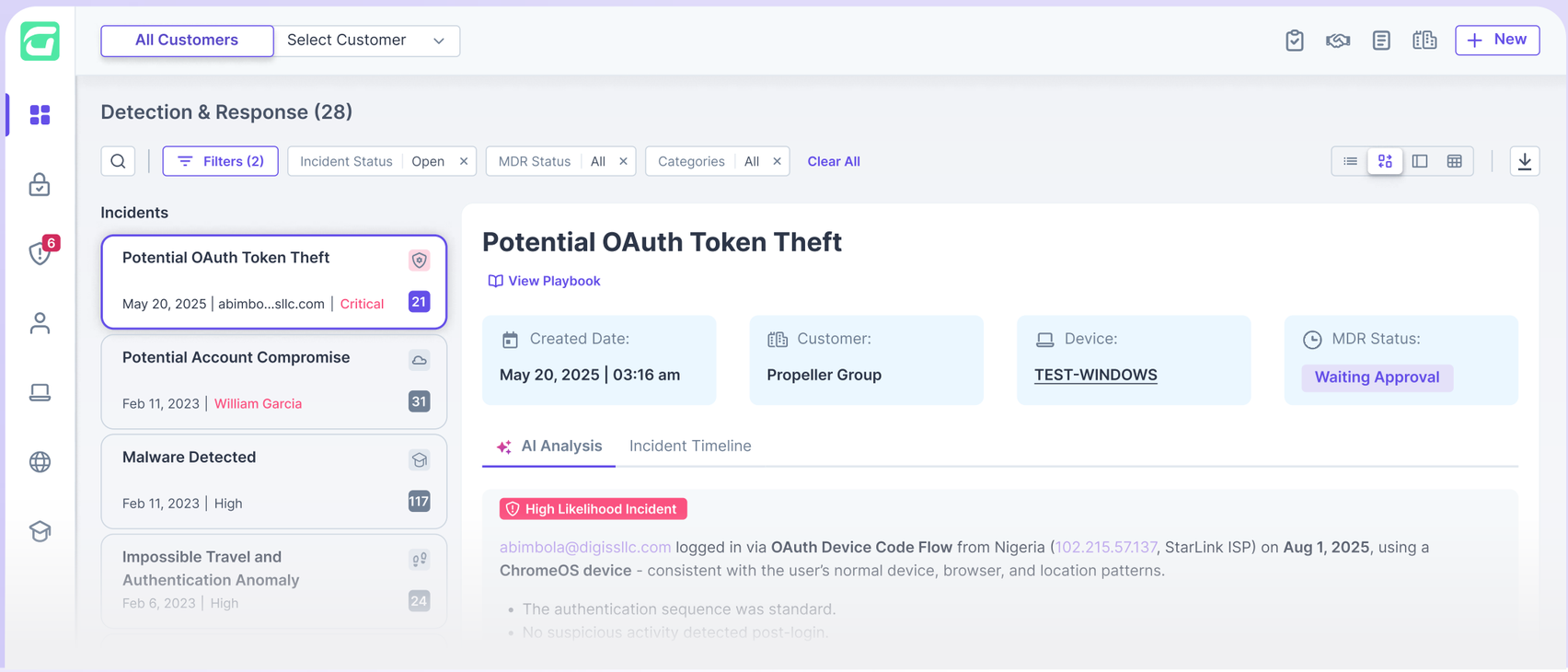
- Microsoft 365
- Google Workspace

Cloud Identity Source:

- Microsoft Entra ID
- Google Identity

Deployment & Management:

- Agentless with secure API integrations (Graph API)
- Enterprise Applications: Detection (read-only) and Response (read-write)
- Permissions are granted per OAuth 2.0 protocol with admin privileges



SentinelOne Singularity Control = Managed EDR

Embedded directly into the Guardz platform and managed by Guardz MDR.
Delivers enterprise-grade endpoint protection with lightweight, autonomous agents.

Behavioral and Static AI Engines:

Detects ransomware, fileless and zero-day threats via real-time analysis of processes and memory without cloud reliance.

Device Control:

Controls USB, Bluetooth, and HID devices to prevent unauthorized access.

Automated Response:

Agents autonomously terminate processes, quarantine files, and use rollback via Windows VSS.

Threat Investigations:

Storyline correlation with integrated VirusTotal and MITRE ATT&CK intelligence.

Firewall Control:

Enforce network access rules based on device location with profile-based policies.

Vulnerability Management:

Scans installed third-party apps and maps CVEs to MITRE ATT&CK.

Policy Management:

Global detection and remediation policies managed per org or customer via Guardz console.

Application Inventory:

Provides versioned software inventory for audit, compliance, and hygiene visibility.

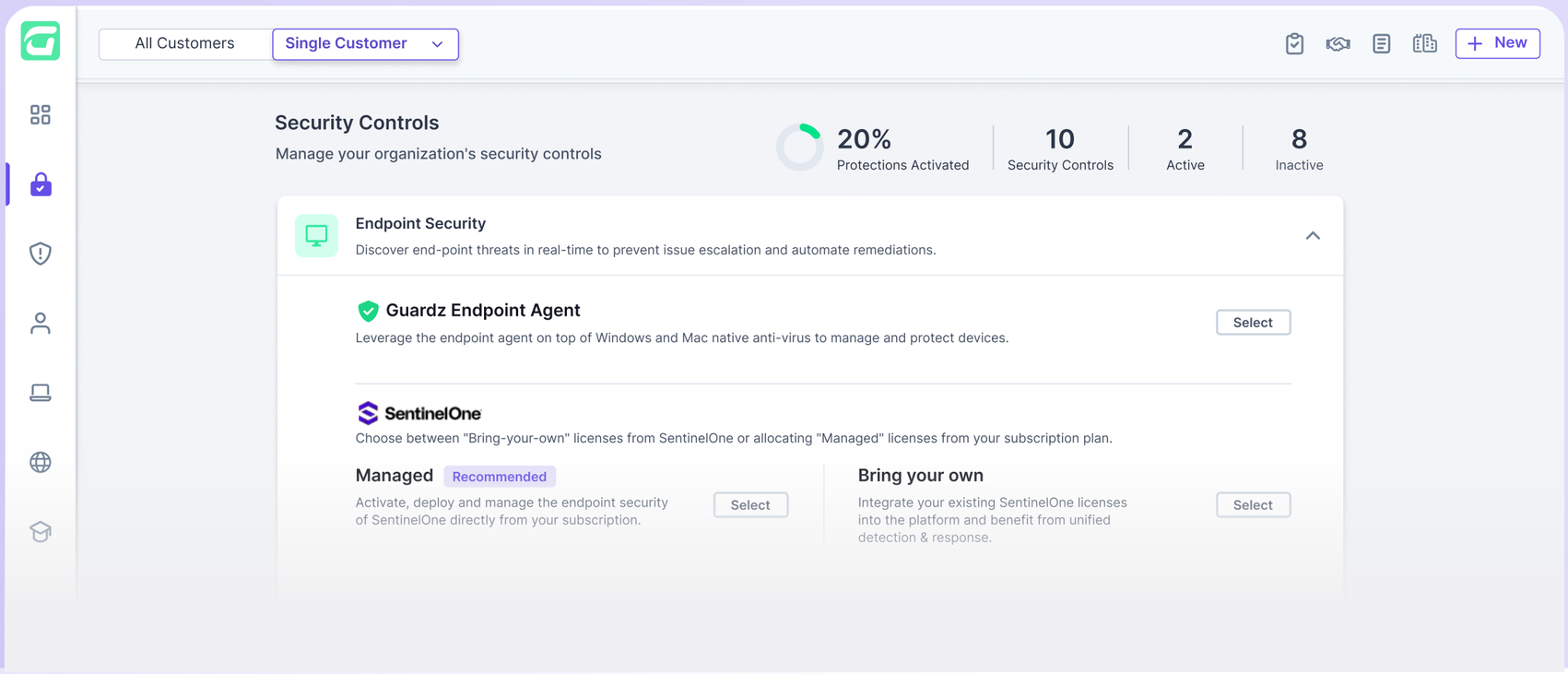
S1 Technical Requirements & Deployment

Supported OS & Platforms:

- Windows 7-11, Server 2008-2019/Core
- macOS Ventura/Monterey/Big Sur
- Linux distros (Ubuntu, RHEL, CentOS, Oracle, AMI)
- Legacy Windows XP/Server 2003
- Containers and VDI (Kubernetes, VMware, Citrix, Hyper-V)

Deployment & Management:

- Silent agent installs using RMM & MDM flows.
- Auto-provisioning from Guardz platform.
- Minimal end-user involvement.
- Alerting via email and syslog.



Core Email Security Capabilities

By integrating Check Point Harmony Email security into the same platform that also safeguards endpoints, identities, and more, Guardz enables service providers to close the gaps that attackers exploit while optimizing daily operations.

AI-Based Anti-Phishing:

Analyzes 300+ indicators per message to stop advanced phishing, BEC, and spoofing attacks.

Inline API Scanning:

Patented pre-delivery and in-mailbox inspection that detects threats missed by Microsoft/Google.

Zero-Day Malware Defense:

Parallel malware analysis and sandboxing to block ransomware and unknown file exploits.

Malicious URL Protection:

URL reputation checks, rewriting, and click-time analysis to prevent web-based attacks.

Allow/Block List Control :

Supports global allow/block lists of senders, domains, IPs and headers.

Internal Email Protection:

Scans lateral emails to stop internal spread of phishing or malware.

Encrypted Attachment Handling:

Inspects password-protected files for hidden threats.

Unified Guardz Experience:

Provisioned and managed directly from Guardz.

Technical Requirements & Deployment

Supported Platforms:

Microsoft 365
Google Workspace

Shared Mailbox Support:

Protection extends to shared mailboxes and group mailboxes.

Unified Policy Management:

All organization-level settings controlled through Guardz.

Deployment Model:

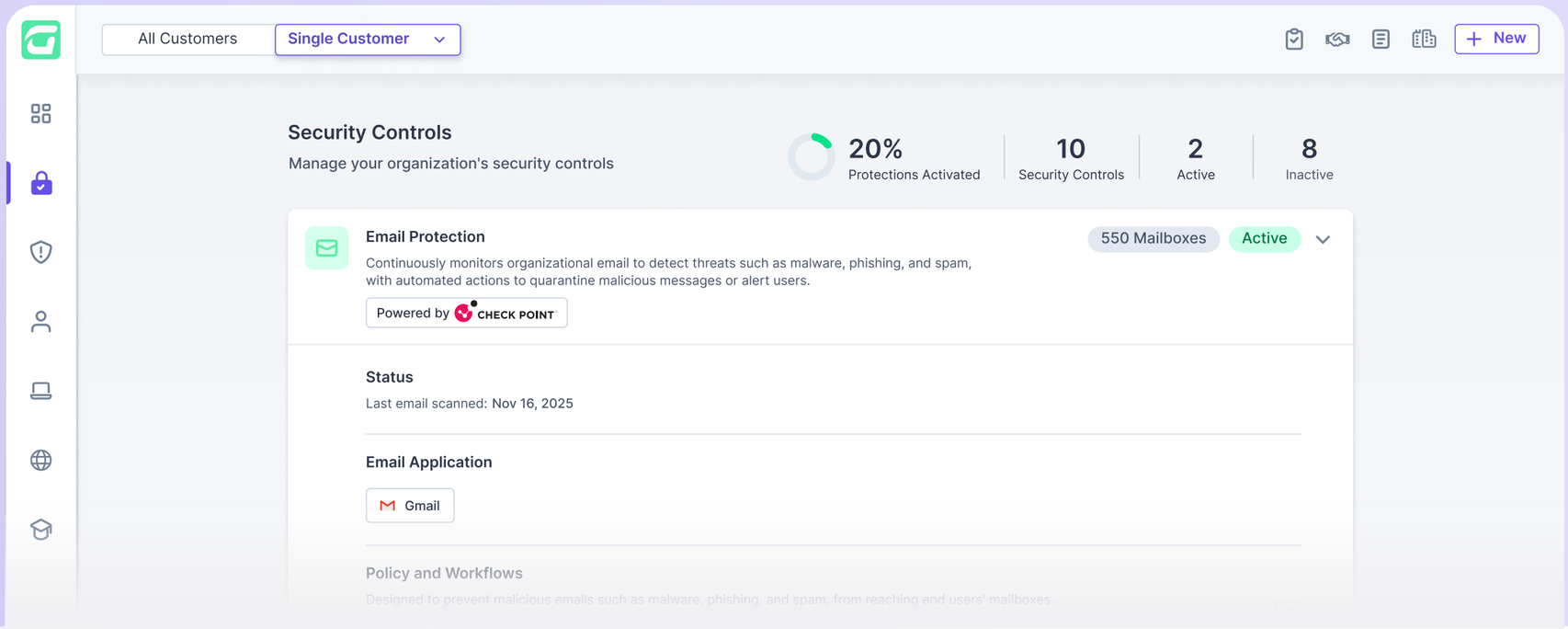
100% API-based; no MX record changes, no SEG, no proxy, no appliances.

Native Quarantine Compatibility:

Works with Microsoft 365 Unified Quarantine.

OAuth Permissions:

Uses secure org-level read/write scopes for scanning and enforcement.



Adaptive Security Awareness Training Capabilities

Guardz provides MSPs with ready-to-launch security training and phishing simulation assets that support consistent delivery of security programs and measurable improvement in user behavior.

Phishing Simulations:

Runs one-click, pre-populated simulations across QR-based phishing, credential harvesting, malicious attachments, and link-based attacks.

Various Difficulty Levels:

Supports low, medium, and advanced simulation difficulty to align with user maturity and risk tolerance.

Landing Pages & Post-Click Training:

Includes pre-populated landing pages and post-click just-in-time training to reinforce safe behavior after interaction.

Training Content Coverage:

Provides a catalog of security awareness modules covering common threats and user-driven risk scenarios.

In-Context Training:

Delivers targeted guidance tied to phishing simulation activity, reinforcing learning at the point of interaction.

Quizzes & Scoring:

Includes knowledge checks after training modules with user scores and the option to retake quizzes to improve results.

AI-Generated Phishing Emails:

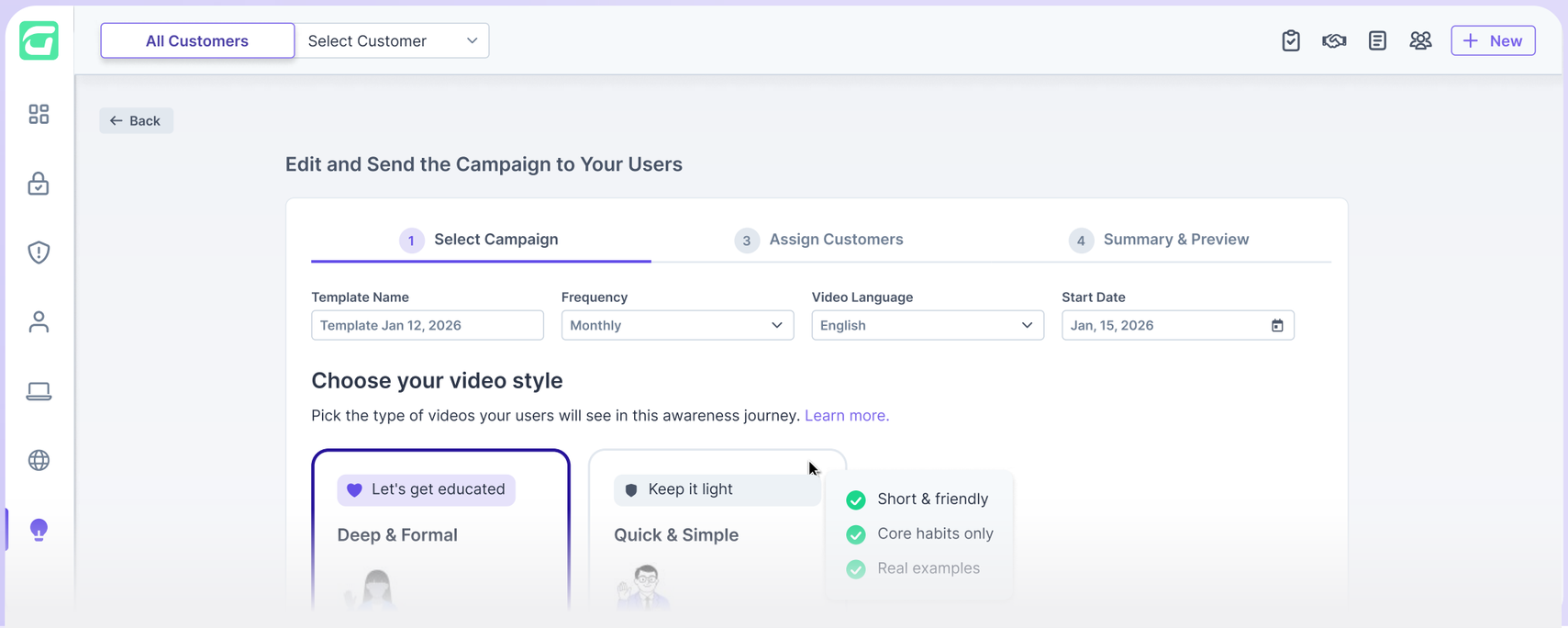
Create realistic, up-to-date phishing emails with AI using tone, industry, and language inputs, fully customizable for any target group.

Real-Time Feedback:

Shows users immediately when an answer is incorrect and provides the correct response to reduce repeat mistakes.

Security Awareness Training Technical Requirements & Deployment

- 7 supported languages: English, Dutch, Brazilian Portuguese, French, German, Spanish, and Hebrew
- Coverage of key threat areas including AI, device security, and data protection
- Regionalized content for Australia, Canada, and the UK
- Flexible delivery schedules with randomized send options
- Adaptive video formats from formal training to micro-learning
- Automated assignment for new customers and users
- Multiple sending domains to improve deliverability



Discover the power of the Guardz platform

Guardz Ultimate Plan - Technical Datasheet

For more information please contact,
Luke Evans
Director
Phone: +442920006424
Email: luke@optimisetech.co.uk
Optimise Tech Solutions