



Cy-Napea®

XDR: Redefining Extended Detection and Response

Experience the future of cybersecurity with advanced XDR capabilities.
Leverage AI-powered insights, multi-layered threat detection, and automated
response to secure your entire digital landscape.

Protecting your business from evolving threats, one step ahead.

Cy-Napea

Cyber Guard



The need for XDR



Only advanced security can combat advanced attacks

- More than 60% of breaches **involve hacking** (requires advanced defenses)
- **80% of businesses** have been attacked
- XDR and Endpoint Protection Platforms (EPP) are associated with an **82.5% reduction in serious security incidents**



The attack & security perimeter is moving beyond the endpoint

- Almost **40% of breaches include compromised credentials**, and 15%+ - **phishing** (EPP solutions address these risks only partially)
- **76% of security** and IT teams struggle with **no common view** over applications and assets



Breach is inevitable – you need to be prepared

- **70 days** to contain a breach
- **USD 4.35 million** – average total cost of a data breach
- **Failure to report** security incidents within a strict time-frame can result in compliance penalties

Sources: “Data Breach Investigations Report”, Verizon, 2024; “Data Breach Investigations Report”, Verizon, 2022”; “Cost of data breach report”, 2022, IBM Security & Ponemon Institute; “Costs and Consequences of Gaps in Vulnerability Response,” ServiceNow, 2020, Investigation or Exasperation? The State of Security Operations”, IDC

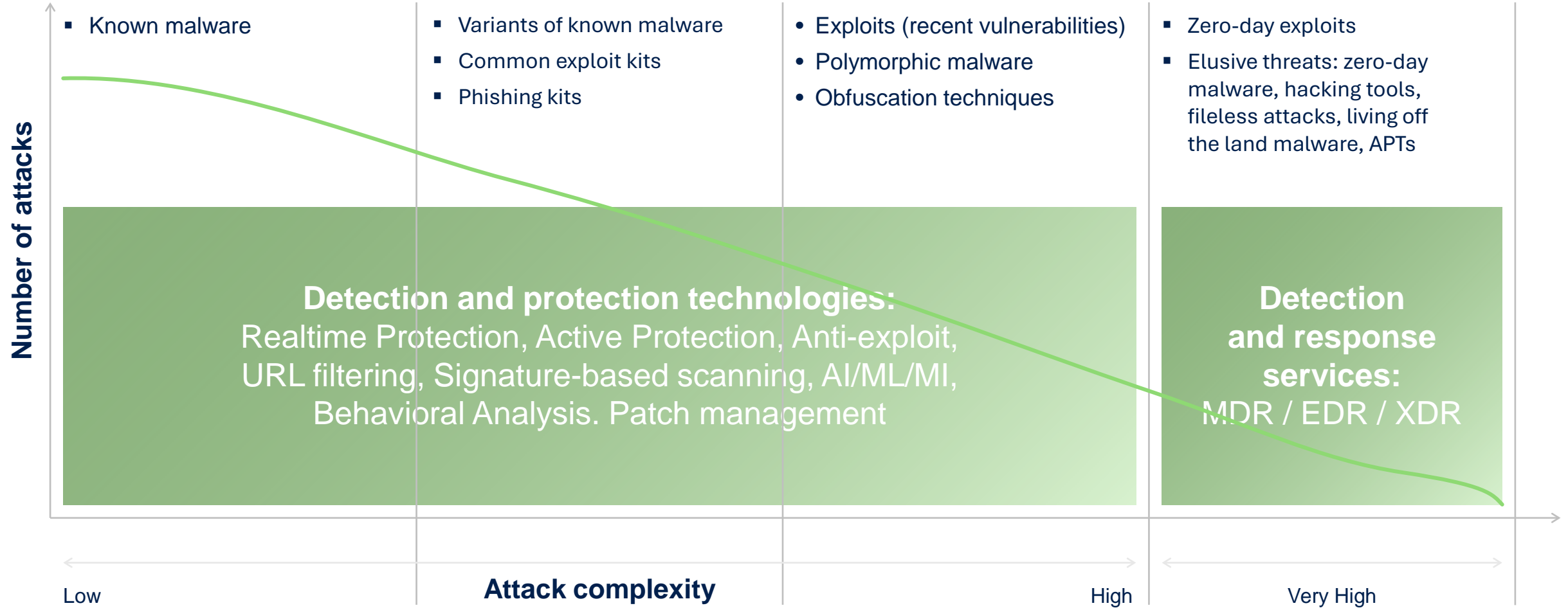
Intro to Managed Endpoint Security Services



	BASIC ENDPOINT SECURITY SERVICES	MANAGED EDR SERVICE	MANAGED XDR SERVICE
Purpose	Detect and block (common threats)	Detect, block, analyze, and respond (all threats)	
Commonly used technology	Antivirus, antimalware	EDR / XDR (adds behavioral anomaly detection, event correlation)	
Protected sources	Endpoint	Endpoint	Endpoint + Additional sources – e.g. email, identity, Cloud apps, network, IoT, etc.
Remediation	NO	YES	
Support	Passive service	Active service according to SLAs up to 24/7	

Get access to advanced threat protection on demand

How advanced endpoint security ensures threat-agnostic protection



Service providers are here to help



Ensure your business is always protected, up and running so you can focus on what matters – your business

Access to scalable IT and security expertise

- Better protection with advanced capabilities
- Value-added management with pre-integration
- Skilled practitioners focused on protecting your business
- Service agility at the pace and cost you require

Rapid response – 24/7 assistance and support

- Technology developed to rapidly detect, recommend and offer extensive, remote remediation and support options
- Can be right-sized to your unique business requirements

Cost-efficiency

- Reduce or remove expensive staffing costs
- Predictable costs based on SLAs
- Move from CapEx to OpEx



Why work with MSP rather than a vendor?



Existing advanced security technologies introduce significant costs, require expensive skillset, and a long time to value. Cy-Napea helps your Provider keep you secure at a cost you can afford.



Cost & complexity



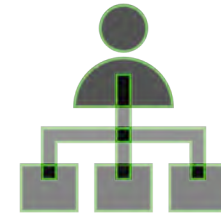
Effective and cost-efficient service for SMB and mid-market



Limited business continuity and solution sprawl



Integrated across NIST – incl. remediation & recovery



Limited compliance and disaster recovery support



Compliance and data protection with the ease you need

Limitations

Cy-Napea opportunity

Cy-Napea® XDR: Top use cases



Protection for most vulnerable attack surfaces – endpoints, email, identity, M365 apps



Detect & block attacks before a breach



Respond before damage is done



Enable compliance and protect sensitive data



Outsource your security and enable 24/7 advanced protection at minimal cost



Streamlined, minutes-not-hours incident investigations



Ensure business continuity during attacks



Ongoing reporting

Protect the most vulnerable attack surfaces



Leverage AI innovations and consolidation to protect clients' high-risk surfaces

Designed to **protect endpoints** with **visibility across the most vulnerable attack surfaces**, incl.:

- **Endpoints** – Windows
- **Email** – Advanced Email Security (Perception Point)
- **Identity** – Entra ID
- **Microsoft 365 apps**, incl. SharePoint, OneDrive, Teams – Collaboration App Protection (Perception Point)



Improved performance

- **Single agent for:** XDR, EDR, MDR, antimalware & anti-ransomware, DLP, backup, disaster recovery, endpoint management and monitoring



Rapid attack prioritization and analysis



Ensure faster response to incidents than ever before with rapid analysis, unlike services based on complex EDR technologies

AI-based attack prioritization

Fast reporting on security incidents

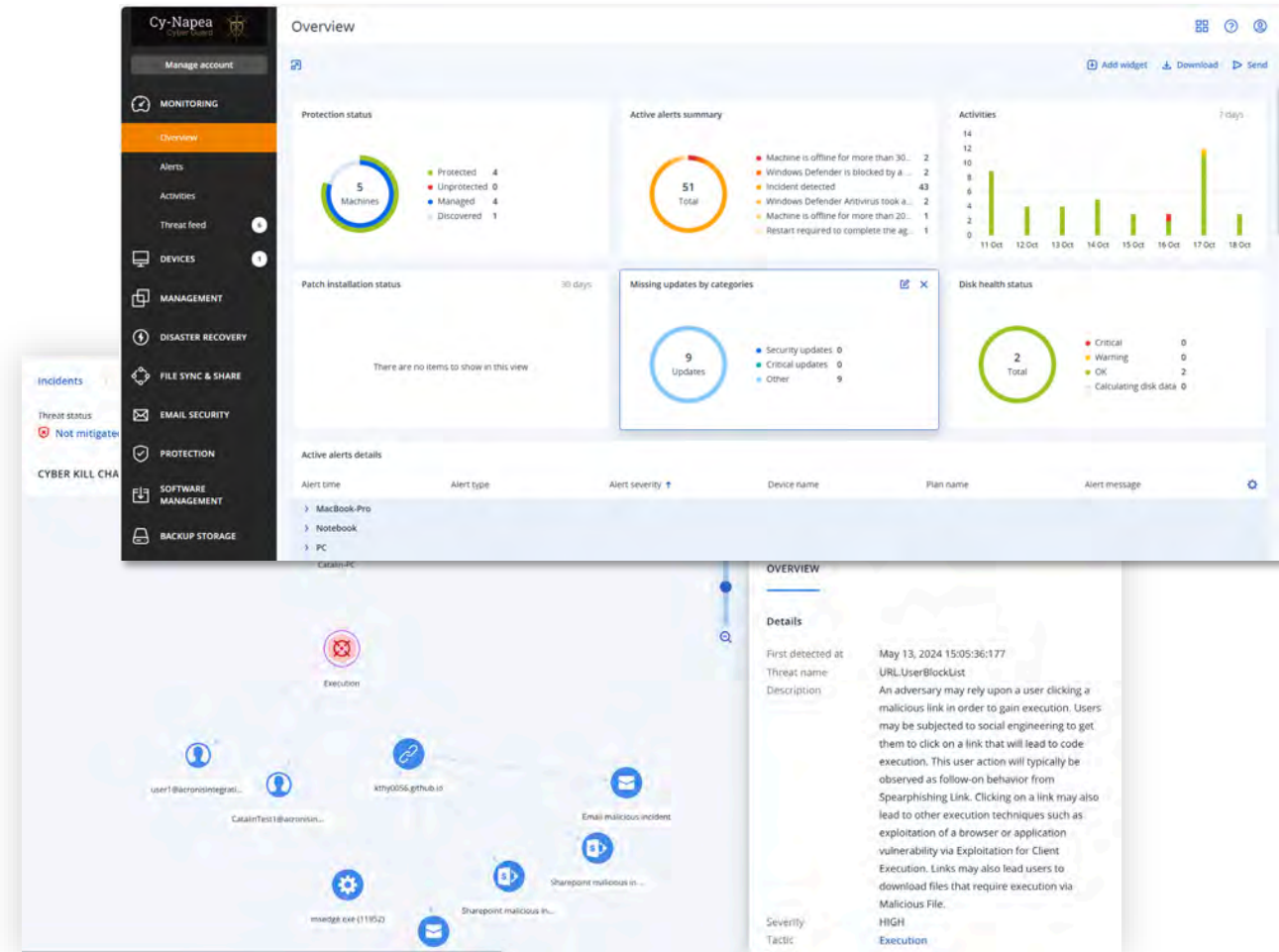
- How did the threat get in?
- How did it hide its tracks?
- What harm did it cause?
- How did it spread?

Minimize productivity disruptions

- Incident analysis done in minutes rather than hours

Reduce security risks

- Protection from advanced threats and targeted attacks: across endpoints, email, identity, Microsoft 365 apps
- Response that stops the breach, ensures continuity and data protection, and prevents future intrusion



XDR that not only remediates but ensures business continuity

Succeed where other solutions fail. Unlock the full power of a platform with integrated capabilities for unmatched business resilience



Investigate further – remote connection, forensic backup



Contain threats – isolation, user session termination



Remediate – stop malicious processes, quarantine, remove attachments & URLs, suspend accounts, rollback



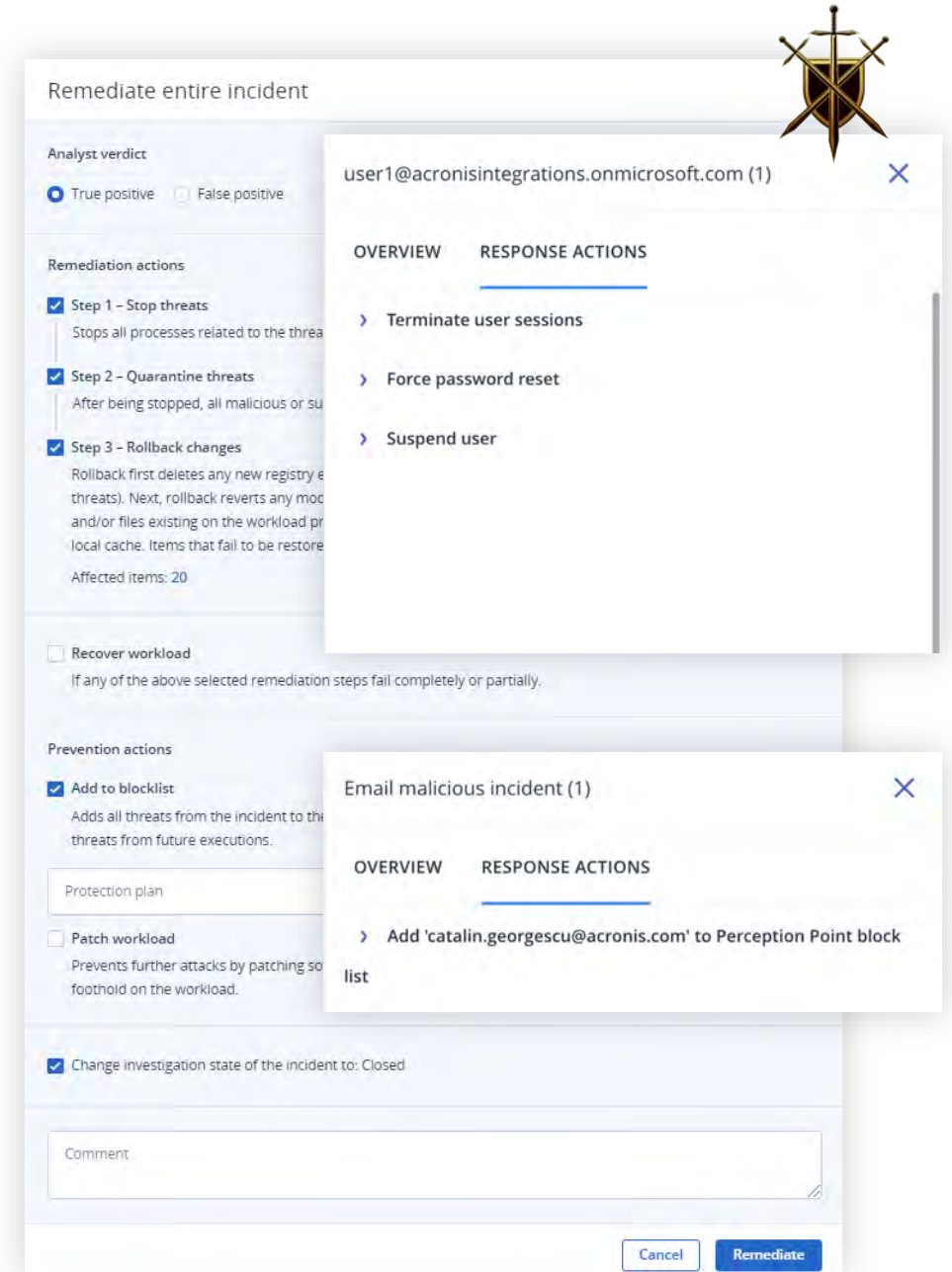
Prevent – patch management, block email address, force password reset



Recover – file/image recovery, attack-specific rollback, disaster recovery



Extends EDR response actions



Effective & Efficient



Stop most threats before they become breaches



Next-generation anti-malware & anti-ransomware: Prevent threats with signature- and behavior-based endpoint protection



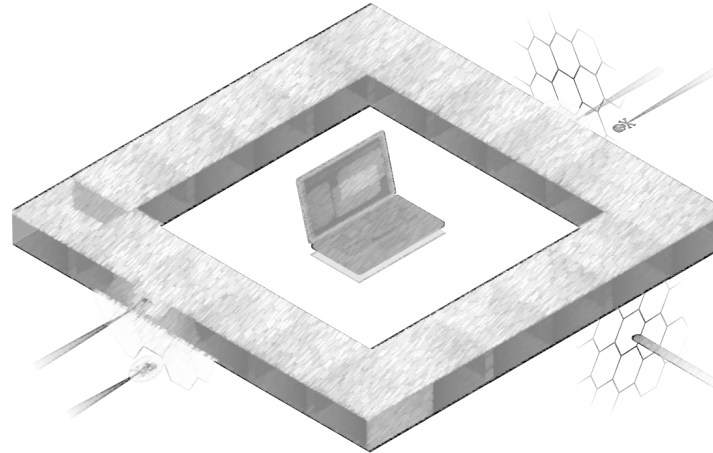
URL filtering: Extend cyber protection to web browsing to prevent attacks from malicious websites



Exploit prevention: Reduce the risks of exploits and malware taking advantage of clients' software vulnerabilities



Smart protection plans: Auto-adjust patching, scanning and backing-up based on threat alarms from Cy-Napea® Cyber Protection Operations Centers



Forensic backup: Enable forensic investigations by collecting digital evidence in image-based backups



Better protection with fewer resources: Protect backups against malware and enable more aggressive scans by offloading data to central storage, including the cloud



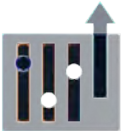





Safe recovery: Prevent threat reoccurrence by integrating anti-malware scans of backups and antivirus database updates into the recovery process



Global and local allowlists: Created from backups to support more aggressive heuristics, preventing false detections

Cy-Napea: Business Continuity Across NIST



						
	GOVERN	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Advanced Security + XDR	<ul style="list-style-type: none">Centralized policy managementRole-based managementInformation-rich dashboardSchedulable reporting	<ul style="list-style-type: none">Software & Hardware inventoryUnprotected endpoint discovery	<ul style="list-style-type: none">Vulnerability assessmentsDevice controlSecurity configuration management	<ul style="list-style-type: none">Threat telemetry across endpoints, identity, email, M365 appsAI/ML-based behavioral detection & anti-ransomwareExploit prevention & URL filteringThreat hurting	<ul style="list-style-type: none">AI-based incident prioritizationAi-guided analysisRemediation and isolationForensic backups	<ul style="list-style-type: none">Rapid rollback of attacksOne-click mass recoverySelf-recovery
Cy-Napea Cyber Protect Cloud	<ul style="list-style-type: none">Provisioning via a single agent and platform	<ul style="list-style-type: none">Software inventoryData classification	<ul style="list-style-type: none">Patch managementDLPBackup integrationCyber scripting	<ul style="list-style-type: none">Email security	<ul style="list-style-type: none">Investigation via remote connection	<ul style="list-style-type: none">Pre-integrated with disaster recovery

Proactive, Active, Reactive protection that also meets compliance reqs. and protects sensitive data.

Powered by award-winning endpoint



AV-Comparatives Approved Business Security

Real-World Protection Test - **0 false positives**

Malware Protection Test - **0 false positive**



AV-Test Certified

Detection and Blocking of Advanced Attacks – **100% detection**

0 false positives



ICSA Labs Certified
0 false positives



VB100 Certified
0 false positives



Gold medal for Endpoint protection



4.5 Excellent



Microsoft Virus Initiative member



Anti-Malware Testing Standard Organization member



Anti-Phishing Working Group member



Anti-Malware Test Lab participant and test winner



VIRUSTOTAL member



Cloud Security Alliance member



Cy-Napea technology

Succeed where point solutions fail. Unlock the full power of a platform with consolidated capabilities

■ Provisioned via a single agent

- 20% faster onboarding of new clients compared to point solutions
- Provisioning of new services in minutes
- Noticeably improved performance of endpoints

■ Award-winning detection technologies:

- Signature & behavior-based detection, AI/ML/MI, anti-exploit, anti-cryptojacking, anti-ransomware, email security with next-generation hardware-level dynamic detection, URL filtering

■ Proprietary and 3rd party threat intelligence

■ Pre-integrated with best-of-breed data protection and endpoint management



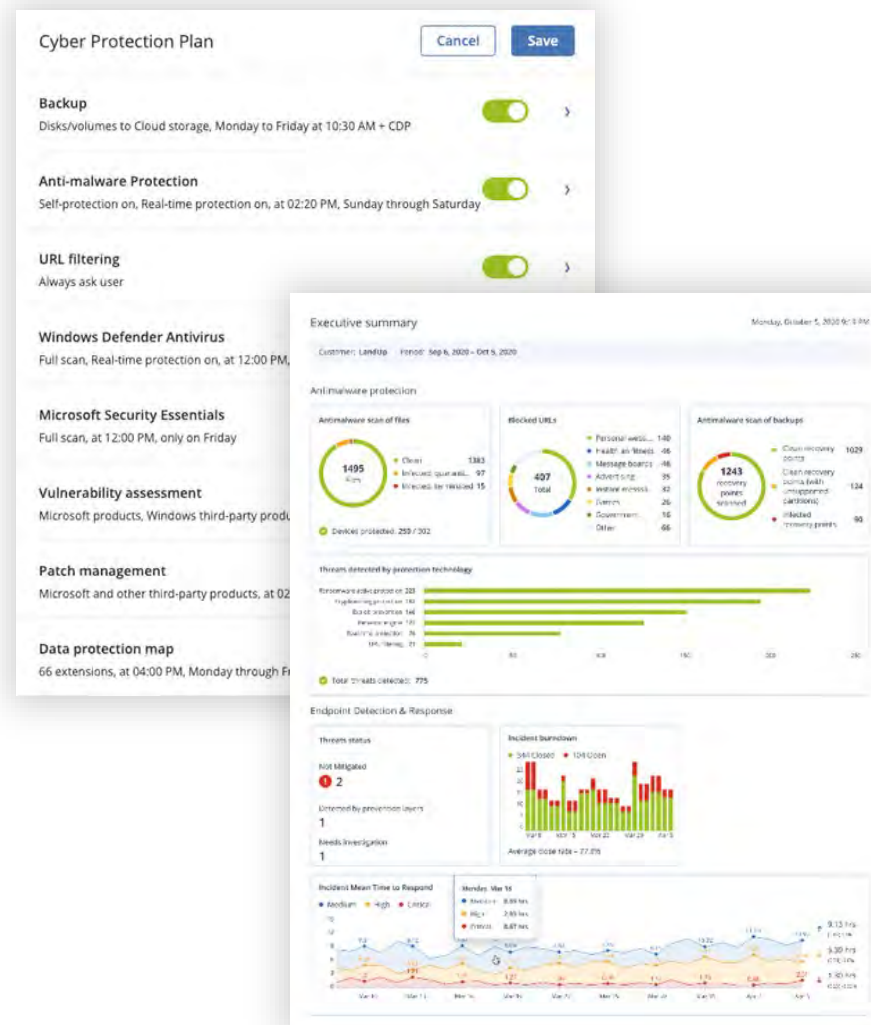
Rapid service provisioning



Full protection across NIST



Better performance



Comprehensive Cyber Protection Platform

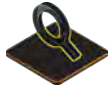


Cross-NIST Platform Powered by AI

Cyber Protect / Cloud platform



Endpoint
Detection
& Response



Incident
Investigation



Endpoint
Protection



Malware
Resistance



Email
Security



Ransomware
Protection



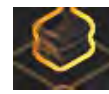
Continuous
Data
Protection



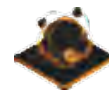
Disaster
Recovery



Data
Visibility



Data Loss
Prevention



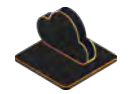
Vulnerability
Assessment



Patch
Management



Remote
Access



Secure File
Sync and
Share

Security

Backup & DR

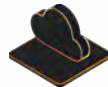
IT Management

Streamlined Administration

Partner Ecosystem



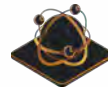
Managed Service
Providers



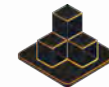
Cloud Service
Providers



RMM/PSA/CSA
ISVs



Network Service
Providers



Resellers and
Distributors

End Customer

Note: RMM (Remote Monitoring Management); PSA (Professional Services Automation); CSA (Cloud Service Automation); ISV (Independent Software Vendor).

Cy-Napea

Cyber Guard



Cy-Napea® XDR

The Future of Cyber Defense

Email: office@cy-napea.com

Phone: +1 (214) 646-3262; +359 884 04 88 03

Website: www.cy-napea.com