

Cy-Napea®

EDR from the Future

Your defense against tomorrow's threats
provided today.

Cy-Napea
Cyber Guard

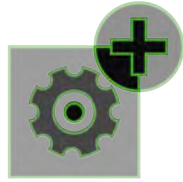


Your Risk is Real and Growing



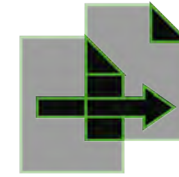
Only advanced security can combat advanced attacks

- **>60%** of breaches **involve hacking**
- **207 days** to identify a breach
- **80% of businesses** have been attacked



Breach is inevitable – are you prepared?

- **USD \$4.35 million** – average per breach
- **70 days** average to contain



For some – compliance is mandatory

- **70% of breaches involve PII**
- **Failure to report security incidents** within a strict time-frame can result in penalties

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

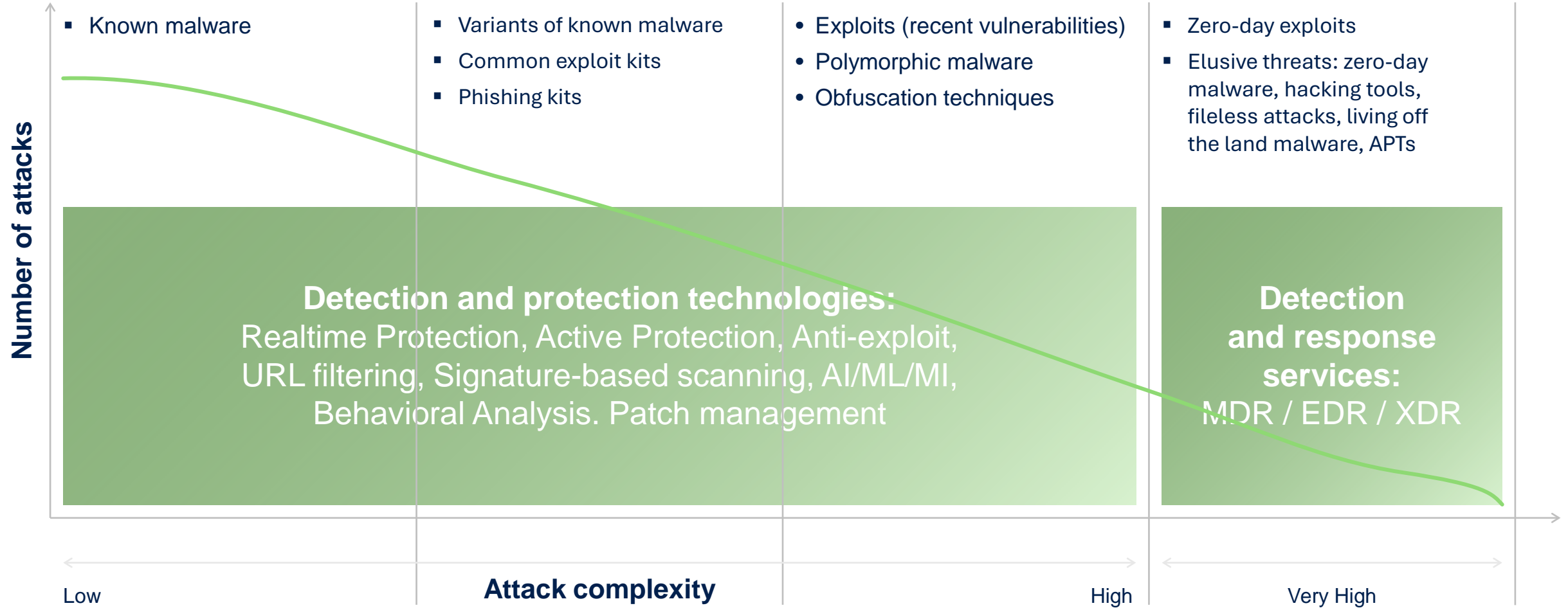
Intro to Managed Endpoint Security Services



	Essential Endpoint Security Services	Advanced Endpoint Security Services
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)
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 endpoint 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.

Challenges with Vendor MDR



Cost beyond IT budget



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

Opportunity with MSP



Limited business continuity and solution sprawl



Protection across NIST: from Identify to Recover



Limited compliance and disaster recovery support



Compliance and data protection with the ease you need

Top 3 use cases



Detect and block attack before breach

- **Monitor and correlate events** on endpoints
- **Block common threats** with award-winning NGAV
- **Detect advanced threats** and analyze in minutes



Respond before damage is done

- **True business continuity** with pre-integrated recovery
- **Reduce impact** – quarantine processes, isolate workloads
- **Limit attack surface** for future protection



Enable compliance and cyber insurance

- **Report on incidents across endpoints**
- **Classify sensitive data**
- **Collect forensic data** in backups



Simplify endpoint security – ensure rapid detection and response to advanced attacks while knowing your business will always remain up and running



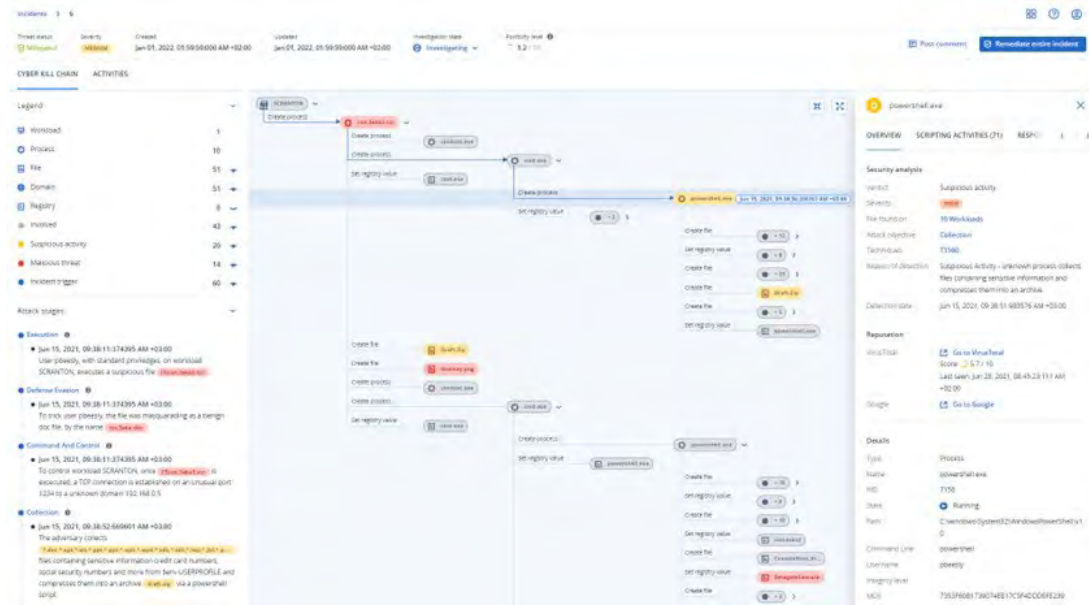
Rapid attack prioritization and analysis



Business continuity with integrated backup and recovery



Effective and efficient service



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

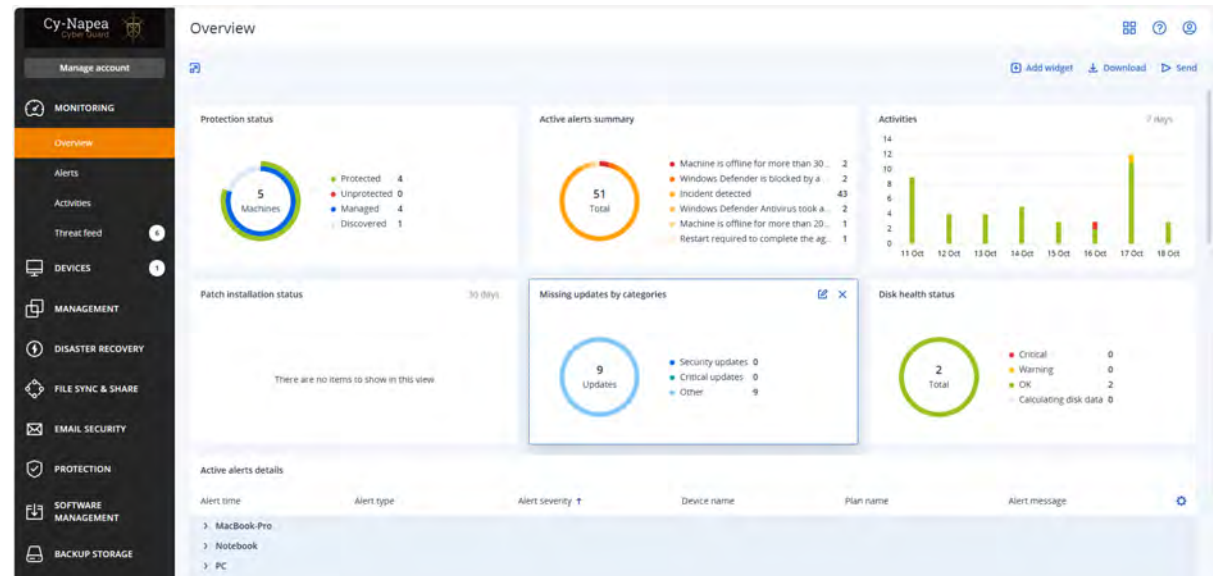
- How did the threat get in?
- How did it hide its tracks?
- What harm did it cause?
- How did it spread?

Minimize productivity disruptions

- Incident analysis done in minutes rather than hours

Reduce security risks

- Protection from advanced threats and targeted attacks
- Response that stops the breach, ensures continuity and data protection, and prevents future intrusion



Unmatched business continuity and resilience

- Succeed where siloed services fail. Ensure your business is protected with the full power of a platform integrating capabilities for unmatched business resilience
- More extensive investigations via remote connection and collection of digital evidence and forensic info in backups.
- Containing threats by network isolating the affected workload
- Remediating attacks by killing malware processes, quarantining threats, and rollbacking changes.
- Preventing incidents from reoccurring with software patch management and by blocking analyzed threats from execution
- Ensure unmatched business continuity with integrated recovery capabilities, including attack-specific rollback, file- or image-level recovery, and disaster recovery
- Ensure that your business will always remain up and running with a rapid, more holistic response to incidents.

Remediate entire incident



Analyst verdict

☒ True positive ☐ False positive



Remediation actions

☒ Step 1 - Stop threats

Stops all processes related to the threat.

☒ Step 2 - Quarantine threats

After being stopped, all malicious or suspicious processes and files are quarantined.

☒ Step 3 - Rollback changes

Rollback first deletes any new registry entries, scheduled tasks or files created by the threat (and any of its children threats). Next, rollback reverts any modifications made by the threat (or its children) to the registry, scheduled tasks and/or files existing on the workload prior to the attack. To optimize speed, rollback tries to restore items from the local cache. Items that fail to be restored will be restored by the system from backup images.

Affected items: 20

☐ Recover workload

If any of the above selected remediation steps fail completely or partially.

Prevention actions

☒ Add to blocklist

Adds all threats from the incident to the blocklist in the selected protection plans. This action will prevent these threats from future executions.

Protection plan

☐ Patch workload

Prevents further attacks by patching software that contains vulnerabilities used by attackers in order to get a foothold on the workload.

☒ Change investigation state of the incident to: Closed

Comment

Cancel

Remediate

Effective & Efficient

Stop most threats before they become breaches



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



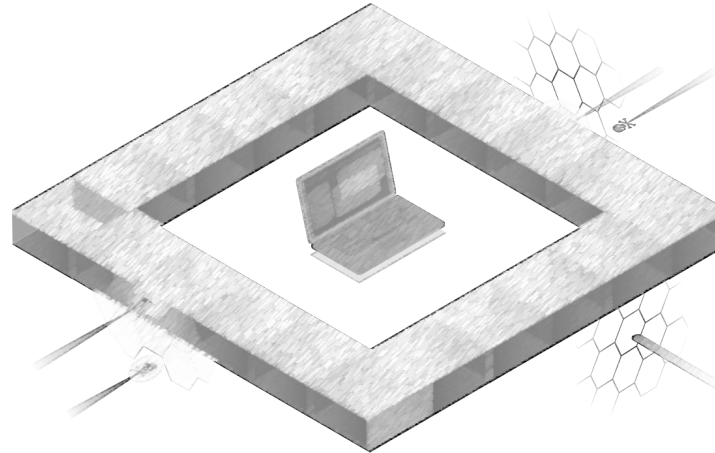
URL filtering: Extend cyber protection to web browsing to prevent attacks from malicious websites



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



IDENTIFY



PROTECT



DETECT



RESPOND



RECOVER

Advanced Security + EDR	<ul style="list-style-type: none">▪ Hardware inventory▪ Unprotected endpoint discovery	<ul style="list-style-type: none">▪ Vulnerability assessments▪ Exploit prevention▪ Device control▪ Security configuration management	<ul style="list-style-type: none">▪ Emerging threats feed▪ Search for IOCs of emerging threats▪ Anti-malware & anti-ransomware▪ AI/ML-based behavioral detection▪ URL filtering	<ul style="list-style-type: none">▪ Rapid incident analysis▪ Workload remediation with isolation▪ Forensic backups	<ul style="list-style-type: none">▪ Rapid rollback of attacks▪ One-click mass recovery▪ Self-recovery
	<ul style="list-style-type: none">▪ Software inventory▪ Data classification	<ul style="list-style-type: none">▪ Patch management▪ DLP▪ Backup integration▪ Cyber 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

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



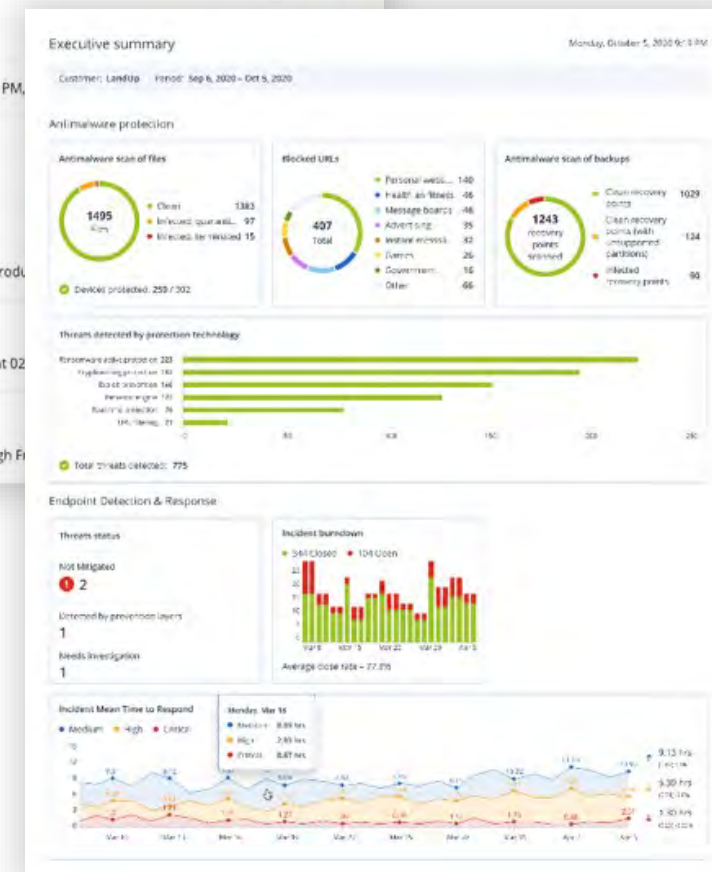
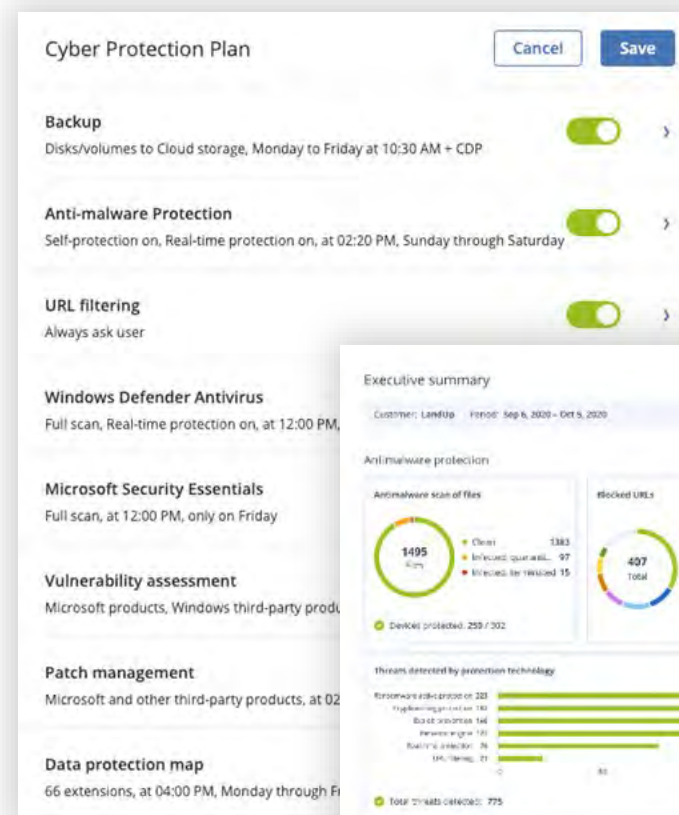
Rapid service provisioning



Full protection across NIST



Better performance



Comprehensive Cyber Protection Platform

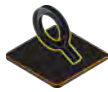
Cross-NIST Platform Powered by AI



Cyber Protect / Cloud platform



Endpoint
Detection
& Response



Incident
Investigation



Endpoint
Protection



Malware
Resistance



Email
Security



Ransomware
Protection



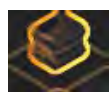
Continuous
Data
Protection



Disaster
Recovery



Data
Visibility



Data Loss
Prevention



Vulnerability
Assessment



Patch
Management



Remote
Access



Secure File
Sync and
Share

Security

Backup & DR

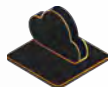
IT Management

Streamlined Administration

Partner Ecosystem



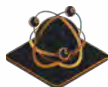
Managed Service
Providers



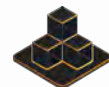
Cloud Service
Providers



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®

EDR from the Future

Let's Shape the Future of
Cybersecurity Together

Email: office@cy-napea.com

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

Website: www.cy-napea.com