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

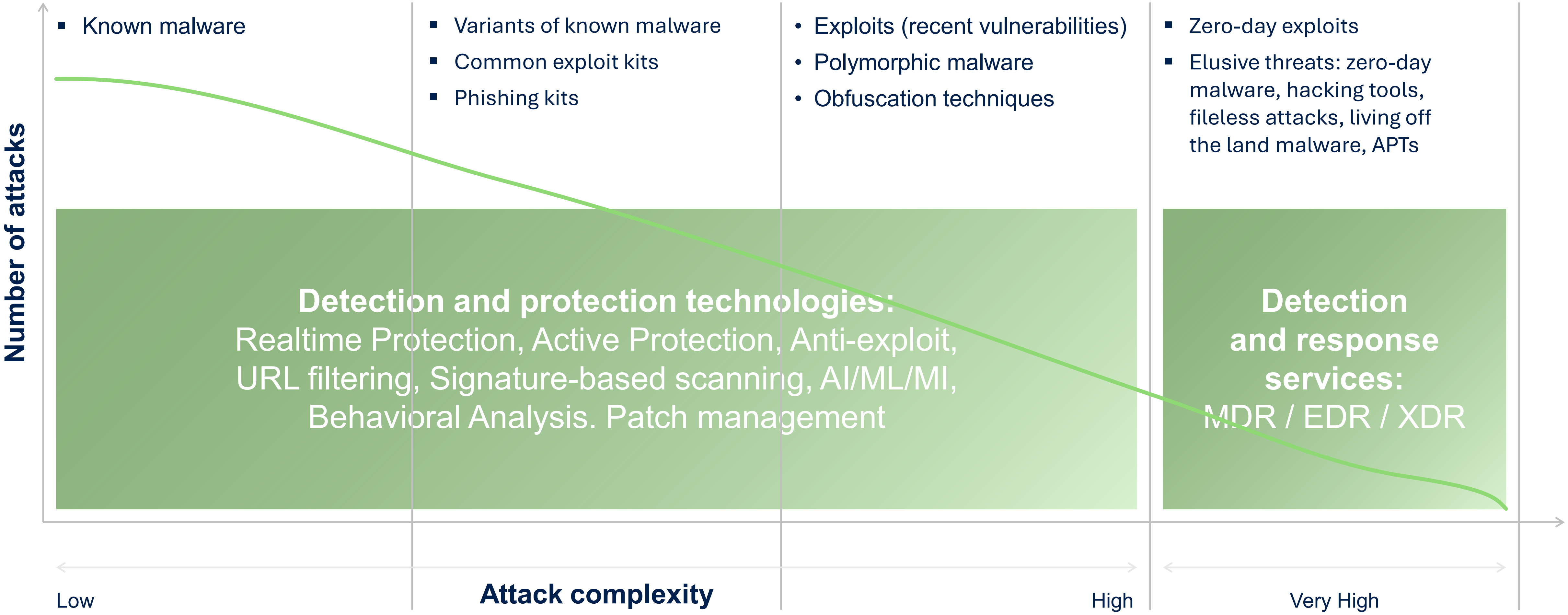
Sources: “Data Breach Investigations Report’, Verizon, 2022”; “Cost of data breach report”, 2022, IBM Security & Ponemon Institute; “Cyber Threats Report”, Cy-Napea®, 2022 “Costs and Consequences of Gaps in Vulnerability Response,” ServiceNow, 2020, Investigation or Exasperation? The State of Security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



- Known malware

- Variants of known malware
- Common exploit kits
- Phishing kits

- Exploits (recent vulnerabilities)
- Polymorphic malware
- Obfuscation techniques

- Zero-day exploits
- Elusive threats: zero-day malware, hacking tools, fileless attacks, living off the land malware, APTs

Detection and protection technologies:
Realtime Protection, Active Protection, Anti-exploit, URL filtering, Signature-based scanning, AI/ML/MI, Behavioral Analysis. Patch management

Detection and response services:
MDR / EDR / XDR

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

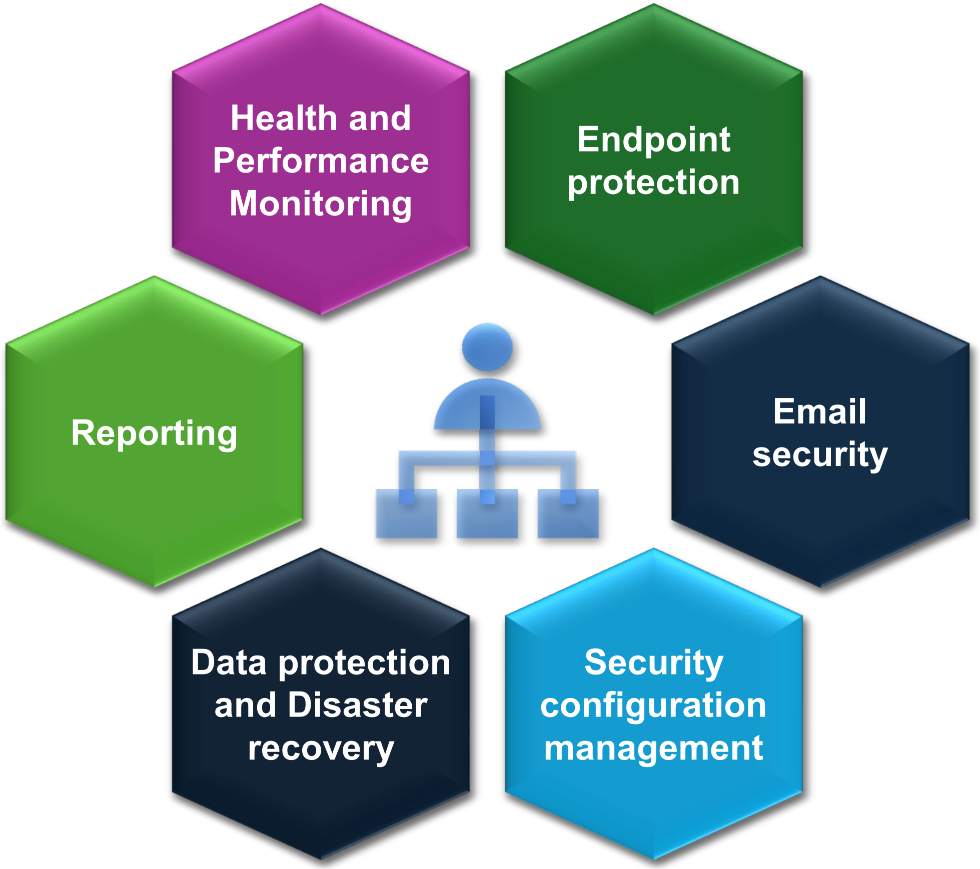
- Better protection with advanced capabilities
- Value-added management with pre-integration
- Skilled practitioners focused on protecting your business
- Service agility at the pace and cost you require

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


Health and Performance Monitoring
Endpoint protection
Reporting
Email security
Data protection and Disaster recovery
Security configuration management

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

Opportunity with MSP

Cost beyond IT budget

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

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

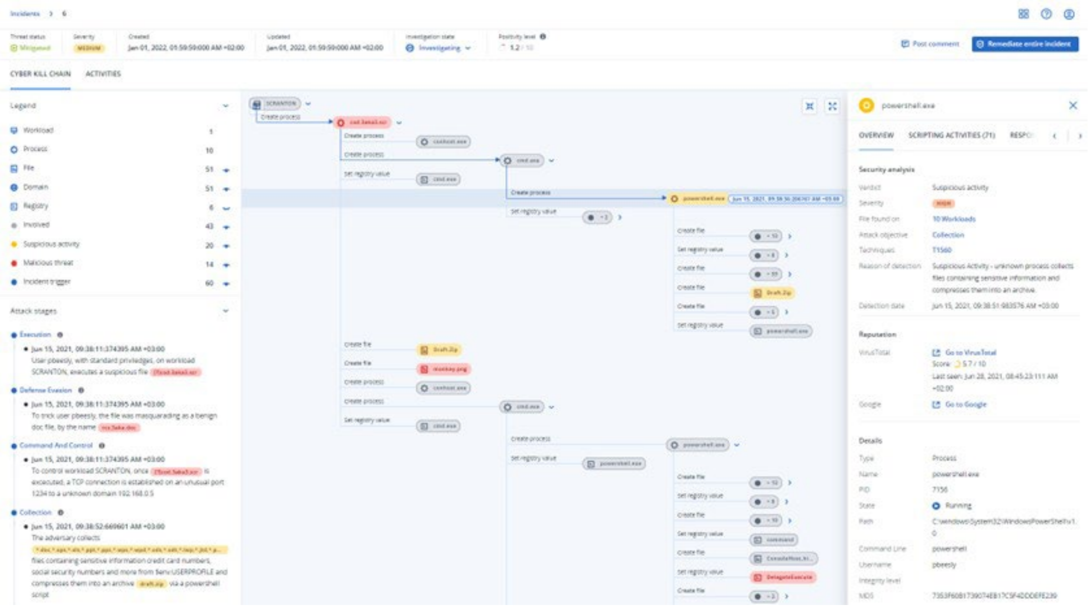
- **True business continuity** with pre-integrated recovery
- **Reduce impact** – quarantine processes, isolate workloads
- **Limit attack surface** for future protection

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



Incidents > 6

Threat status: Mitigated | Severity: MEDIUM | Created: Jan 01, 2022, 01:59:59:000 AM +02:00 | Updated: Jan 01, 2022, 01:59:59:000 AM +02:00 | Investigation state: Investigating | Positivity level: 1.2 / 10

Post comment | Remediate entire incident

CYBER KILL CHAIN | ACTIVITIES

Legend

Workload	1
Process	10
File	51
Domain	51
Registry	6
Involved	43
Suspicious activity	20
Malicious threat	14
Incident trigger	60

Attack stages

- Execution
  - Jun 15, 2021, 09:38:11:374395 AM +03:00
    User pbeesly, with standard priviledges, on workload SCRANTON, executes a suspicious file [illegible]
- Defense Evasion
  - Jun 15, 2021, 09:38:11:374395 AM +03:00
    To trick user pbeesly, the file was masquerading as a benign doc file, by the name [illegible]
- Command And Control
  - Jun 15, 2021, 09:38:11:374395 AM +03:00
    To control workload SCRANTON, once [illegible] is executed, a TCP connection is established on an unusual port 1234 to a unknown domain 192.168.0.5
- Collection
  - Jun 15, 2021, 09:38:52:669601 AM +03:00
    The adversary collects [illegible] files containing sensitive information credit card numbers, social security numbers and more from $env:USERPROFILE and compresses them into an archive draft.zip via a powershell script

powershell.exe

OVERVIEW | SCRIPTING ACTIVITIES (71) | RESPO...

Security analysis

Verdict	Suspicious activity
Severity	HIGH
File found on	10 Workloads
Attack objective	Collection
Techniques	T1560
Reason of detection	Suspicious Activity - unknown process collects files containing sensitive information and compresses them into an archive.
Detection date	Jun 15, 2021, 09:38:51:983576 AM +03:00

Reputation

VirusTotal	Go to VirusTotal Score: 5.7 / 10 Last seen: Jun 28, 2021, 08:45:23:111 AM +02:00
Google	Go to Google

Details

Type	Process
Name	powershell.exe
PID	7156
State	Running
Path	C:\windows\System32\WindowsPowerShell\v1.0
Command Line	powershell
Username	pbeesly
Integrity level	
MD5	7353F60B1739074EB17C5F4DDDEFE239

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

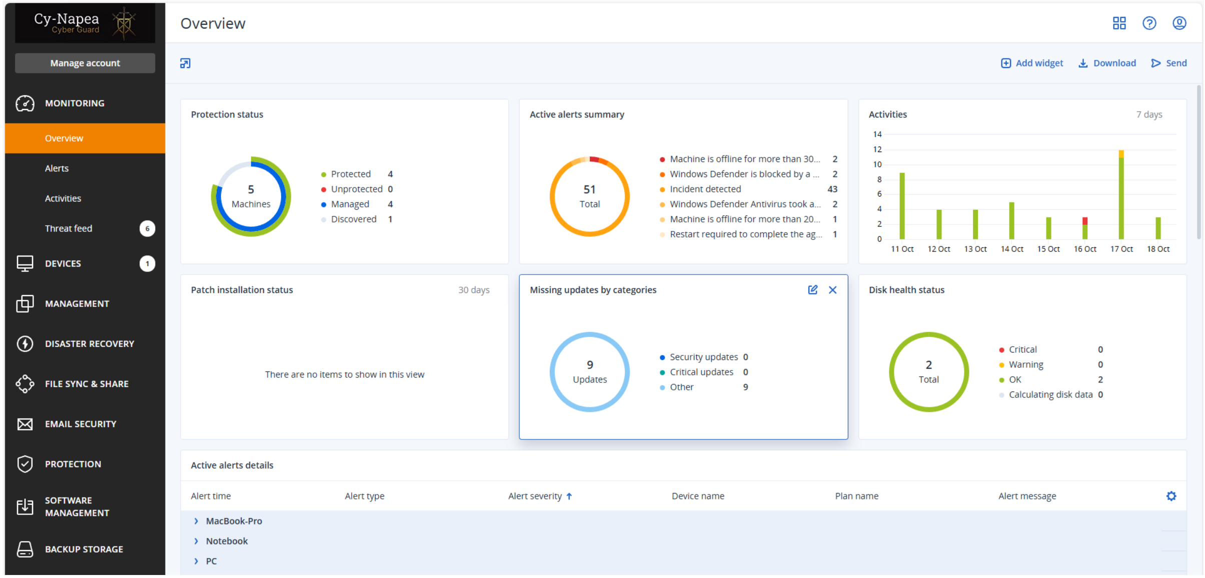
- How did the threat get in?
- How did it hide its tracks?
- What harm did it cause?
- How did it spread?

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



Protection status

● Protected	4
● Unprotected	0
● Managed	4
● Discovered	1

Active alerts summary

● Machine is offline for more than 30...	2
● Windows Defender is blocked by a ...	2
● Incident detected	43
● Windows Defender Antivirus took a...	2
● Machine is offline for more than 20...	1
● Restart required to complete the ag...	1

Activities 7 days

Patch installation status 30 days

There are no items to show in this view

Missing updates by categories

● Security updates	0
● Critical updates	0
● Other	9

Disk health status

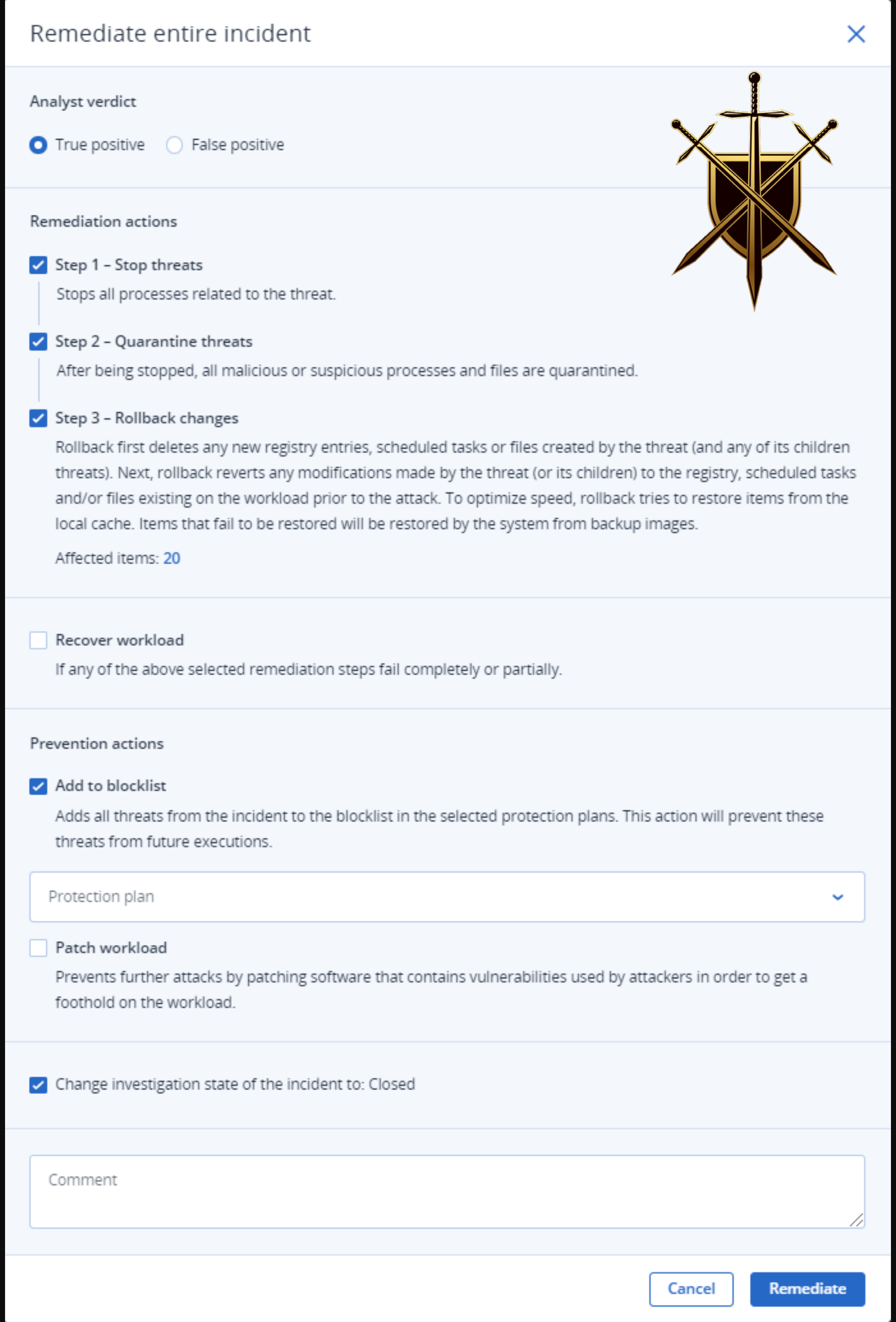
● Critical	0
● Warning	0
● OK	2
● Calculating disk data	0

Active alerts details

Alert time	Alert type	Alert severity ↑	Device name	Plan name	Alert message
› MacBook-Pro					
› Notebook					
› PC					

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 you business will always remain up and running with a rapid, more hollistic 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.

□ 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

Effective & Efficient

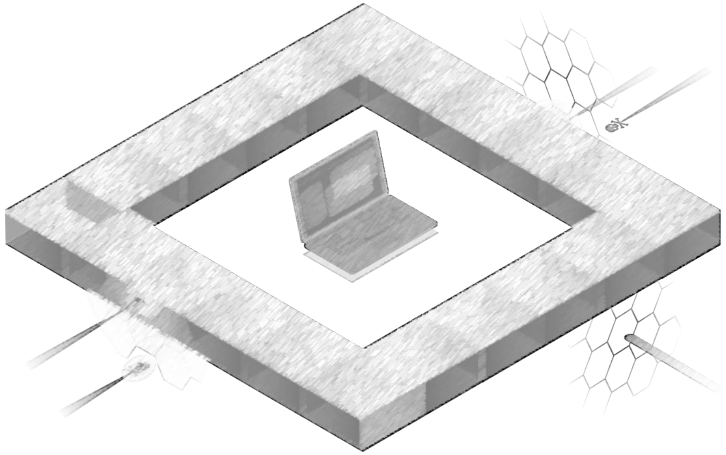
Stop most threats before they become breaches

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	▪ Hardware inventory ▪ Unprotected endpoint discovery	▪ Vulnerability assessments ▪ Exploit prevention ▪ Device control ▪ Security configuration management	▪ Emerging threats feed ▪ Search for IOCs of emerging threats ▪ Anti-malware & anti-ransomware ▪ AI/ML-based behavioral detection ▪ URL filtering	▪ Rapid incident analysis ▪ Workload remediation with isolation ▪ Forensic backups	▪ Rapid rollback of attacks ▪ One-click mass recovery ▪ Self-recovery
Cy-Napea® Cyber Protect Cloud	▪ Software inventory ▪ Data classification	▪ Patch management ▪ DLP ▪ Backup integration ▪ Cyber scripting	▪ Email security	▪ Investigation via remote connection	▪ 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

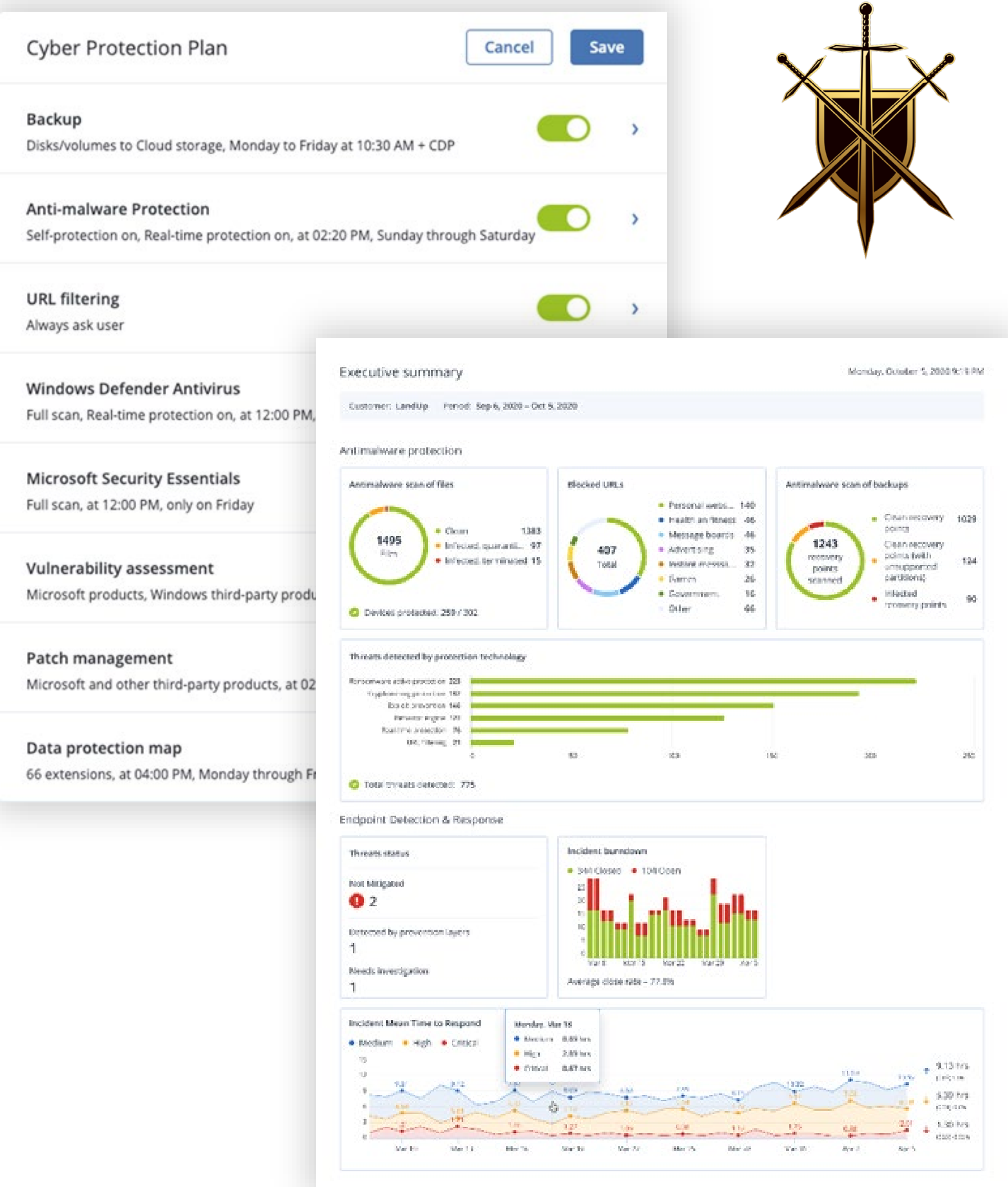
Succeed where point solutions fail. Unlock the full power of a platform with consolidated capabilities

- **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



Cyber Protection Plan

Cancel | Save

Backup
Disks/volumes to Cloud storage, Monday to Friday at 10:30 AM + CDP

Anti-malware Protection
Self-protection on, Real-time protection on, at 02:20 PM, Sunday through Saturday

URL filtering
Always ask user

Windows Defender Antivirus
Full scan, Real-time protection on, at 12:00 PM,

Microsoft Security Essentials
Full scan, at 12:00 PM, only on Friday

Vulnerability assessment
Microsoft products, Windows third-party produ

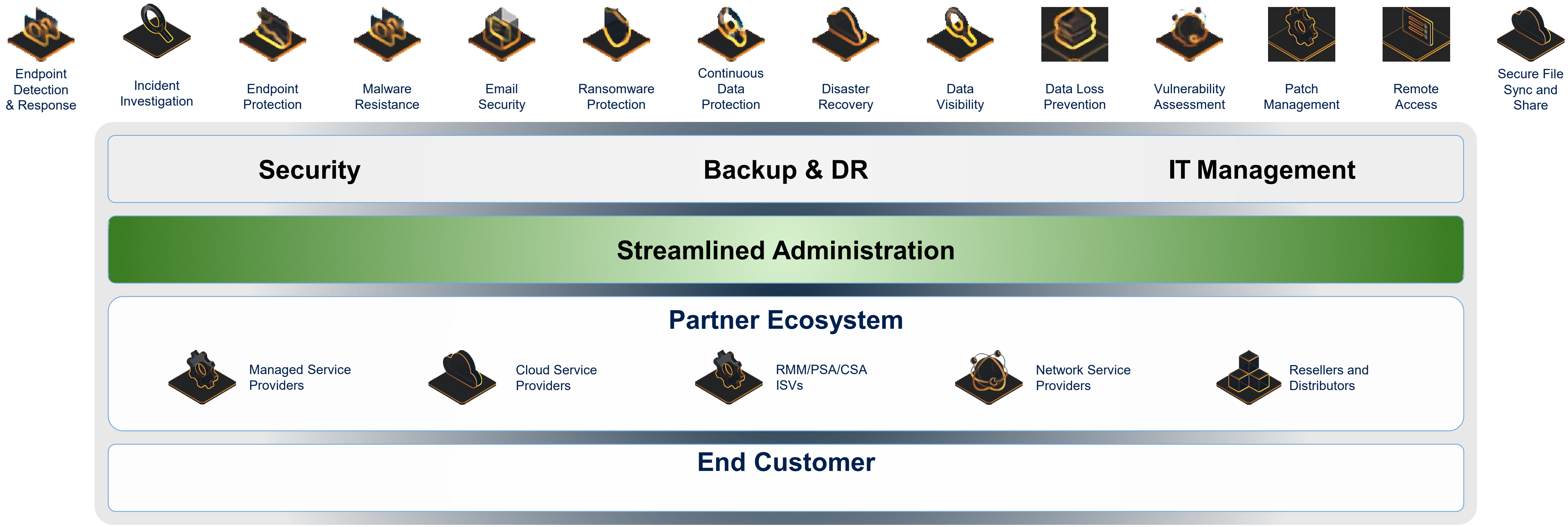
Patch management
Microsoft and other third-party products, at 02

Data protection map
66 extensions, at 04:00 PM, Monday through Fr

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