Cy-Napea®

XDR: Redefining Extended Detection and Response

Cy-Napea
Cyber Guard

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.

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

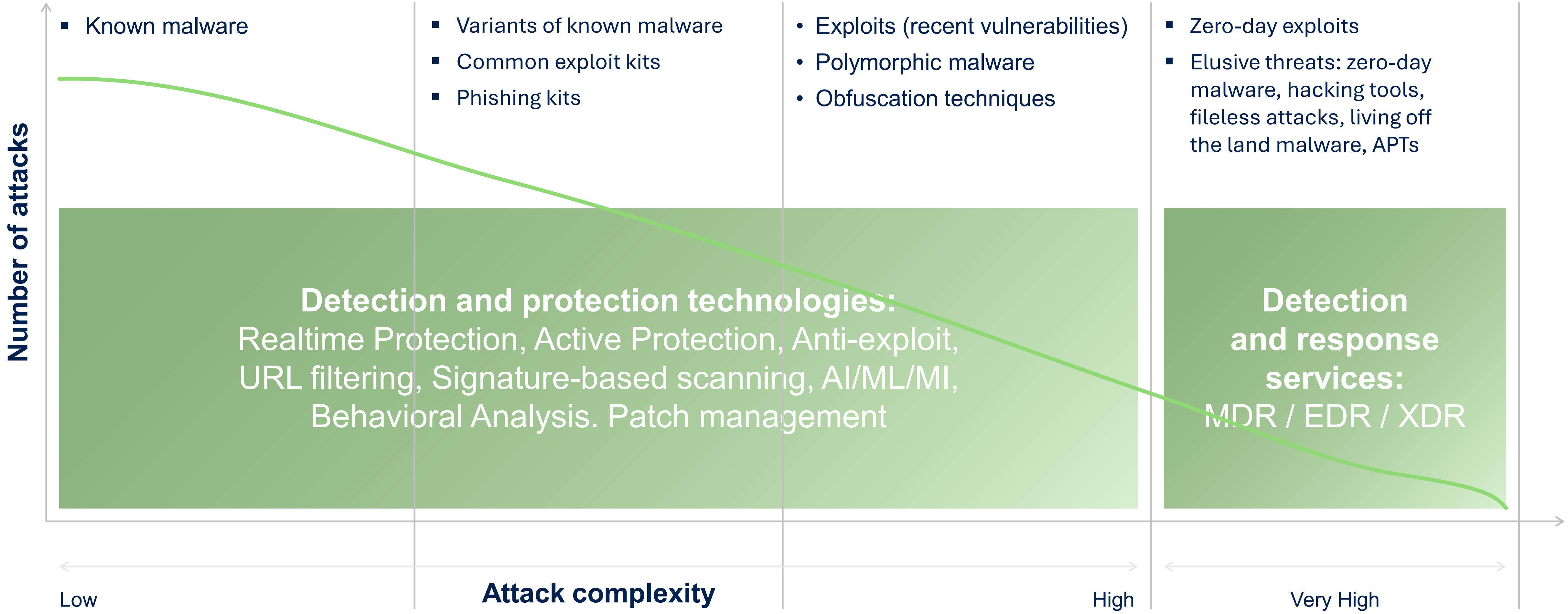
Sources: "Data Breach Investigations Report', Verizon, 2024; "Data Breach Investigations Report', Verizon, 2022"; "Cost of data breach report", 2022, IBM Security & Ponemon Institute; "Costs and Consequences of Gaps in Vulnerability Response," ServiceNow, 2020, Investigation or Exasperation? The State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



Number of attacks

- 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

Low

Attack complexity

High

Very High

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

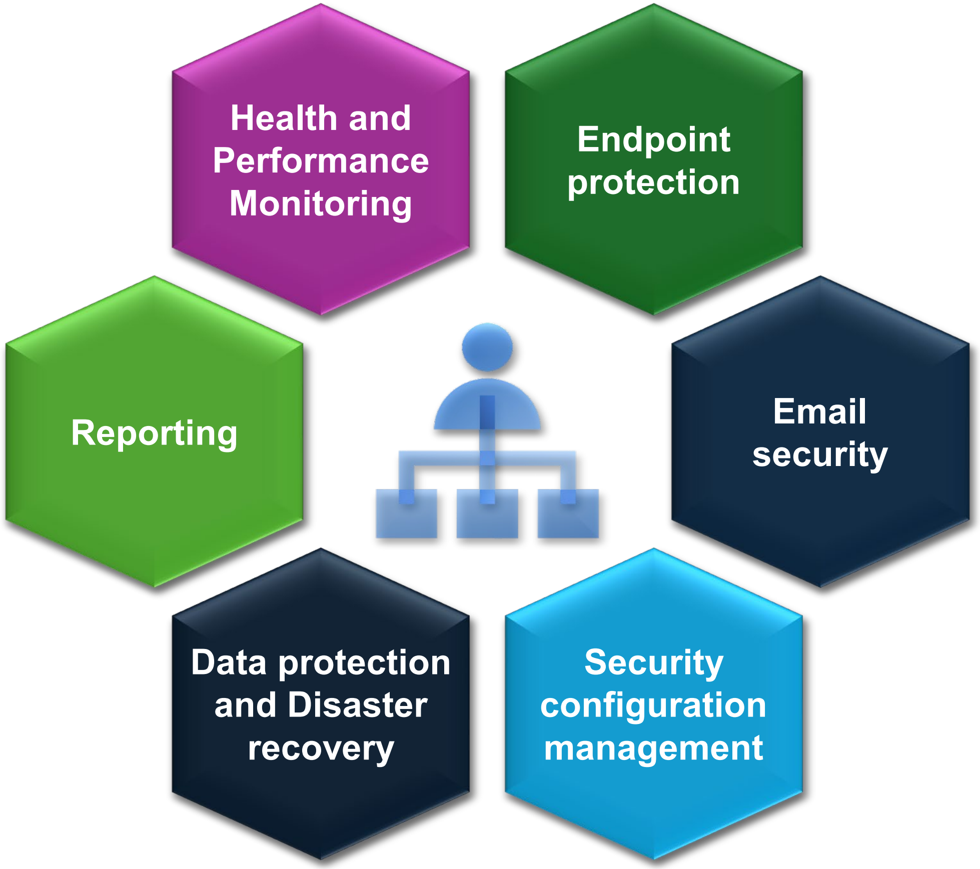
- Better protection with advanced capabilities
- Value-added management with pre-integration
- Skilled practitioners focused on protecting your business
- Service agility at the pace and cost you require

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 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.

Limitations	Cost & complexity	Limited business continuity and solution sprawl	Limited compliance and disaster recovery support
Cy-Napea opportunity	Effective and cost-efficient service for SMB and mid-market	Integrated across NIST – incl. remediation & recovery	Compliance and data protection with the ease you need

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

PERCEPTION POINT™

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

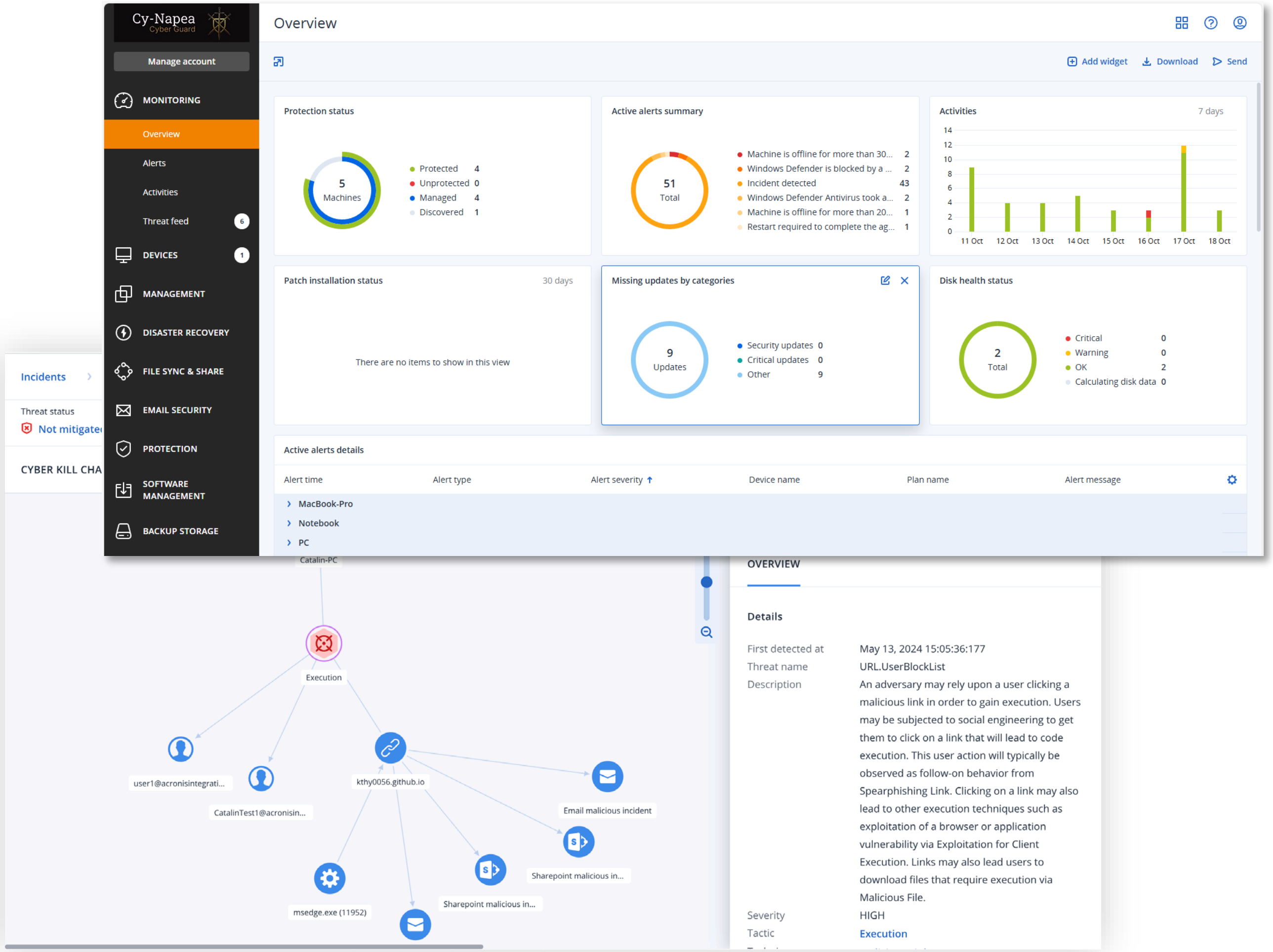
- How did the threat get in?
- How did it hide its tracks?
- What harm did it cause?
- How did it spread?

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



Protection status

5 Machines

Protected	4
Unprotected	0
Managed	4
Discovered	1

Active alerts summary

51 Total

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

Patch installation status 30 days

There are no items to show in this view

Missing updates by categories

9 Updates

Security updates	0
Critical updates	0
Other	9

Disk health status

2 Total

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					

Threat status

Not mitigate

Details

First detected at May 13, 2024 15:05:36:177

Threat name URL.UserBlockList

Description An adversary may rely upon a user clicking a malicious link in order to gain execution. Users may be subjected to social engineering to get them to click on a link that will lead to code execution. This user action will typically be observed as follow-on behavior from Spearphishing Link. Clicking on a link may also lead to other execution techniques such as exploitation of a browser or application vulnerability via Exploitation for Client Execution. Links may also lead users to download files that require execution via Malicious File.

Severity HIGH

Tactic Execution

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

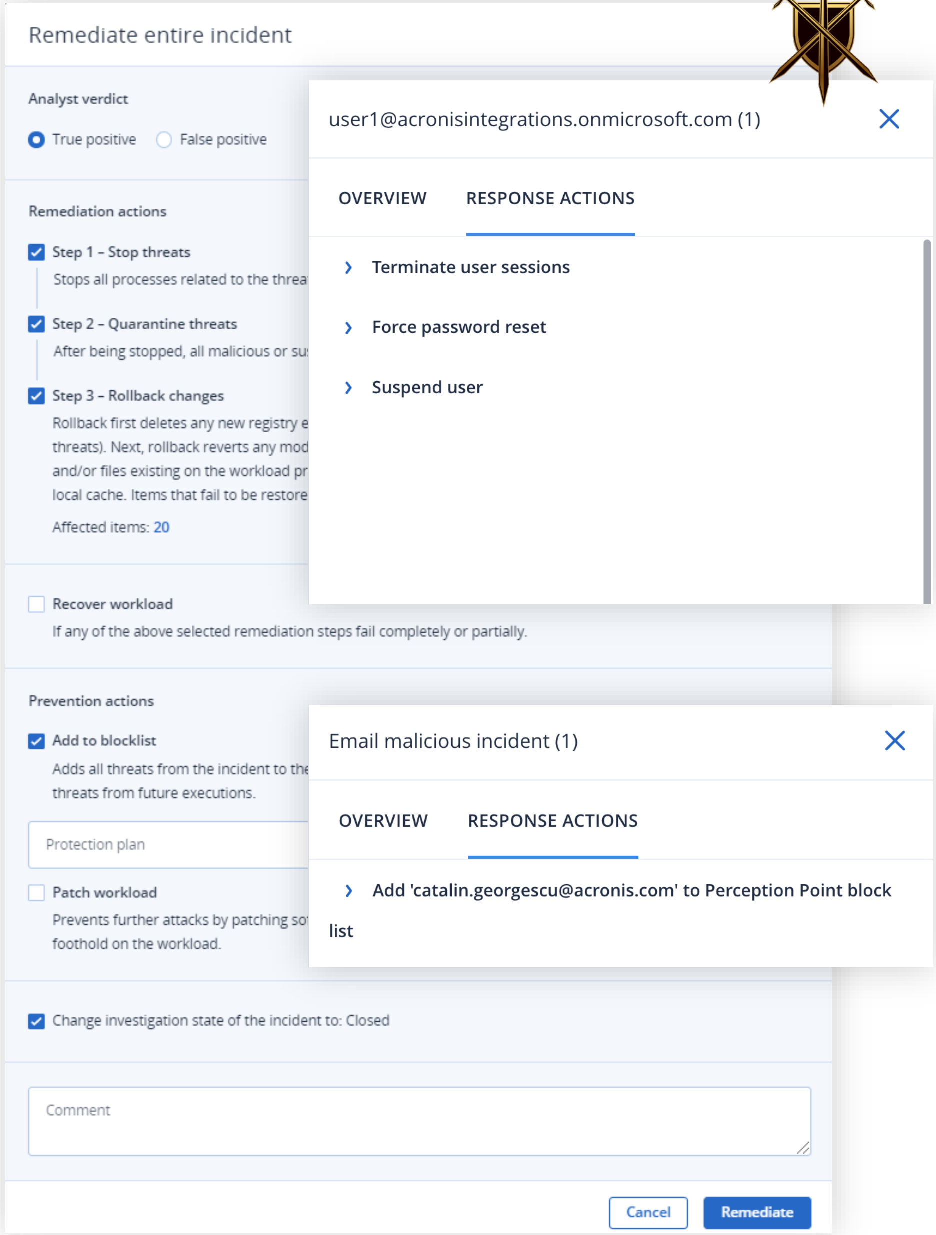
Contain threats – isolation, user session termination

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



Remediate entire incident

Analyst verdict

● True positive ○ False positive

Remediation actions

☑ Step 1 – Stop threats

Stops all processes related to the threa

☑ Step 2 – Quarantine threats

After being stopped, all malicious or su

☑ Step 3 – Rollback changes

Rollback first deletes any new registry e threats). Next, rollback reverts any mod and/or files existing on the workload pr local cache. Items that fail to be restore

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 threats from future executions.

Protection plan

□ Patch workload

Prevents further attacks by patching so foothold on the workload.

☑ Change investigation state of the incident to: Closed

Comment

user1@acronisintegrations.onmicrosoft.com (1)

› Terminate user sessions

› Force password reset

› Suspend user

Email malicious incident (1)

› Add 'catalin.georgescu@acronis.com' to Perception Point block list

Effective & Efficient

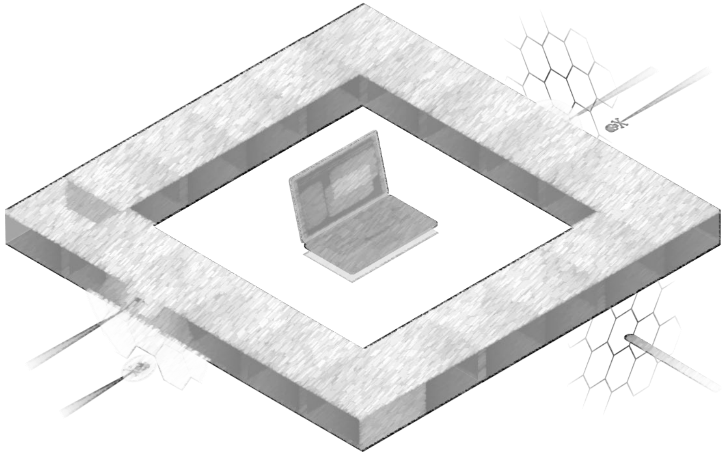
Stop most threats before they become breaches

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	▪ Centralized policy management ▪ Role-based management ▪ Information-rich dashboard ▪ Schedulable reporting	▪ Software & Hardware inventory ▪ Unprotected endpoint discovery	▪ Vulnerability assessments ▪ Device control ▪ Security configuration management	▪ Threat telemetry across endpoints, identity, email, M365 apps ▪ AI/ML-based behavioral detection & anti-ransomware ▪ Exploit prevention & URL filtering ▪ Threat hurting	▪ AI-based incident prioritization ▪ Ai-guided analysis ▪ Remediation and isolation ▪ Forensic backups	▪ Rapid rollback of attacks ▪ One-click mass recovery ▪ Self-recovery
Cy-Napea Cyber Protect Cloud	▪ Provisioning via a single agent and platform	▪ Software inventory ▪ Data classification	▪ Patch management ▪ DLP ▪ Backup integration ▪ Cyber scripting	▪ Email security	▪ Investigation via remote connection	▪ 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

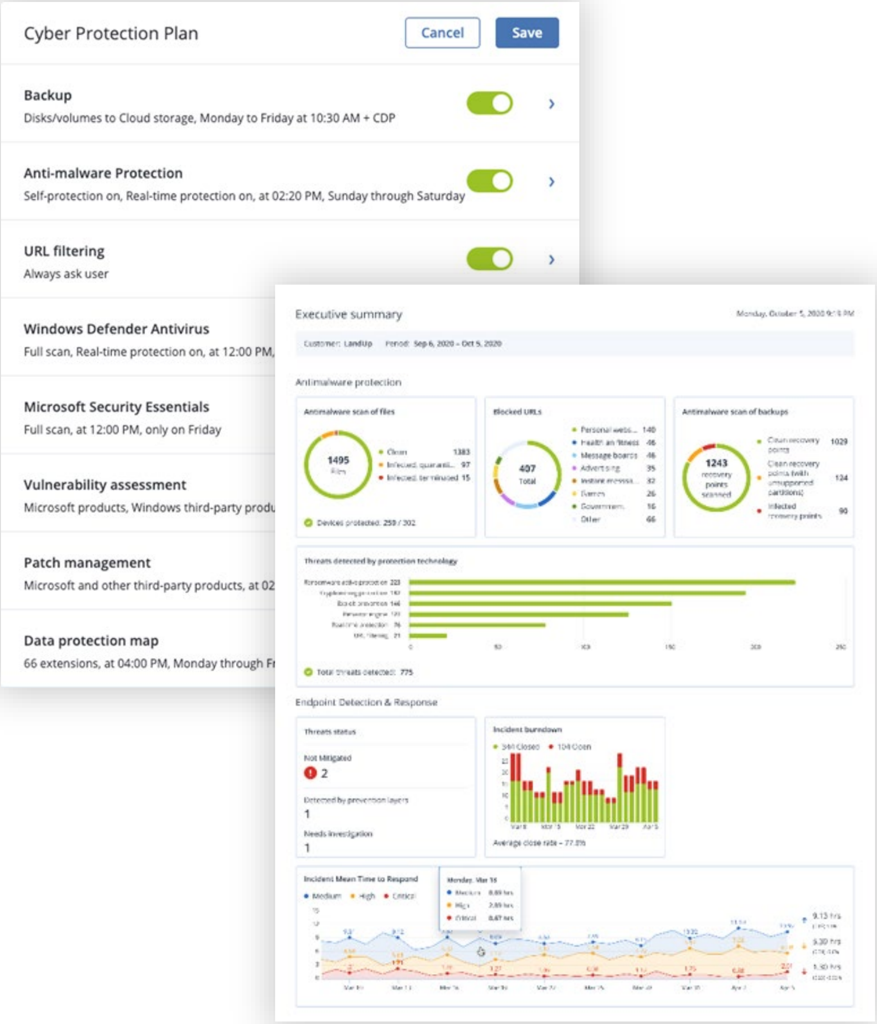
Succeed where point solutions fail. Unlock the full power of a platform with consolidated capabilities

- **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



Cyber Protection Plan

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

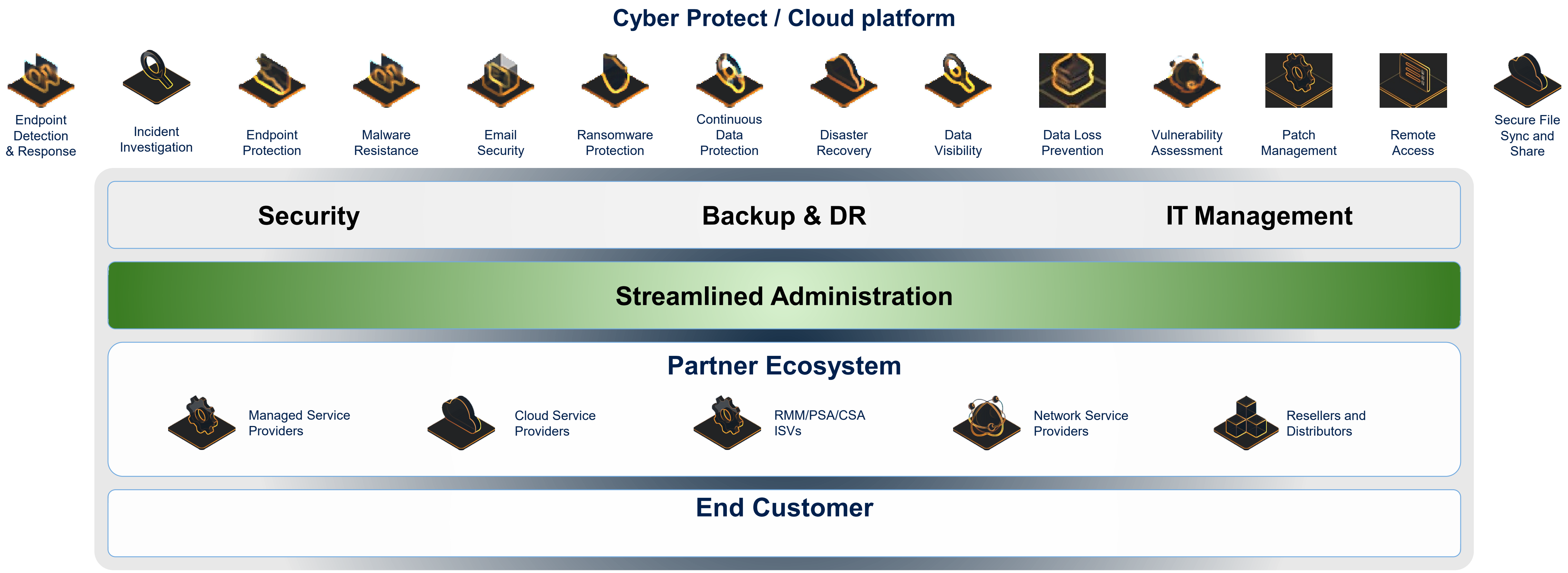
Executive summary

Monday, October 5, 2020

Customer: LandUp Period: Sep 6, 2020 – Oct 5, 2020

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