IT NATION™ SECURE

hosted by CONNECTWISE

Acronis

MSPs on the Edge: Advanced Security with EDR

June 7, 2023

Dimitri Korahais

Senior Solutions Engineer

Justin Ceballos

Strategic Partner Executive

#CyberFit

The new world of threats

Natural disasters

- Only 6% of outages are caused by natural disasters(1)
- Affects facilities and infrastructure

Pandemics

- Requires a different kind of planning scenario
- Affects people

Hardware failure, software corruption

Up to 30M SMBs are vulnerable to IT failure without comprehensive monitoring(2)

Accidental data deletion

14% of data loss is caused by human error, such as deleting or overwriting files(3)

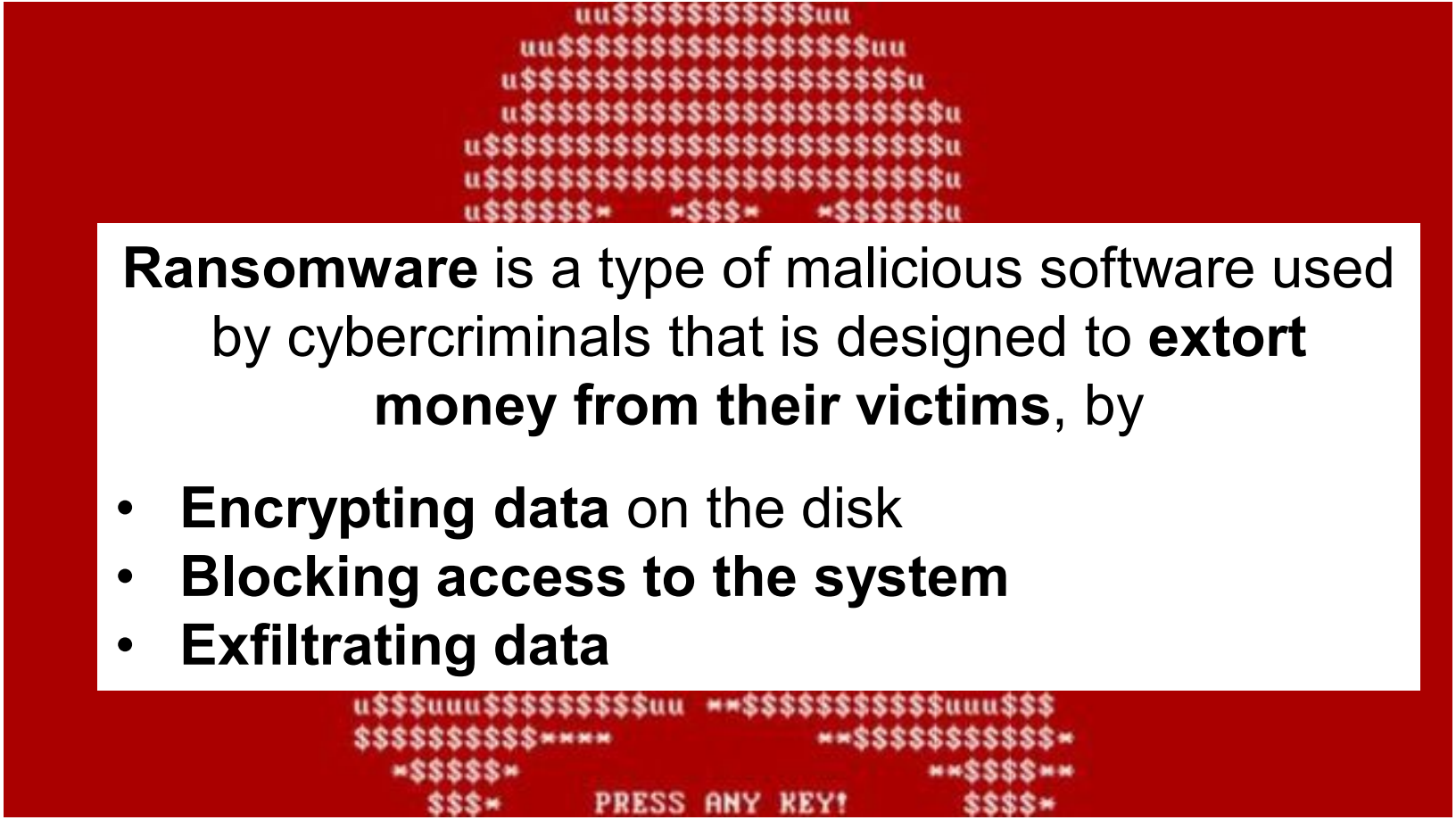
Cyberattacks

- 93% of businesses were attacked within the past three years(2)
- Malware attacks increased by 25% in 2019(4)
- By 2021 cybercrimes will cost $6 trillion per year(4)

Natural

Human

(1) Actual Tech Media, (2) IDC, (3) Tech Radar, (4) Symantec 2019 ISTR



Ransomware is a type of malicious software used by cybercriminals that is designed to **extort money from their victims**, by

- **Encrypting data** on the disk
- **Blocking access to the system**
- **Exfiltrating data**

The threat landscape is becoming more complex

80%

of companies reported to have been attacked in H2, 2021

57%

of attacks are missed by traditional antivirus solutions

69%

of MSPs spend more time managing tools than defending against threats

Sources: Acronis Cyberthreats Report 2022, Acronis Cyber Readiness Report, 2020, FBI

What if you could rely on just one integrated solution?

Cut
cyber protection costs by up to 50%

Boost
your monthly recurring revenue

Deliver
unmatched cyber protection

Advanced Security – Quick Overview

A complete endpoint security solution to protect various types of workloads, based on a combination of classic signature-based engine as well as next-gen set of modern technologies

Full-stack endpoint security

Acronis Active Protection (Anti-ransomware), enhanced with exploit prevention, URL filtering, anti-malware detection for backed-up data, and improved detection rate to catch more threats faster

Security automation and management

Smart protection plans, auto-allow list custom apps, automatic malware scans, and AV definitions updates as part of the recovery process help deliver services effortlessly

Integrated with backup & DR

Immediate data recovery in case of ransomware attack as well as backup capabilities within forensic data brings unique value-added functionality and fastest time-to-recovery

What is EDR?

EDR (Endpoint Detection and Response)
is an event correlation security platform, capable of identifying **advanced threats or in-progress attacks** – and then doing something about it.

Gartner - Primary EDR capabilities:

- Detect security incidents
- Contain the incident at the endpoint
- Investigate security incidents
- Provide remediation guidance

The need for EDR

Only advanced security can combat advanced attacks

More than 60% of breaches **involve some form of hacking**

On average, it takes organizations **207 days to** identify a breach

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

76% of security and IT teams struggle with **no common view** over applications and assets

For many – compliance is mandatory

Regulations require organizations to **report security incidents** within a strict time-frame – e.g. 72 hours for GDPR

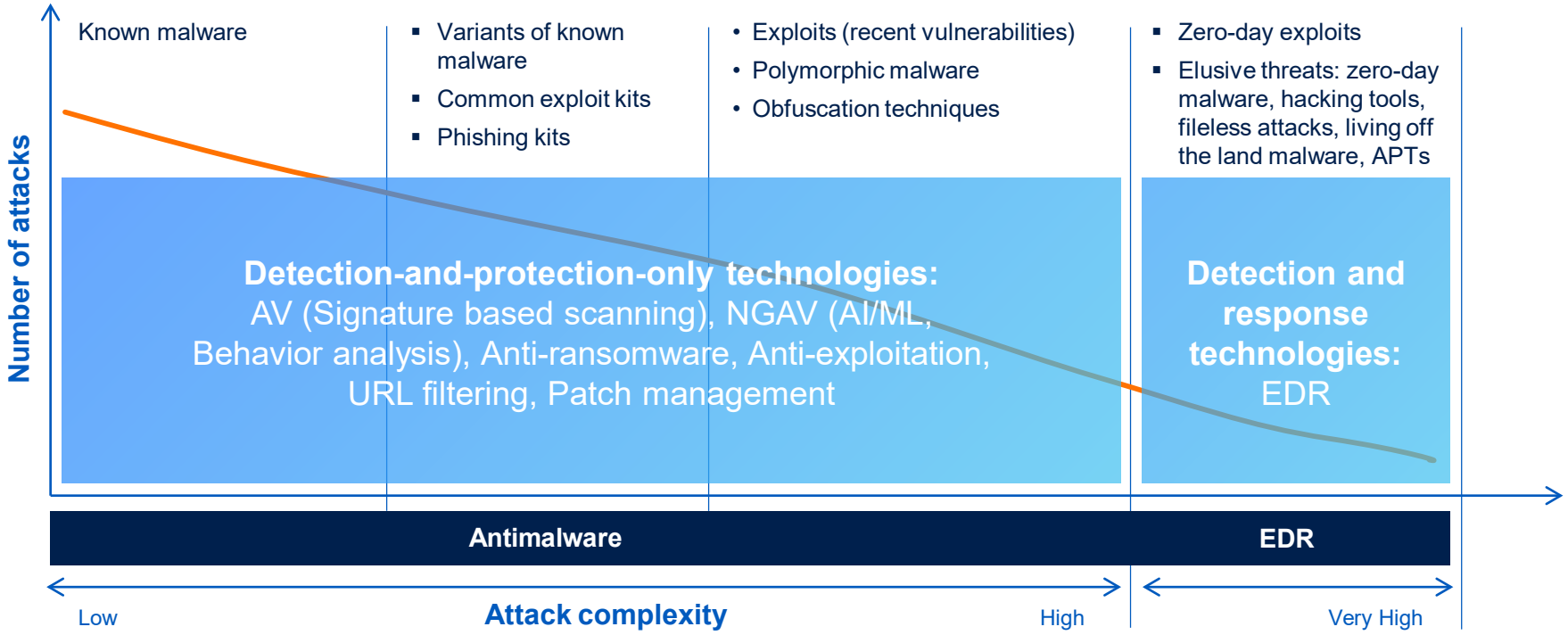
70% of breaches involve PII (post-incident analysis required for reporting for regulatory purposes)

Sources: "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

Comparing Antimalware vs EDR

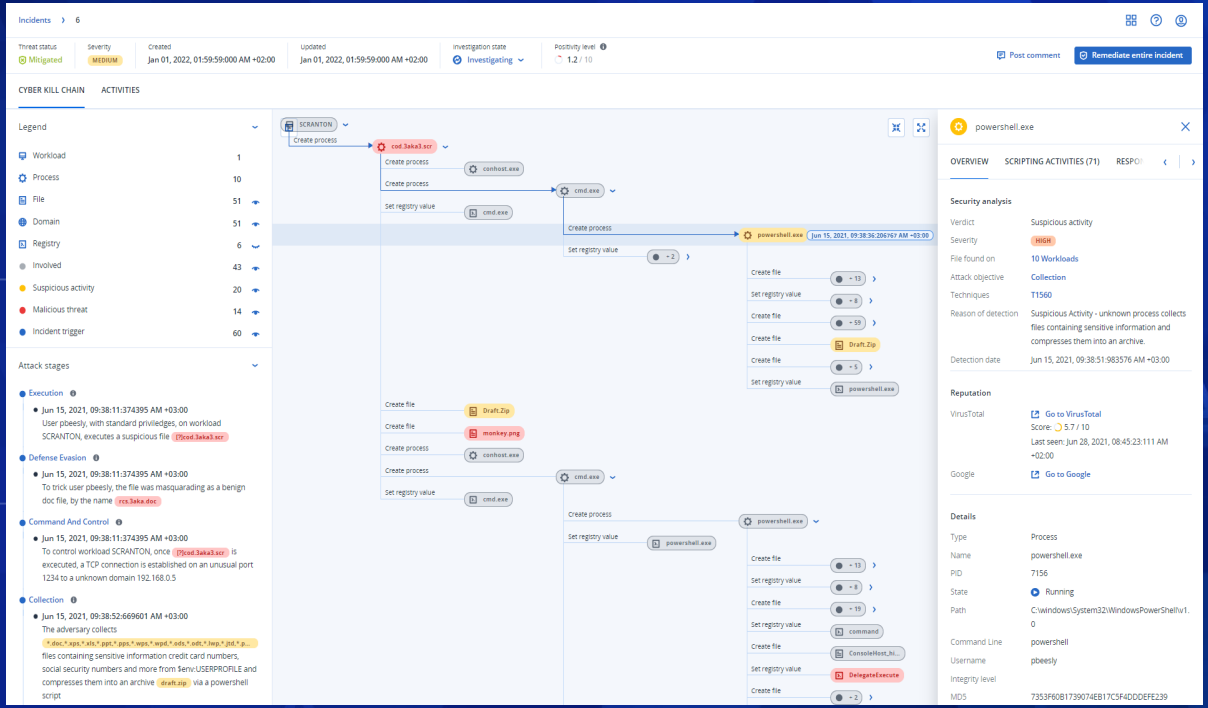
Category	Antimalware	EDR
Focus	Block/prevent attack	Post-incident detection and response
Detection Technology	Detects and stops **"known bad"** files, processes or behaviors	Detects **"intent"** by *correlating a series of actions* an attacker performs to be successful at achieving its objective
Visibility into attacks	Low Shows only detected and blocked threats.	High – broader scope of incidents Maps steps of the attack to show: • How did it get in? • How did it hide its tracks? • What did it harm? • How did it spread?
Response capabilities	Automatically blocks "known bad" processes and quarantines threats	Provides response capabilities to: • Contain the incident at the endpoint • Investigate security incidents • Provide remediation

How EDR helps to protect against threats

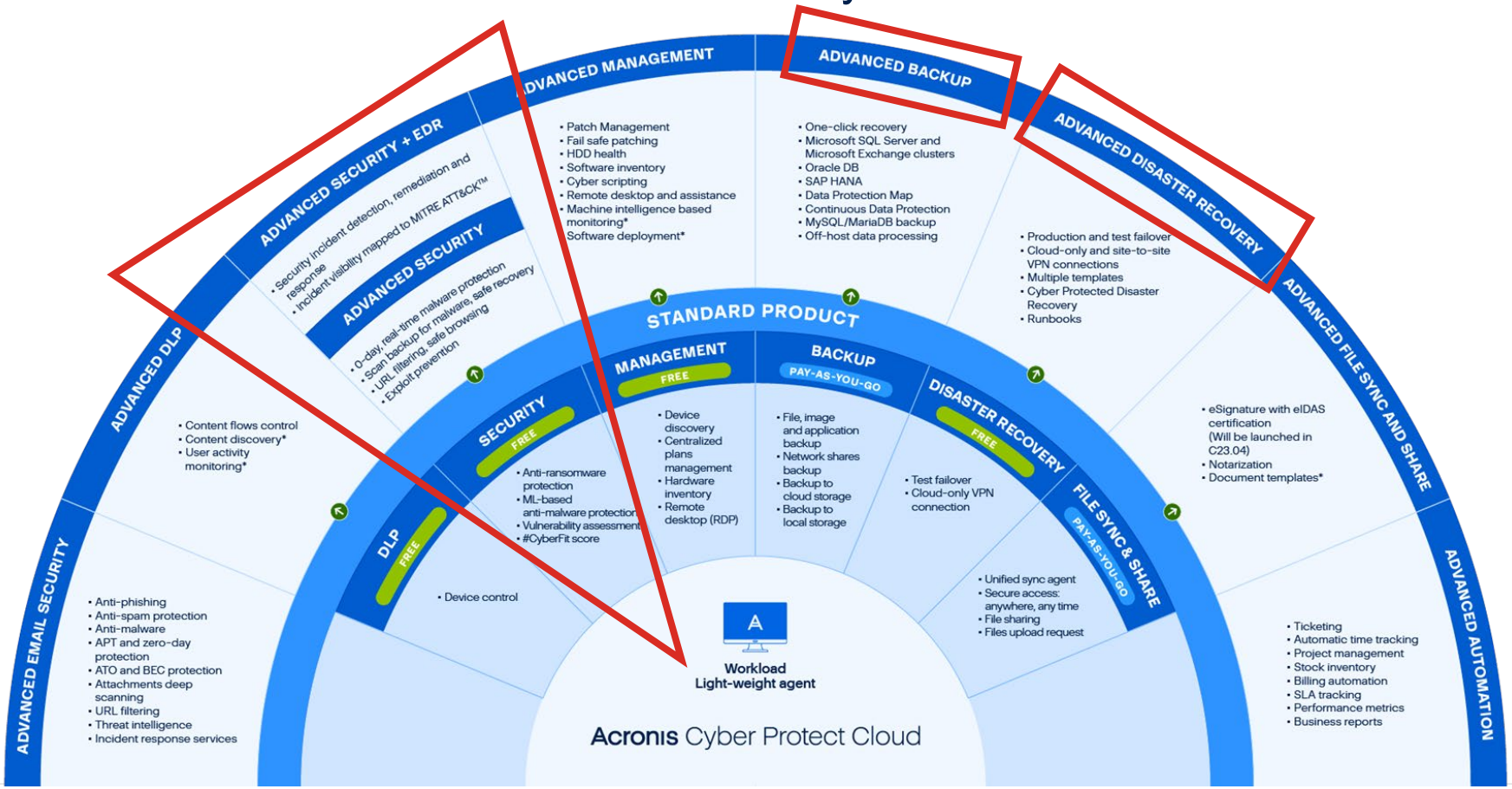


Acronis Advanced Security + EDR Functionality

1. **Rapid attack prioritization and analysis**
2. **Integrated remediation options**
3. **Unified scalable platform**



EDR as Part of Acronis Cyber Protect Cloud



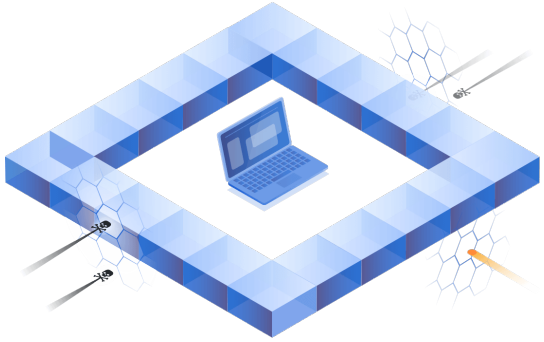
Builds on functionalities of Advanced Security

Next-generation anti-malware: 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 Acronis Cyber Protection Operations Centers



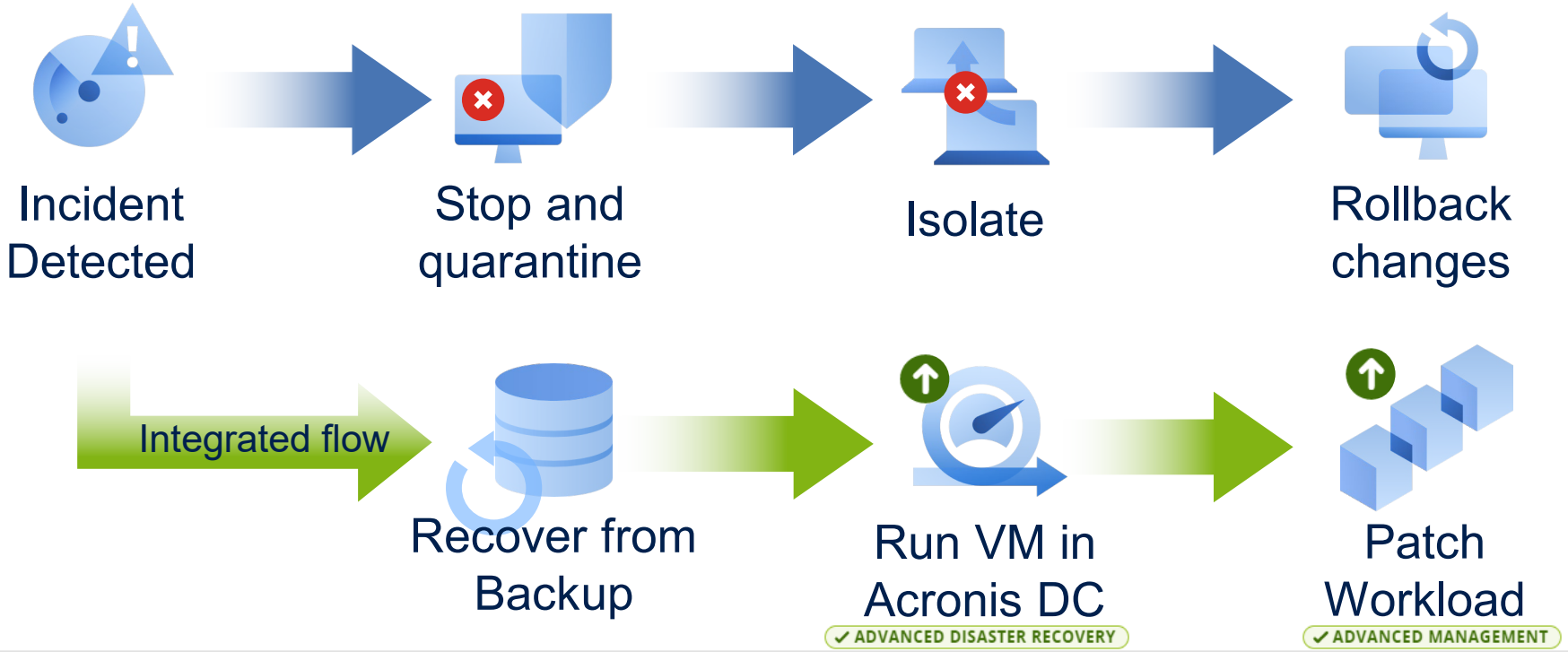
Forensic backup: Enable forensic investigations by collecting digital evidence in image-based backups

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

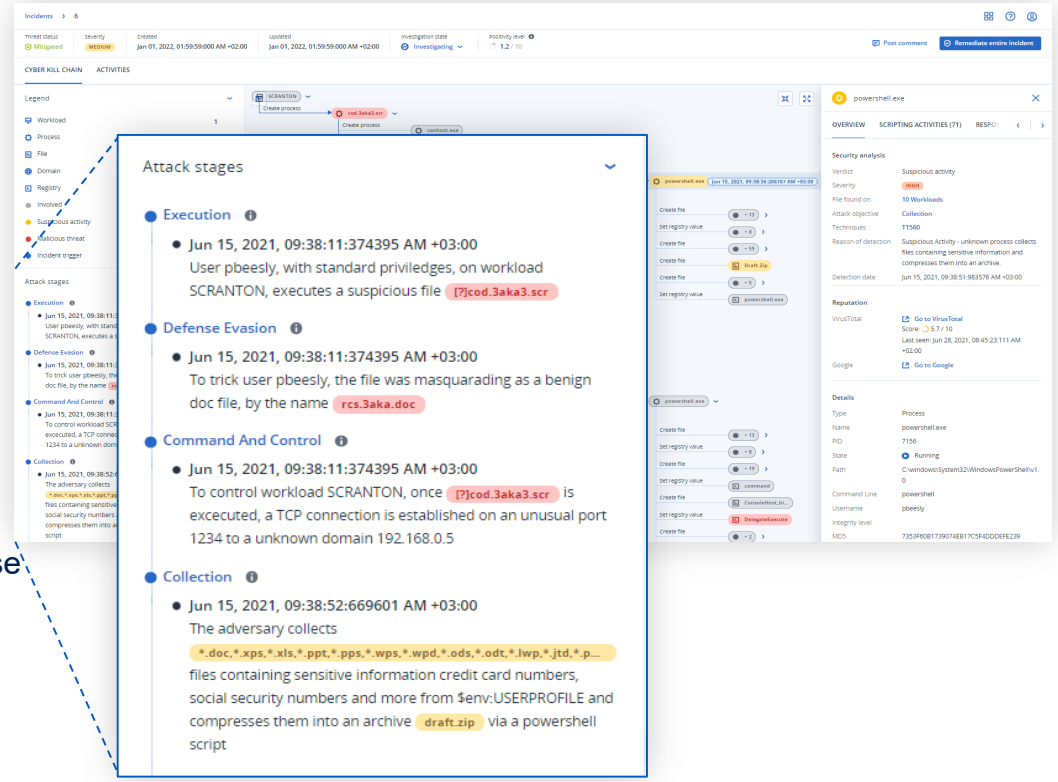
Respond & Remediate
Take advantage of Integrated flow



Analyze attacks in minutes

Analyze attacks with ease and speed:

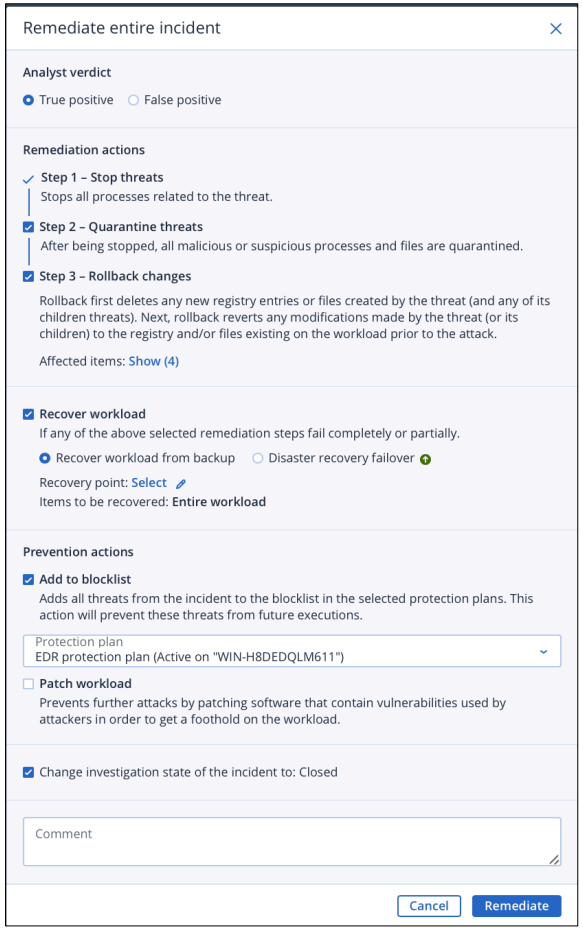
- **Prioritized visibility of suspicious activities** across endpoints – not a flat list of all alerts
- **Visibility into the attack chain evolution –** mapped to the MITRE framework
  - How did it get in?
  - How did it hide its tracks?
  - How did it cause harm?
  - How did it spread?
- **Save money and time**
  Reduce need for specialized training and expertise



Stop the breach

- Investigate further using remote connection and forensic backup
- Contain threats: Isolate the machine from the network
- Remediate: Kill malware processes, quarantine threats, and roll back changes.
- Prevent recurrence: Apply matches and block analyzed threats from execution
- Ensure business continuity: Use integrated recovery capabilities, including attack-specific rollback, file- or image-level recovery, and disaster recovery

Select actions and take action with a single click.



Acronis EDR demo

Advanced Security + EDR: Top 4 use cases

Detect and block attack before breach

- **Monitor and correlate events** on endpoints
- **Block common threats** with award-winning endpoint protection
- **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

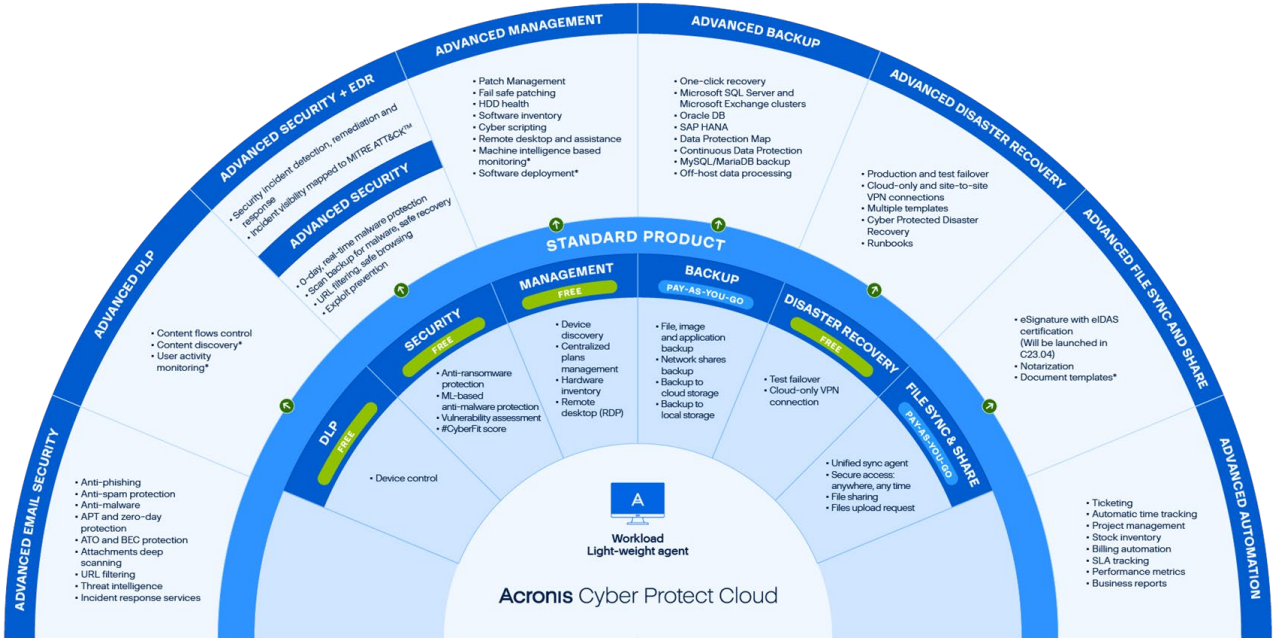
Enable compliance and cyber insurance

- **Report on incidents across endpoints** based on MITRE ATT&CK®
- **Classify sensitive data**
- **Collect forensic data** in backups

Consolidate solutions

- **Rapidly launch & scale through** an MSP-class platform
- **Reduce costs with** unified service management

Best-in-breed backup combined with integrated security and management



Optimize for every workload **Rapidly launch services** **Consolidate vendors**

Q&A

Visit Acronis Booth 504 for an in-depth demo!

Acronis
Cyber Foundation

Building a more knowledgeable future

#CyberFit

Create, spread and protect knowledge with us!

- Building new schools
- Providing educational programs
- Publishing books

www.acronis.org

Don't forget to fill out your

SESSION SURVEY