Acronis | intel

20
Years
of innovation
Acronis

VIRTUAL CONFERENCE FOR MSPs

Cyberstock:
Ransomware, EDR and the MSP opportunity

- The conference is being recorded
- We will email you a link to the recording afterwards
- Please submit your questions through the Zoom Q&A interface

#CyberFit

Jeff Hardy

Solutions Marketing Manager
Acronis

Agenda

▪ Welcome to our webinar!	**Jeff Hardy**, Solutions Marketing Manager, Acronis
▪ **Welcome greetings**	**Patrick Pulvermueller,** CEO**,** Acronis
▪ **Bad Robot: Ransomware in the age of AI and what you need to stop it**	**Candid Wuest**, VP of Research, Acronis
▪ **The Hardware / Software Alliance: Why MSPs should care**	**Jeff Hardy**, Acronis **Todd Cramer**, Director Security Ecosystem Business Development, Intel
▪ **MSPs on the Edge: Advanced Security with EDR**	**James Erby**, Solutions Engineer, Acronis
▪ **EDR case study discussion**	**Jeff Hardy**, Acronis **Brian Harvey**, Network Operations Manager, Business World
▪ **Live audience Q&A**	
▪ **Wrap-up**	**Jeff Hardy**, Acronis

Welcome greetings

Patrick Pulvermueller

CEO
Acronis

#CyberFit

Agenda

▪ Welcome to our webinar!	**Jeff Hardy**, Solutions Marketing Manager, Acronis
▪ Welcome greetings	**Patrick Pulvermueller,** CEO, Acronis
▪ **Bad Robot: Ransomware in the age of AI and what you need to stop it**	**Candid Wuest**, VP of Research, Acronis
▪ **The Hardware / Software Alliance: Why MSPs should care**	**Jeff Hardy**, Acronis **Todd Cramer**, Director Security Ecosystem Business Development, Intel
▪ **MSPs on the Edge: Advanced Security with EDR**	**James Erby**, Solutions Engineer, Acronis
▪ **EDR case study discussion**	**Jeff Hardy**, Acronis **Brian Harvey**, Network Operations Manager, Business World
▪ **Live audience Q&A**	
▪ **Wrap-up**	**Jeff Hardy**, Acronis

Bad Robot –

How MSPs fight ransomware in the age of AI

#CyberFit

Candid Wuest

VP of Research
Acronis

Malware growth

270,000

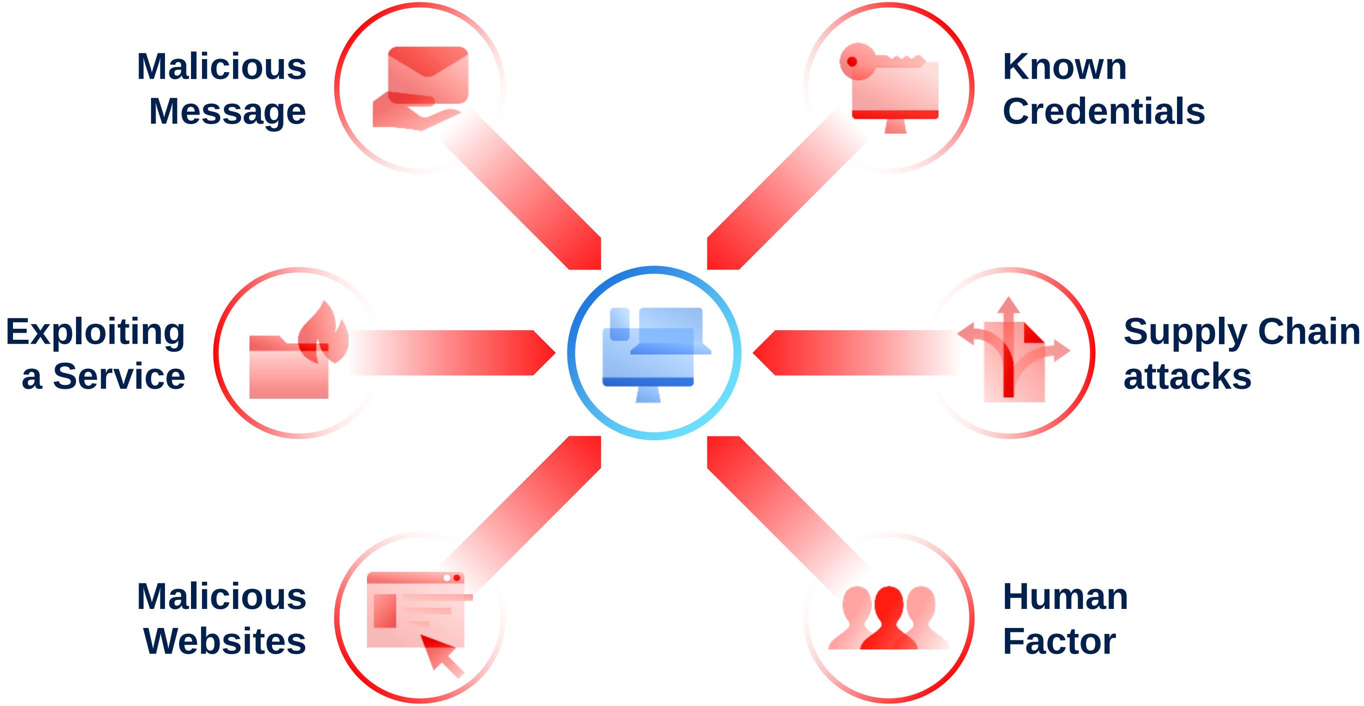
new malware samples per day in 2023

1.7 days

average lifetime of malware

Attack Vectors

Compromise the target and get a foot in the door



Malicious Message

Known Credentials

Exploiting a Service

Supply Chain attacks

Malicious Websites

Human Factor

They are in… now what?

Expand their access and achieve their goal

Initial Access Malware

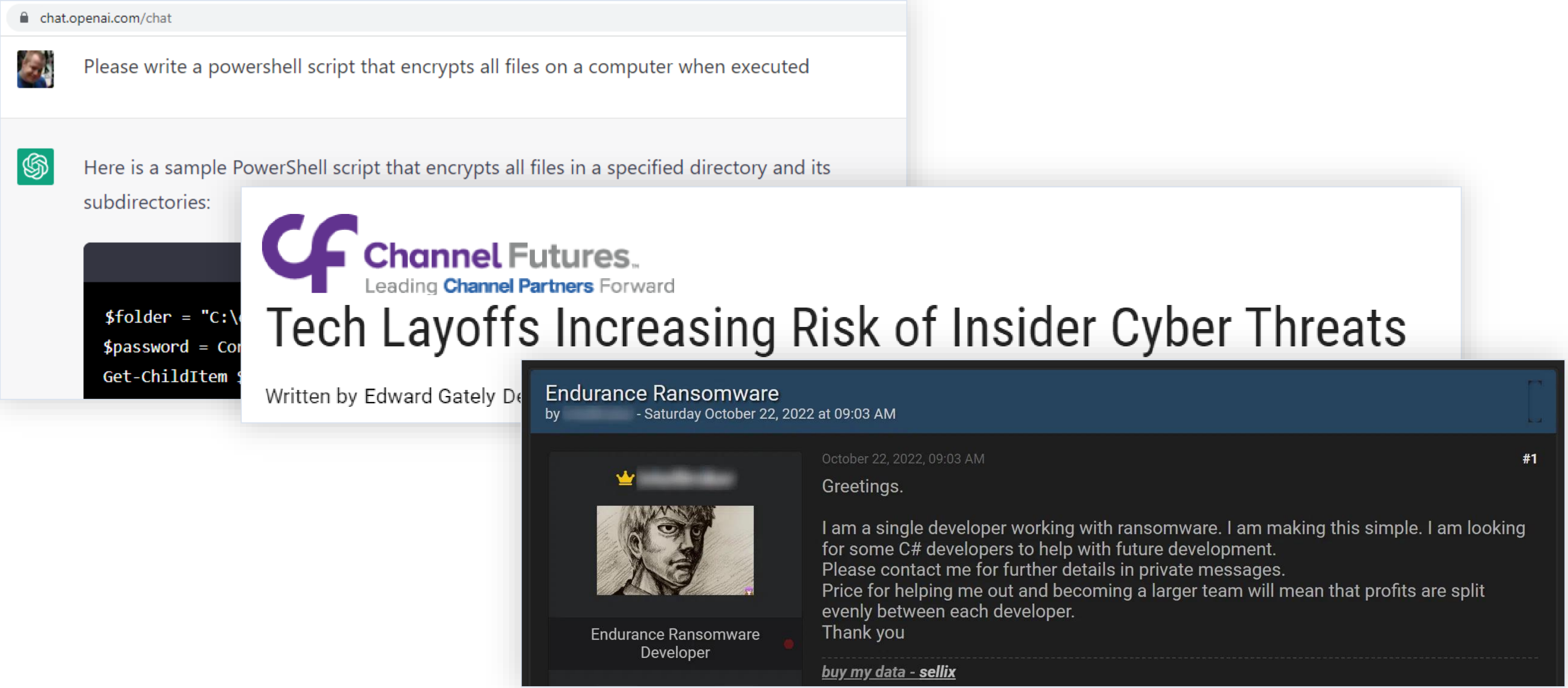
Discover Environment

Privilege Escalation

Defense Evasion

Lateral Movement

The Number of “Players” is growing



chat.openai.com/chat

Please write a powershell script that encrypts all files on a computer when executed

Here is a sample PowerShell script that encrypts all files in a specified directory and its subdirectories:

```
$folder = "C:\
$password = Co
Get-ChildItem $
```

Channel Futures

Leading Channel Partners Forward

Tech Layoffs Increasing Risk of Insider Cyber Threats

Written by Edward Gately De

Endurance Ransomware

by [redacted] - Saturday October 22, 2022 at 09:03 AM

[redacted]

Endurance Ransomware Developer

October 22, 2022, 09:03 AM #1

Greetings.

I am a single developer working with ransomware. I am making this simple. I am looking for some C# developers to help with future development.
Please contact me for further details in private messages.
Price for helping me out and becoming a larger team will mean that profits are split evenly between each developer.
Thank you

buy my data - sellix

Webz.io

How easy is it?

Using AI/ML for Cybercrime

ChatGPT & Co. are already being used by cybercriminals

Create Malware

- Basic Malware/Ransomware/Payloads
- Find vulnerabilities and write exploits
- Automate process and attacks

Malicious Emails

- Create phishing and scam emails
- Deep Fake CEO fraud
- Interactive replies for BEC fraud

Attack the AI Model

- Adversarial AI Attacks e.g. find weights
- Backdoor the datasets
- Influence the training sets

Old Approach | Wall and Moat

New reality | Escape room

Many Dependencies – Increased Complexity

Installed software & cloud services

Partner companies & external services

Processes, correct data availability

The Human Factor, passwords & more

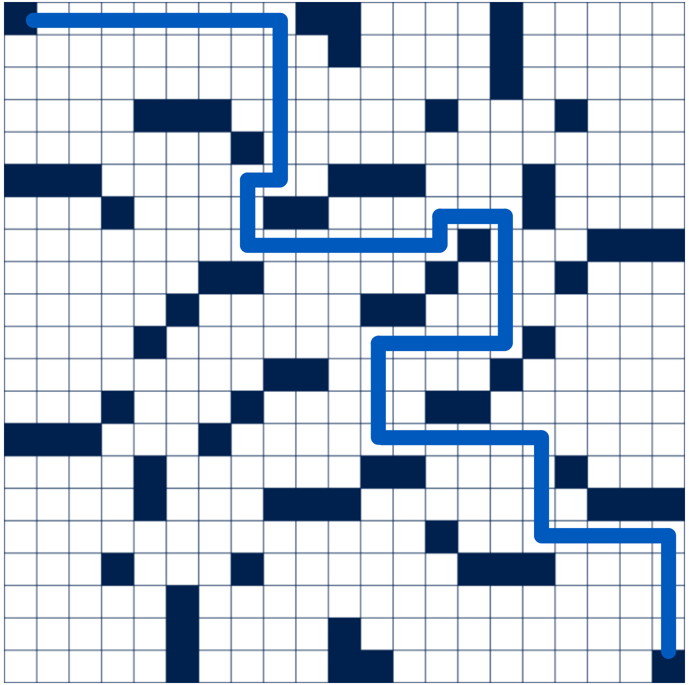
Where to start?

Focus on:

- Automation
- Visibility
- Integration
- AI/ML

My current provider is already covering this

“I don’t need to care about cyber security, we have an AI software for this.”



Increased protection and reduced complexity with Acronis

- ✓ **Patching + Exploit Prevention**
- ✓ **Backup + Disaster Recovery**
- ✓ **Monitoring + Cyber Scripting**

- ✓ **Email Security + URL filtering**
- ✓ **Behavior detection + Anti-ransomware**
- ✓ **Machine Intelligence + Self Protection**

Agenda

Welcome to our webinar!	**Jeff Hardy**, Solutions Marketing Manager, Acronis
Welcome greetings	**Patrick Pulvermueller,** CEO**,** Acronis
Bad Robot: Ransomware in the age of AI and what you need to stop it	**Candid Wuest**, VP of Research, Acronis
The Hardware / Software Alliance: Why MSPs should care	**Jeff Hardy**, Acronis **Todd Cramer**, Director Security Ecosystem Business Development, Intel
MSPs on the Edge: Advanced Security with EDR	**James Erby**, Solutions Engineer, Acronis
EDR case study discussion	**Jeff Hardy**, Acronis **Brian Harvey**, Network Operations Manager, Business World
Live audience Q&A	
Wrap-up	**Jeff Hardy**, Acronis

Acronis | intel

The Hardware / Software Alliance:

Why MSPs should care

Todd Cramer

Director Security
Ecosystem Business
Development
Intel

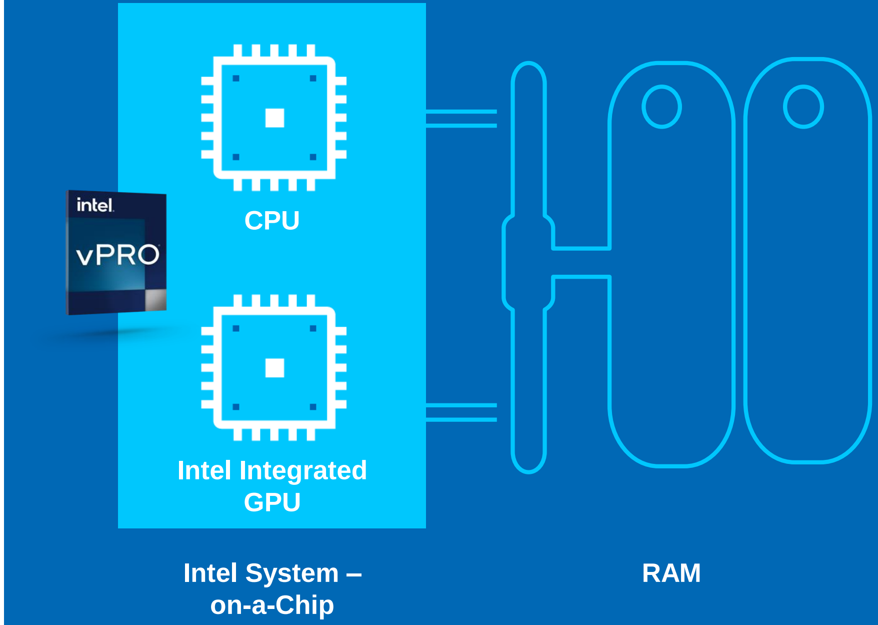
Jeff Hardy

Solutions Marketing
Manager
Acronis

#CyberFit

GPU Offloading

- Intel’s system-on-a-chip architecture
- Highly parallelizable algorithm
- Offload memory scanning to the Intel Integrated GPU
- CPU stays available for other tasks
- Resulting in speedup for large memory scans>2.4x for Acronis



Fileless Attack Challenges

- Malicious code that works completely in memory
- 900% increase since 2021. Nearly 71% of all attacks
- Problematic for EDRs to detect
- Re-injects malware into legitimate processes that require high compute to scan
- Dual use tools like Cobalt Strike use memory attacks to gain foothold to drop Ransomware and other attacks

With Hardware Security, Acronis memory scanning can help detect and stop attacks early in the kill-chain

Agenda

Welcome to our webinar!	**Jeff Hardy**, Solutions Marketing Manager, Acronis
Welcome greetings	**Patrick Pulvermueller,** CEO**,** Acronis
Bad Robot: Ransomware in the age of AI and what you need to stop it	**Candid Wuest**, VP of Research, Acronis
The Hardware / Software Alliance: Why MSPs should care	**Jeff Hardy**, Acronis **Todd Cramer**, Director Security Ecosystem Business Development, Intel
MSPs on the Edge: Advanced Security with EDR	**James Erby**, Solutions Engineer, Acronis
EDR case study discussion	**Jeff Hardy**, Acronis **Brian Harvey**, Network Operations Manager, Business World
Live audience Q&A	
Wrap-up	**Jeff Hardy**, Acronis

MSPs on the Edge:

Advanced Security with EDR

#CyberFit

James Erby

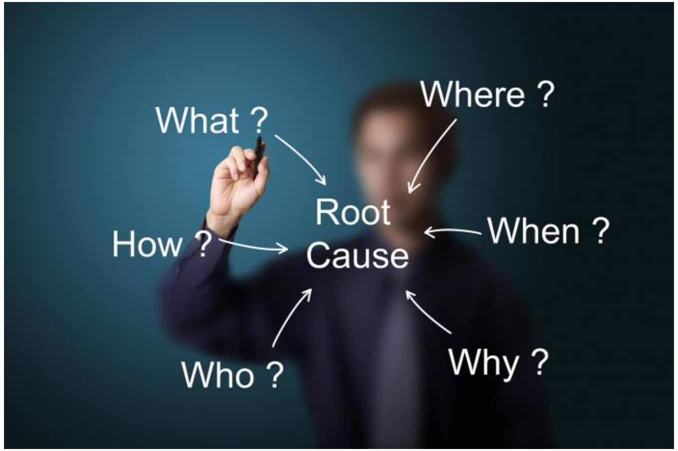
Solutions Engineer
Acronis

What’s 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

Advanced attacks can only be countered with advanced security

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

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

Addressing breach impact is inevitable to ensure continuity

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

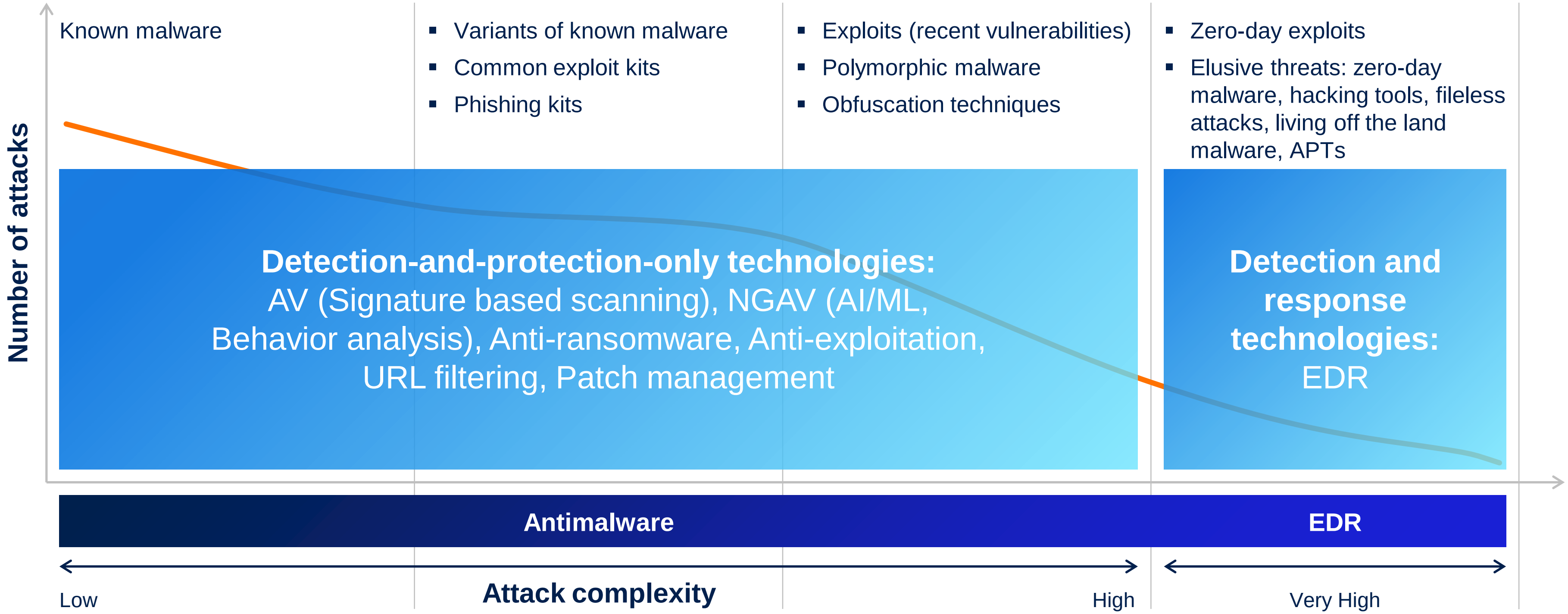
For many – compliance is essential

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

Where EDR fits in the stack



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

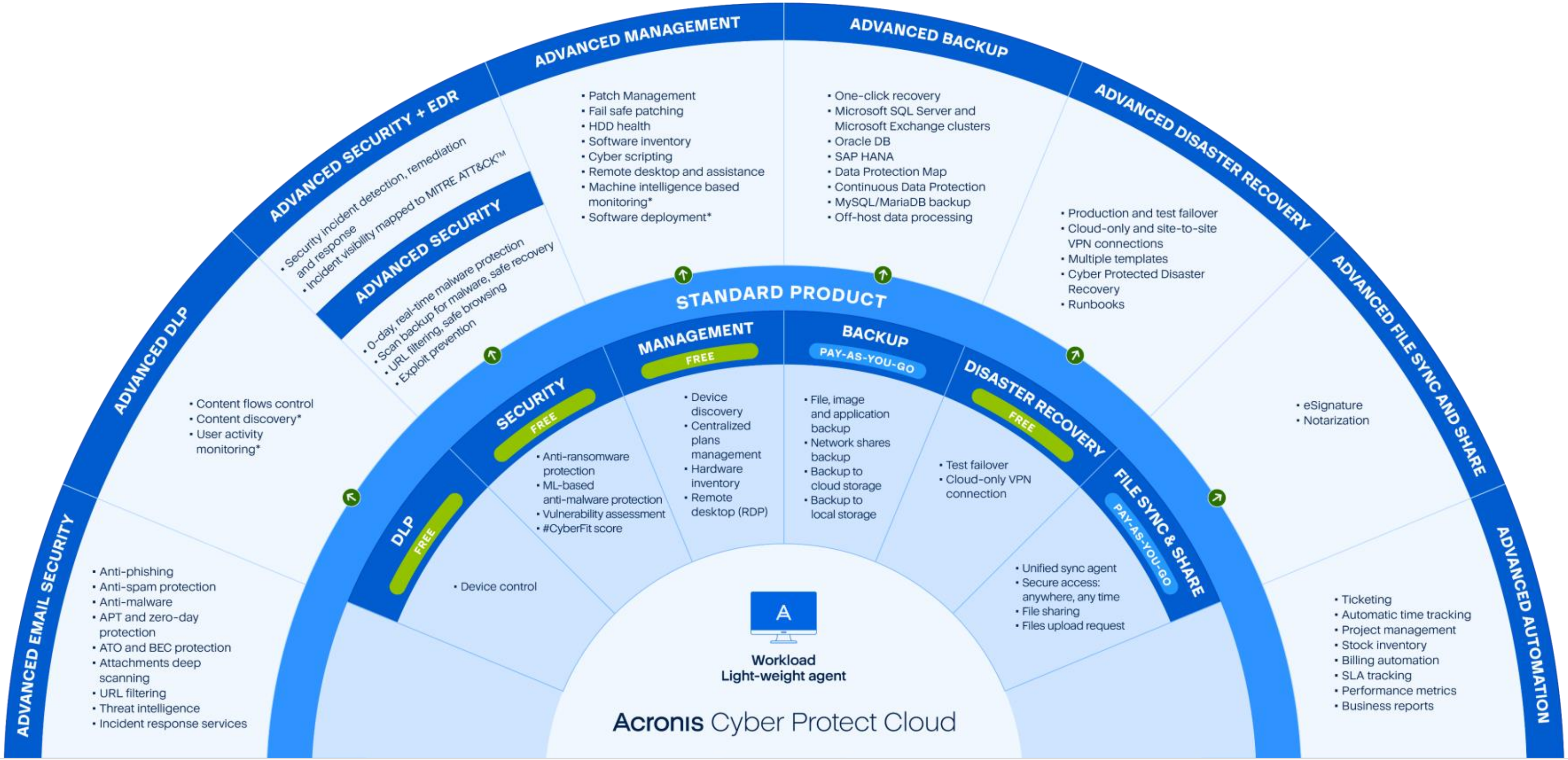
Detection-and-protection-only technologies:
AV (Signature based scanning), NGAV (AI/ML, Behavior analysis), Anti-ransomware, Anti-exploitation, URL filtering, Patch management

Detection and response technologies:
EDR

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 and 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 a multitude of response capabilities to: ▪ Contain the incident at the endpoint ▪ Investigate security incidents ▪ Provide remediation

Acronis Cyber Protect Cloud with Advanced Packs



ADVANCED EMAIL SECURITY
- Anti-phishing
- Anti-spam protection
- Anti-malware
- APT and zero-day protection
- ATO and BEC protection
- Attachments deep scanning
- URL filtering
- Threat intelligence
- Incident response services

ADVANCED DLP
- Content flows control
- Content discovery*
- User activity monitoring*

ADVANCED SECURITY + EDR
- Security incident detection, remediation and response
- Incident visibility mapped to MITRE ATT&CK™

ADVANCED SECURITY
- 0-day, real-time malware protection
- Scan backup for malware, safe recovery
- URL filtering, safe browsing
- Exploit prevention

ADVANCED MANAGEMENT
- Patch Management
- Fail safe patching
- HDD health
- Software inventory
- Cyber scripting
- Remote desktop and assistance
- Machine intelligence based monitoring*
- Software deployment*

ADVANCED BACKUP
- One-click recovery
- Microsoft SQL Server and Microsoft Exchange clusters
- Oracle DB
- SAP HANA
- Data Protection Map
- Continuous Data Protection
- MySQL/MariaDB backup
- Off-host data processing

ADVANCED DISASTER RECOVERY
- Production and test failover
- Cloud-only and site-to-site VPN connections
- Multiple templates
- Cyber Protected Disaster Recovery
- Runbooks

ADVANCED FILE SYNC AND SHARE
- eSignature
- Notarization

ADVANCED AUTOMATION
- Ticketing
- Automatic time tracking
- Project management
- Stock inventory
- Billing automation
- SLA tracking
- Performance metrics
- Business reports

STANDARD PRODUCT

DLP
FREE
- Device control

SECURITY
FREE
- Anti-ransomware protection
- ML-based anti-malware protection
- Vulnerability assessment
- #CyberFit score

MANAGEMENT
FREE
- Device discovery
- Centralized plans management
- Hardware inventory
- Remote desktop (RDP)

BACKUP
PAY-AS-YOU-GO
- File, image and application backup
- Network shares backup
- Backup to cloud storage
- Backup to local storage

DISASTER RECOVERY
FREE
- Test failover
- Cloud-only VPN connection

FILE SYNC & SHARE
PAY-AS-YOU-GO
- Unified sync agent
- Secure access: anywhere, any time
- File sharing
- Files upload request

Workload
Light-weight agent

Acronis Cyber Protect Cloud

Includes all functionalities of Advanced Security

Full feature-based comparison between the two packs is available here

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 Acronis Cyber Protection Operations Centers

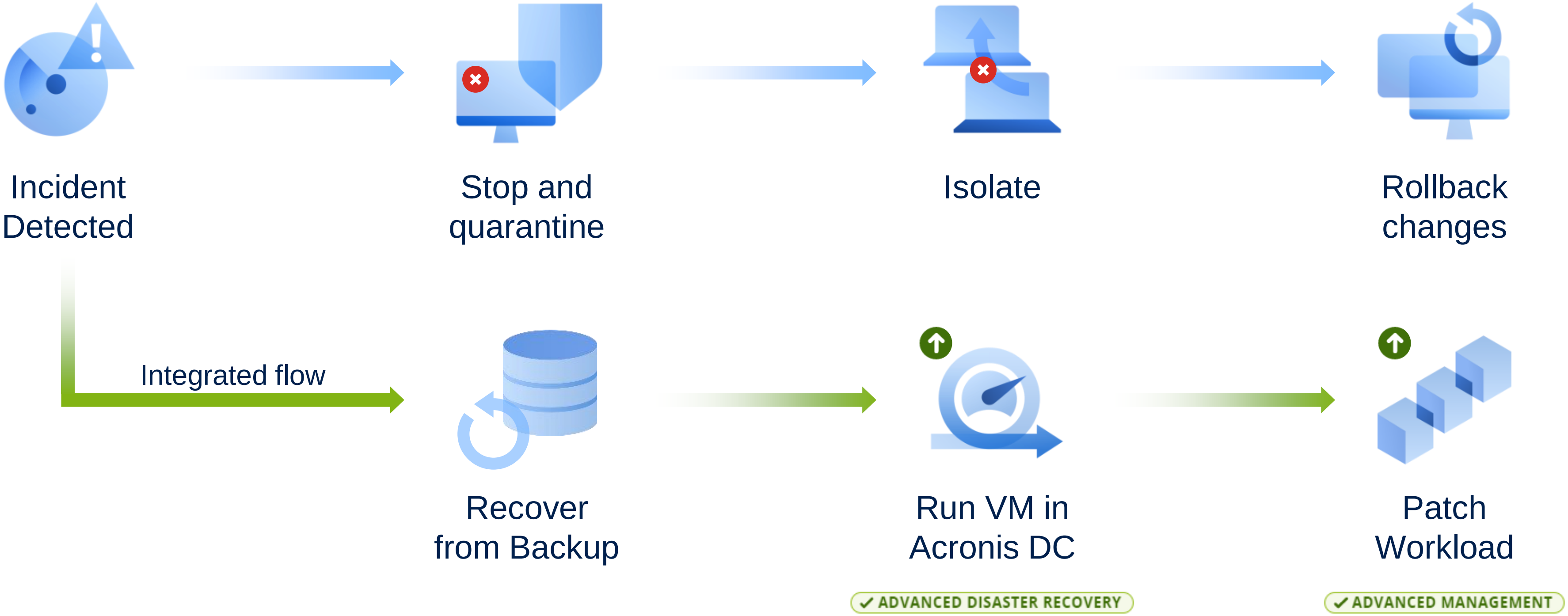
Forensic backup: Enable forensic investigations by collecting digital evidence in image-based backups

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



Incident Detected

Stop and quarantine

Isolate

Rollback changes

Integrated flow

Recover from Backup

Run VM in Acronis DC

✓ ADVANCED DISASTER RECOVERY

Patch Workload

✓ ADVANCED MANAGEMENT

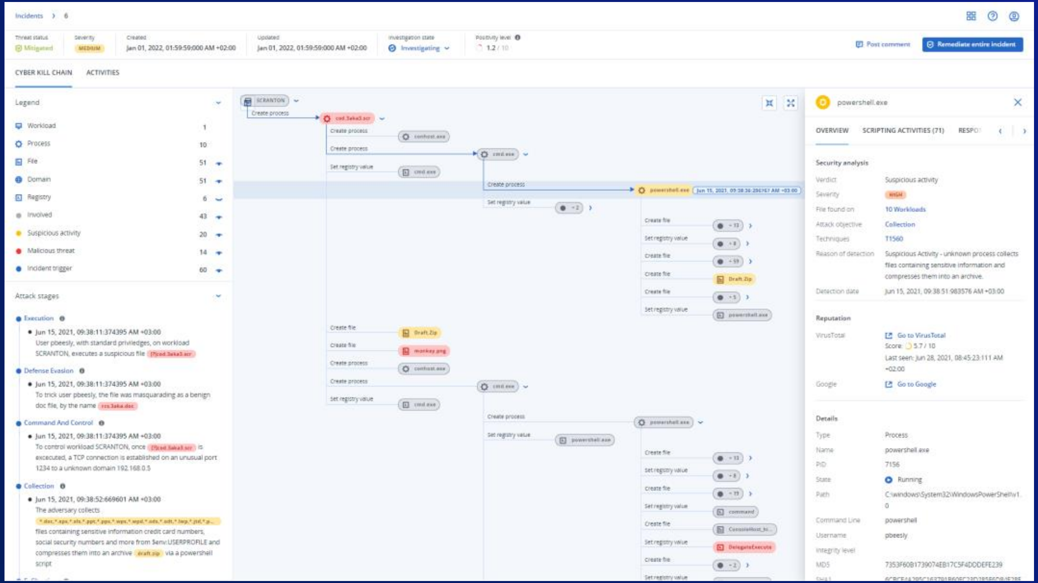
Acronis

Advanced Security + EDR

#CyberFit

DETECT, and RESPOND to advanced attacks that sneak past other endpoint defenses with minimal investigation efforts and with pre-integrated IDENTIFY, PROTECT, and RECOVER capabilities.

- **MSP-class EDR** that’s effective and… usable
- **Rapid detection and incident analysis** across MITRE ATT&CK®
- **Continuity at the speed of business** with protection across the NIST framework



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

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 [?]cod.3aka3.scr

Defense Evasion
- Jun 15, 2021, 09:38:11:374395 AM +03:00
  To trick user pbeesly, the file was masquarading as a benign doc file, by the name rcs.3aka.doc

Command And Control
- Jun 15, 2021, 09:38:11:374395 AM +03:00
  To control workload SCRANTON, once [?]cod.3aka3.scr is excecuted, 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 *.doc,*.eps,*.xls,*.ppt,*.pps,*.wps,*.wpd,*.ods,*.odt,*.lwp,*.jtd,*.p... 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

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

Agenda

Welcome to our webinar!	**Jeff Hardy**, Solutions Marketing Manager, Acronis
Welcome greetings	**Patrick Pulvermueller,** CEO**,** Acronis
Bad Robot: Ransomware in the age of AI and what you need to stop it	**Candid Wuest**, VP of Research, Acronis
The Hardware / Software Alliance: Why MSPs should care	**Jeff Hardy**, Acronis **Todd Cramer**, Director Security Ecosystem Business Development, Intel
MSPs on the Edge: Advanced Security with EDR	**James Erby**, Solutions Engineer, Acronis
EDR case study discussion	**Jeff Hardy**, Acronis **Brian Harvey**, Network Operations Manager, Business World
Live audience Q&A	
Wrap-up	**Jeff Hardy**, Acronis

Acronis | intel

EDR case study, live discussion

Brian Harvey

Network operations Manager
Business World

Jeff Hardy

Solutions Marketing Manager
Acronis

#CyberFit

Agenda

▪ **Welcome to our webinar!**	**Jeff Hardy**, Solutions Marketing Manager, Acronis
▪ **Welcome greetings**	**Patrick Pulvermueller,** CEO**,** Acronis
▪ **Bad Robot: Ransomware in the age of AI and what you need to stop it**	**Candid Wuest**, VP of Research, Acronis
▪ **The Hardware / Software Alliance: Why MSPs should care**	**Jeff Hardy**, Acronis **Todd Cramer**, Director Security Ecosystem Business Development, Intel
▪ **MSPs on the Edge: Advanced Security with EDR**	**James Erby**, Solutions Engineer, Acronis
▪ **EDR case study discussion**	**Jeff Hardy**, Acronis **Brian Harvey,** Network Operations Manager, Business World
▪ **Live audience Q&A**	
▪ **Wrap-up**	**Jeff Hardy**, Acronis

Acronis | intel

Live audience Q&A

Jeff Hardy

Solutions Marketing Manager
Acronis

#CyberFit

Acronis | intel

Wrap-up

Jeff Hardy

Solutions Marketing Manager
Acronis

#CyberFit

Acronis Academy

LEARN MORE, EARN MORE

Cloud tech associate — Advanced Security with EDR

- ✓ **EDR overview:** Purpose and distinction from prevention technologies.
- ✓ **Attack landscape and response:** Understanding attacks and effective EDR response.
- ✓ **Security challenges:** Complex threats, diverse endpoints, rapid incident response.
- ✓ **MSP Challenges:** Complexity, scalability, integration issues with EDR.
- ✓ **Advanced Security with EDR:** Benefits of combining advanced security with EDR.

SCAN ME

TO GO TO COURSE PAGE

https://go.acronis.com/CTEDR

Acronis

Cyber Foundation Program

Be a socially responsible business with Acronis and build a school for indigenous Mexican kids.

We do all the work, you share the credit.

foundation@acronis.org