MRB SECURE

CYBERSIXER # 2: AI IN CYBER SECURITY

OCTOBER 2024

AI IN CYBER SECURITY

2:00pm	Welcome Participants & Partners
2:25pm	Peter Kohlöffel : Tech Wise Solutions - Introduction
2:30pm	Ian Nettleton : MRB Secure
2:40pm	Brecht Mohonathan : SMART Stadiums
3:00pm	Jacques Smit : Acronis AI, Cyber Security
3:30pm	Ian Nettleton : Closing Remarks, Introduce Peter Kohloffel & Jacques Smit
3:35pm	Peter Kohloffel from Tech Wise Solutions & Jacques Smit host Q & A with Special Guests
4:30pm	Networking & Refreshments

SPECIAL GUESTS

WOMEN	MEN
Relebohile Mkhize	Dominic Hendricks
Sarah Barber	Joshua Richards

OUR PARTNERS

Acronis

lessrisk.biz

MR3 vSOC

Acronis

MR3 SECURE

veeAM

4TRess
Digital Defence Integration

KnowBe4

OUR PARTNERS

BRIEF HISTORY & THANKS

- Registered in 2010, owner run & self funded
- BBB-EE Rating Level 2
- Focused on Cyberhealth of Orgs with speciality in the Data Protection space.
- Operations in SA and EU (Portugal based)
- Acronis Platinum Cybersecurity Partner (15 Globally)

MRB SECURE

OUR CORE SERVICES

1. Holistic Security Review with Tailored Solution Bundles
2. vSOC Services
3. Security Awareness
4. Compliance & Risk Management
5. Data Protection as a Service

MRB
SECURE

SECURITY SERVICES

1. Holistic Security Review

2. Regulatory Compliance

3. Tailored Bundles

4. Expertly Crafted by seasoned professionals

Powered By

4TRESS
Digital Defence Integration

MRB SECURE

VIRTUAL SECURITY OPS CENTRE

1. Basic SOC as a Service

2. Standard SOC as a Service – SME's

3. Advanced SOC as a Service

4. Enterprise SOC as a Service

5. Computer Incident Response Team (CIRT)

Powered By

MRB SECURE

MRB SECURE

SECURITY AWARENESS PACKAGES

1. Fully Automated Simulated Phishing Attacks
2. World’s Largest Library of awareness training content
3. AI-Driven Training Recommendations
4. Build Proficiency Using Assessments
5. Integrate With Active Directory

Powered By

Acronis KnowBe4

MRB SECURE

COMPLIANCE

1. Disaster Recovery & Business Continuity Planning
2. ISO 22301 27701, 2700
3. Compliance in IT
4. Compliancy Roadmap
5. Readiness Assessment

Powered By

lessrisk.biz

MRB SECURE

DATA PROTECTION - dpaas

1. Managed Services (Backup & Restore)

2. Ransomware & Malware Protection

3. E-Mail Protection

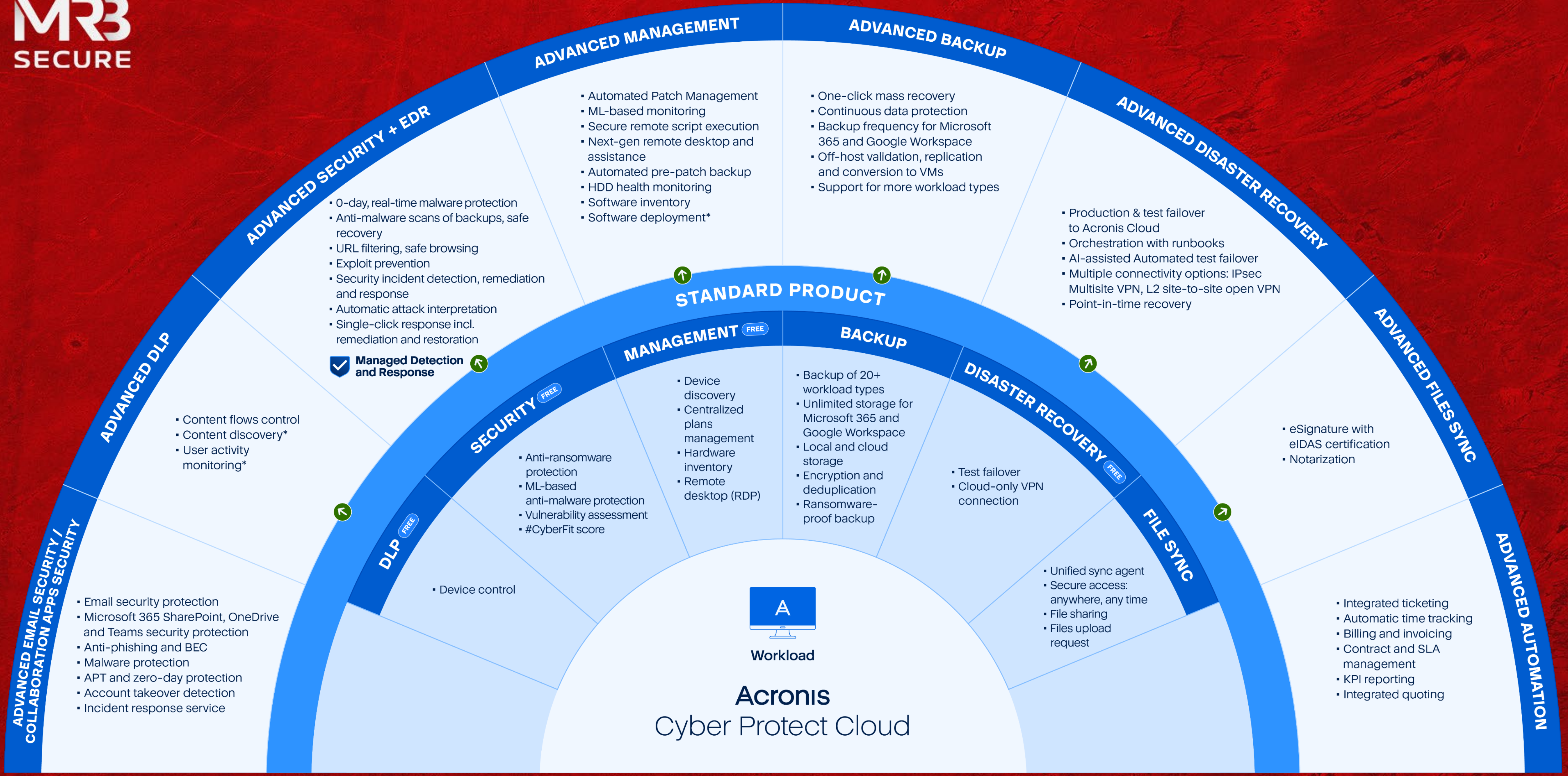
4. Business Resilience

5. Forensics

Powered By

Acronis

MRB SECURE



ADVANCED EMAIL SECURITY / COLLABORATION APPS SECURITY

- Email security protection
- Microsoft 365 SharePoint, OneDrive and Teams security protection
- Anti-phishing and BEC
- Malware protection
- APT and zero-day protection
- Account takeover detection
- Incident response service

ADVANCED DLP

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

ADVANCED SECURITY + EDR

- 0-day, real-time malware protection
- Anti-malware scans of backups, safe recovery
- URL filtering, safe browsing
- Exploit prevention
- Security incident detection, remediation and response
- Automatic attack interpretation
- Single-click response incl. remediation and restoration

Managed Detection and Response

ADVANCED MANAGEMENT

- Automated Patch Management
- ML-based monitoring
- Secure remote script execution
- Next-gen remote desktop and assistance
- Automated pre-patch backup
- HDD health monitoring
- Software inventory
- Software deployment*

ADVANCED BACKUP

- One-click mass recovery
- Continuous data protection
- Backup frequency for Microsoft 365 and Google Workspace
- Off-host validation, replication and conversion to VMs
- Support for more workload types

ADVANCED DISASTER RECOVERY

- Production & test failover to Acronis Cloud
- Orchestration with runbooks
- AI-assisted Automated test failover
- Multiple connectivity options: IPsec Multisite VPN, L2 site-to-site open VPN
- Point-in-time recovery

ADVANCED FILES SYNC

- eSignature with eIDAS certification
- Notarization

ADVANCED AUTOMATION

- Integrated ticketing
- Automatic time tracking
- Billing and invoicing
- Contract and SLA management
- KPI reporting
- Integrated quoting

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

- Backup of 20+ workload types
- Unlimited storage for Microsoft 365 and Google Workspace
- Local and cloud storage
- Encryption and deduplication
- Ransomware-proof backup

DISASTER RECOVERY FREE

- Test failover
- Cloud-only VPN connection

FILE SYNC

- Unified sync agent
- Secure access: anywhere, any time
- File sharing
- Files upload request

ADV. PACK SPECIAL OFFER 30%

THANK YOU

MRB
SECURE

DP WORLD
WANDERERS STADIUM

Smart Stadium Technologies

The **DP World Wanderers Stadium** is at the forefront of innovation, utilizing advanced technologies to deliver a superior fan experience, optimize operations, and enhance security.

By integrating connected infrastructure, smart analytics, and real-time data, the stadium has streamlined operations and improved fan engagement.

Key initiatives such as seamless WiFi connectivity, personalized SMS interactions, and proactive resource management ensure an unparalleled event experience, setting a new standard for modern sports / hybrid venues.

by Brecht Mohonathan (CFO)

Defining the Smart Stadium

Connected Facilities

Using 5G & High Speed WIFI, the stadium integrates a network of devices allow us to monitor and control various systems, from power usage and pitch maintenance to security and Fan WIFI

Personalized Experiences

Fans can access real-time information, order food and drinks, and even customize their future experiences through our 3rd party partnerships, digital platforms and the soon to launch Mobile app

Operational Efficiency via CRM & Analytics Tools

Advanced data analytics and automation help our stadium managers optimize workflows, reduce costs, and make data-driven decisions based on data collected from our various systems

Digital Operations Centre

The dedicated IT Operations Centre manages our digital capabilities and serves as a central control area from which all connected devices are monitored and managed

Enhancing Stadium Operations

1

Secured High Speed Fan WIFI

Our fully managed redundant & scalable WIFI solution enables Fans to remain connected throughout the entire venue with seamless handover through the stadium

2

Custom CRM Tool

Our CRM tool is prepped to manage all fan & tenant interactions allowing us to craft personalized experiences for future engagement. The “report an issue module” opens our facilities & security desk to all fans allowing for active reporting of issues from your seat improving our visibility and the overall fan experience

3

Automated Concessions

Via our 3rd Party Integrations which is activated for larger events. The in seat ordering capabilities streamline the food and beverage service, reducing wait times and improving customer satisfaction.

Enhancing Stadium Operations

4

Dedicated IT Operations Centre

Our fully managed dedicated IT Operations Centre manages our complete suite of Digital solutions with active monitoring and response to any incidents that occur both on and off event days

5

Integrated Service Desks

Our CRM tool directly feeds into the appropriate service desks allowing for efficient resolution of queries and interactions raised throughout the stadium by both fans and tenants

6

Live Broadcasting & Streaming

Our infrastructure has been completely setup to facilitate secured live broadcasting and streaming of events for both local and international media that cover events at the stadium. This is done via a separate dedicated network that has been built specifically to enable secure media broadcast and streaming

Improving Venue Security 2025

1

Intelligent Surveillance

We will soon be piloting Advanced video analytics and facial recognition to enhance security monitoring, enabling early detection and rapid response to potential threats.

2

Access Control

Biometric Identification and automated access systems will ensure only authorized personnel can enter restricted areas, improving overall venue security.

3

Emergency Response

Integrated communication systems and emergency protocols enable our stadium staff to coordinate and respond quickly to any incidents or crises.

Sustainable Solutions For Mother Earth

Energy Efficiency

Smart building technologies, such as LED lighting, intelligent HVAC systems, and renewable energy sources, reduce the stadium's carbon footprint and operating costs.

Water Conservation

Innovative water management systems, including a borehole and greywater recycling, help minimize water usage and promote sustainable practices.

Waste Reduction

Comprehensive waste management strategies, including recycling contribute to the stadium's overall environmental sustainability efforts.

The Future of Smart Stadiums

As technology continues to advance, smart stadiums will evolve into increasingly sophisticated venues, providing both fans and operators with an unparalleled experience. With features such as seamless mobile integration, predictive analytics, and sustainable solutions, the future of smart stadiums is set to redefine how we enjoy and manage live events.

To stay at the forefront of these changes, we are committed to continuous innovation and improvement at **The DP World Wanderers Stadium.** This includes investing in cutting-edge technology and applications that facilitate real-time engagement.

Furthermore, ongoing collaboration with industry leaders and technology partners will ensure we can swiftly integrate new solutions. By fostering a culture of adaptability and forward-thinking, we aim to enhance the overall experience for fans and operators alike, ensuring that **The DP World Wanderers Stadium** remains ahead in the smart stadium movement in South Africa.

Thank You

DP WORLD

WANDERERS
STADIUM

AI & ML in Cybersecurity and Data Protection

October 2024

#CyberFit

Jacques Smit

Strategic Executive

How I Learned to Stop Worrying and Let the Machines Take Over… But Not Really

#CyberFit

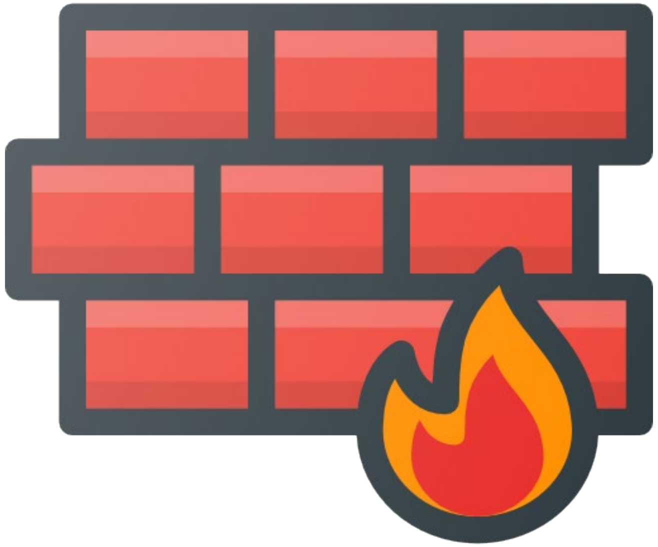
Jacques Smit

Strategic Executive

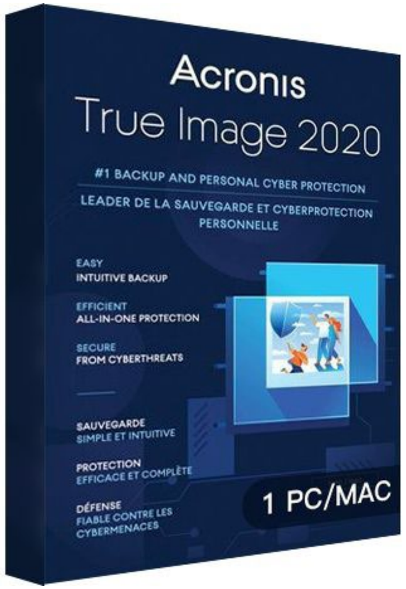
There are many things in our lives that have been simplified.

But why is it that Cyber Security and Data Protection has gone the other way?

It used to be simple



Install a firewall



Create a backup

But, technology and talent needs changed

01

IT moved to the Cloud.

10M+ Cloud servers globally

02

The volume and importance of data grew exponentially.

2ZB 2010 to 181ZB 2025
1ZB is 1,000,000,000,000 GB

03

New productivity and SaaS apps increase risk.

30,000 Global SaaS Apps

04

The need for skilled talent expanded.

3.5M Open Cybersecurity jobs

In response, we had to learn and use an increasing number of applications to service their your needs for

Backup, Security, DR, Management and Automation

Ransomware protection

Backup forensics

Anti-malware

Hard drive health monitoring

79%

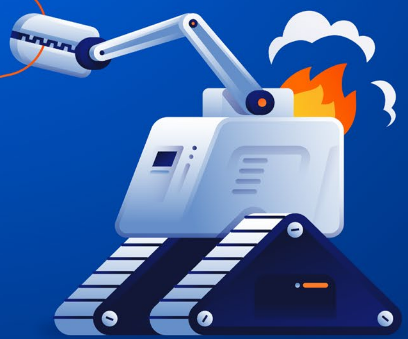
Of organizations rely on up to **10 different services**

Patch management

Continuous data protection

Vulnerability assessments

URL filtering



Organizations are trying to defend data with complex patchworks of unconnected solutions

This result is more

Cyberthreats.

Vendors.

Agents.

Invoices.

Risk.

Updates.

Trainings.

Complexity.

Complexity Management Strategies?

Continue on current course adding more vendors and staff to manage the increasing complexity and customer demands.

1

Consolidate around a set of purpose-built and integrated SP technologies that reduce complexity and increase control and customer satisfaction.

2

Only one of these strategies wins...

Acronis

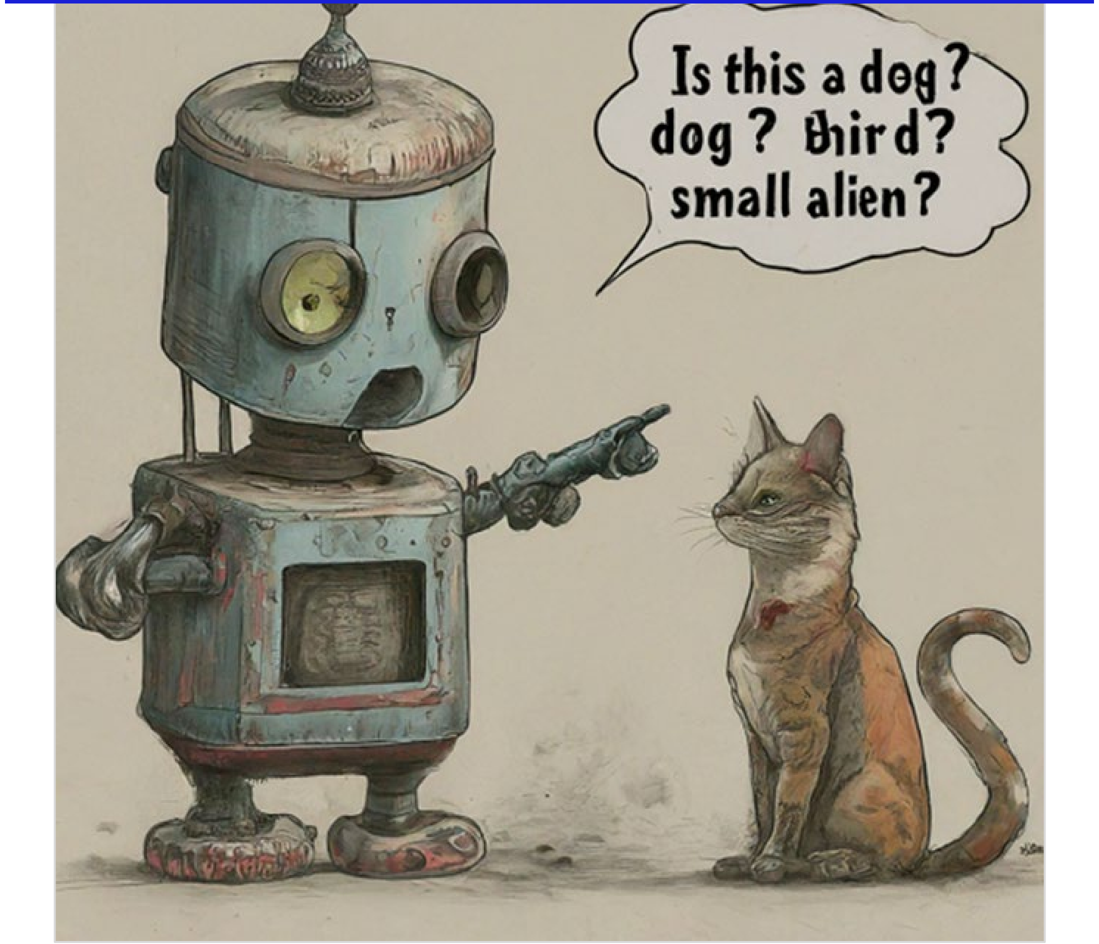
Acronis

#CyberFit

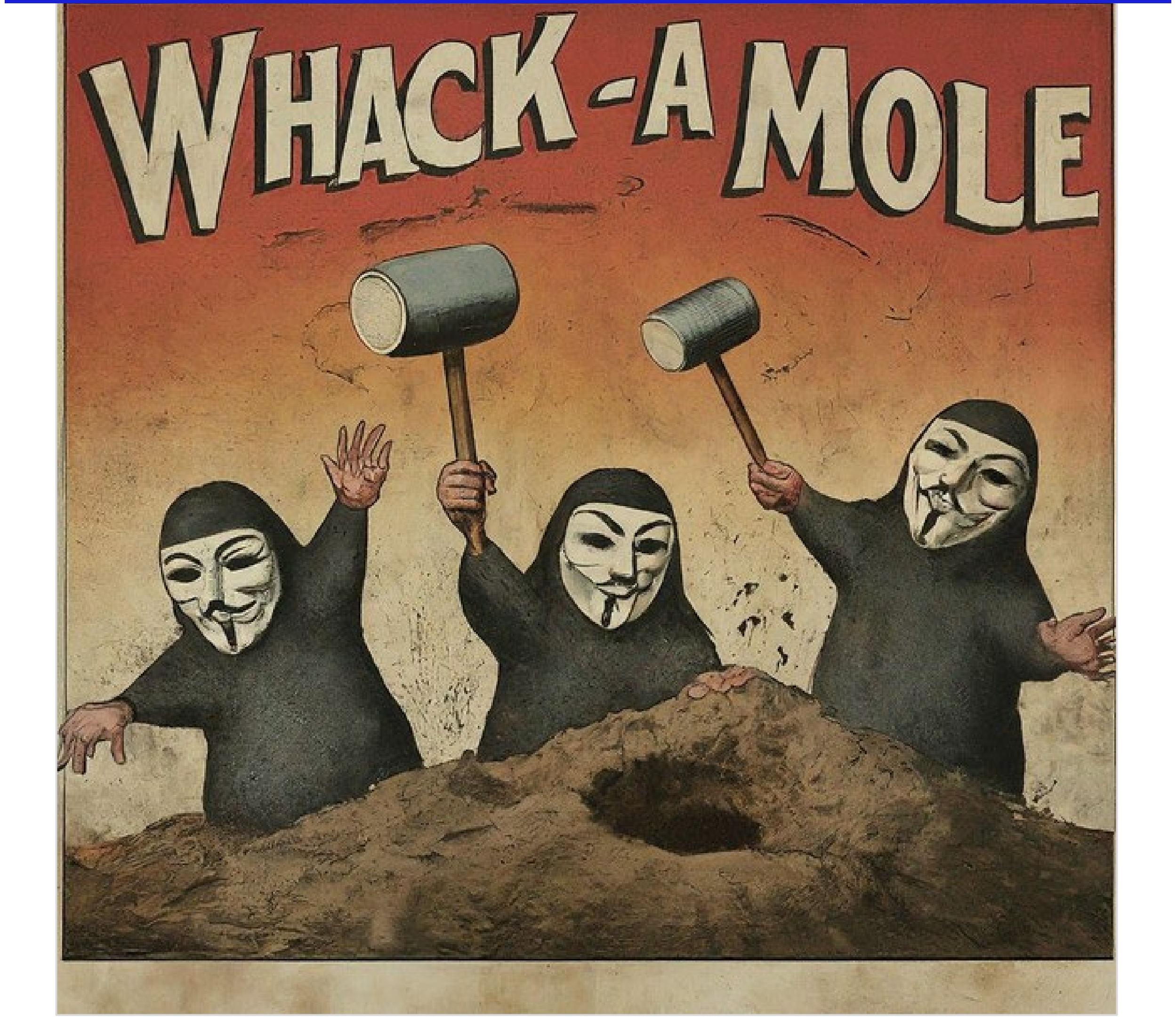
The Role of AI & ML in Cybersecurity

Artificial intelligence?

Machine Learning?



Traditional Threat Detection



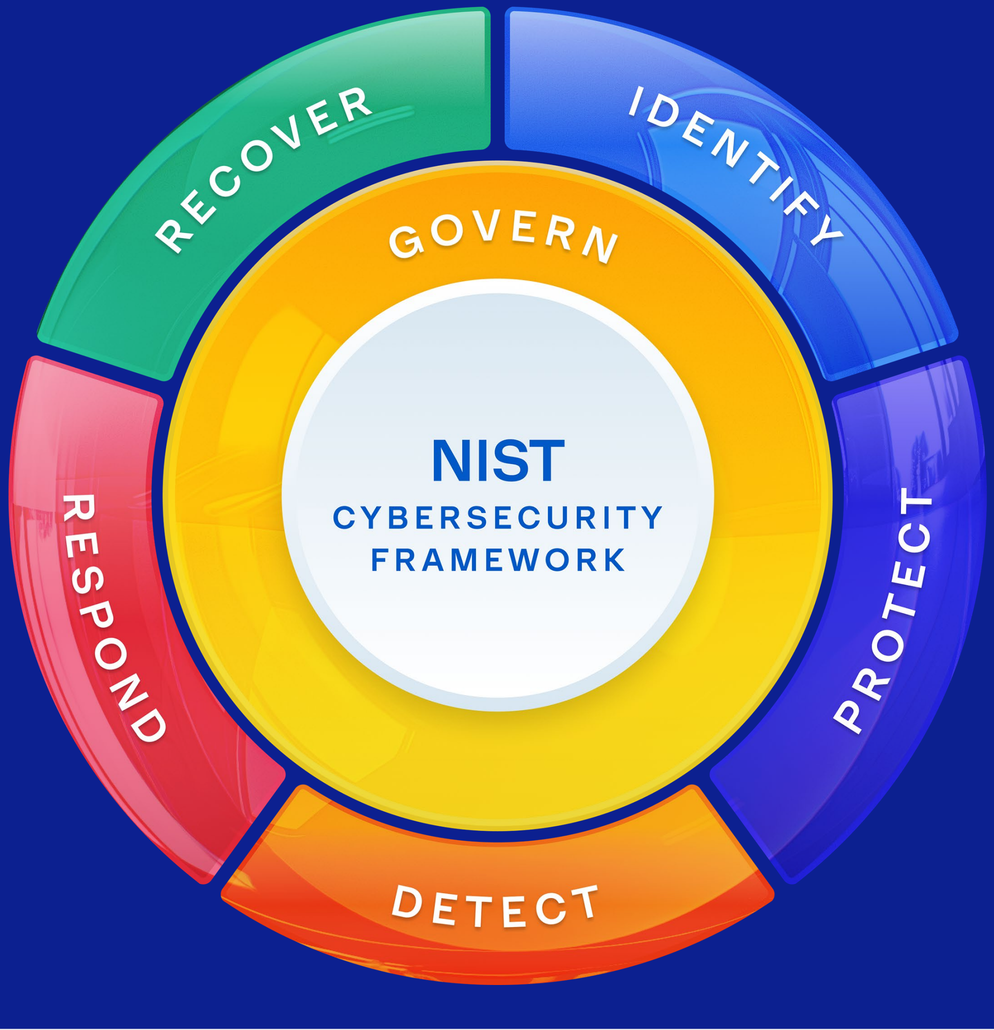
Acronis

#CyberFit

Why Acronis Cyber Protect Cloud?

Modernize your cybersecurity and backup with integrated AI / ML

Acronis Cyber Protect: Complete coverage of NIST 2.0 CS framework



Govern

- Provisioning via a single agent and platform
- Centralized policy management
- Role-based management
- Information-rich dashboard
- Schedulable reporting

Identify

- Software and hardware inventory
- Unprotected endpoint discovery
- Content discovery
- Data classification
- Vulnerability assessments

Protect

- Security configuration management
- Patch management
- Device control
- Data loss prevention
- Security training

Detect

- AI- and ML-based behavioural detection
- Exploit prevention
- Anti-malware and anti-ransomware
- Email security
- URL filtering

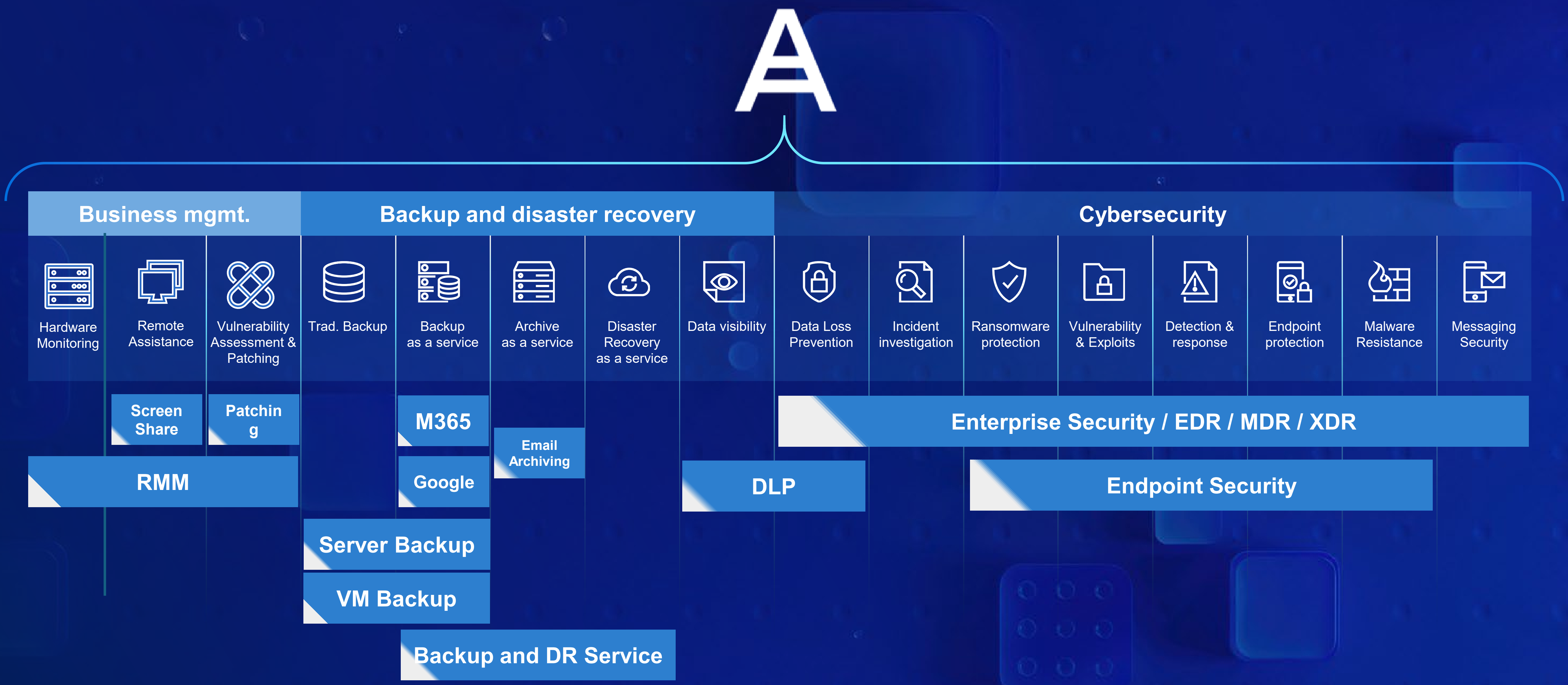
Respond

- Rapid incident prioritization
- Incident analysis
- Workload remediation with Isolation
- Forensic backups
- Remote access for investigation

Recover

- Rapid rollback of attacks
- One-click mass recovery
- Self-recovery
- Backup integration
- Disaster recovery Integration

Consolidation with Acronis



Business mgmt.

Backup and disaster recovery

Cybersecurity

Hardware Monitoring

Remote Assistance

Vulnerability Assessment & Patching

Trad. Backup

Backup as a service

Archive as a service

Disaster Recovery as a service

Data visibility

Data Loss Prevention

Incident investigation

Ransomware protection

Vulnerability & Exploits

Detection & response

Endpoint protection

Malware Resistance

Messaging Security

Screen Share

Patchin g

M365

Email Archiving

Enterprise Security / EDR / MDR / XDR

RMM

Google

DLP

Endpoint Security

Server Backup

VM Backup

Backup and DR Service

Acronis

Source: Gartner, IDC, McKinsey Cyber Market Map

Acronis
Cyber Protect Cloud

One Platform, One Agent,
All within One Protection Plan

Complete coverage of NIST framework:
Govern, Identify, Protect, Detect, Respond and Recover

DATA PROTECTION

Backup

Standard Backup

- Backup of 25+ workload types
- Local and cloud storage
- Encryption and deduplication
- Ransomware-proof backup
- **Microsoft 365**
  - Exchange Online, SharePoint Online, OneDrive, Teams, OneNote
  - Email Archiving
  - Group management

Advanced Backup

- One-click mass recovery
- Continuous data protection
- Backup frequency for Microsoft 365 and Google Workspace
- Off-host validation, replication, and conversion to VMs
- Support for additional workload types
- Backup notarization

Disaster Recovery

FREE

- Test failover
- Cloud-only VPN connection

Advanced DR

- Production and test failover to Acronis Cloud
- Orchestration with runbooks
- AI-assisted Automated test failover
- Fast Automated Failback with near-zero downtime
- Multiple connectivity options:
  - IPsec Multisite VPN, L2 site-to-site open VPN, Cloud-only VPN

CYBERSECURITY

Detection and Response

FREE

- AI-based anti-malware protection
- #CyberFit score (Security posture assessment)
- Device control

Advanced Security + EDR

- Gen AI-guided incident investigation, analysis, automated response
- Single-click response, including attack-specific rollback and recovery
- Next Generation Antivirus (NGAV)
- Anti-ransomware protection
- 0-day and exploit protection
- URL filtering
- Anti-malware scans of backups

Advanced Security + XDR

- Extended endpoint protection with visibility and response across most vulnerable attack surfaces - email, identity, Microsoft 365 apps
- Gen AI-guided incident investigation, analysis, response and recovery

Advanced Security + MDR

- 24/7/365, Continuous monitoring with expedited investigation from security analysts
- Event triage, prioritization, and rapid response including recovery

SaaS Security

Advanced Email Security

- Phishing and Quishing prevention
- Business Email Compromise prevention
- Malware protection
- APT and zero-day protection
- Account takeover detection
- Incident response service
- Microsoft 365, Google Workspace, Exchange and any SMTP supporting email service

Advanced Collaboration Apps Security

- Microsoft 365 SharePoint, OneDrive and Teams security protection
- Malware protection
- APT and zero-day protection
- Incident response service

Security Awareness Training

- Rich and engaging library of training courses
- Phishing simulation and exercises
- Mobile-friendly learning experience
- Available in multiple major languages

OPERATIONS

Management

FREE

- **Endpoint**
  - Device Sense™ device discovery
  - Hardware inventory
  - Vulnerability assessment (Windows/Mac/Linux)
  - Remote desktop (RDP)
- **Microsoft 365**
  - Security posture risks dashboard
  - User management (onboard, offboard)

Advanced Management - Endpoint

- Software inventory
- Vulnerability assessment (third-party apps)
- Automated patch management
- ML-based monitoring
- Software deployment
- AI-enabled remote scripting
- Automated pre-patch backup
- HDD health monitoring
- Next-gen remote desktop and assistance

Advanced Management - Microsoft 365

- Remediation of tenant security posture risks
- Remediation of user security posture risks

Automation

Advanced Automation

- Integrated ticketing
- Automatic time tracking
- Billing and invoicing
- Contract and SLA management
- Stock inventory management
- KPI reporting
- Integrated quoting

Acronis

#CyberFit

Improved Data Security And Management AI

AI/ML in Acronis

Acronis AI/ML research and development

Cybersecurity

AI/ML models and services for detecting threats on all stages of program execution – downloading, pre-execution and execution, detecting malicious docs (PDF, JS, etc.)

Smart Backup/DR

Models and algorithms to improve efficient of backup and recovery policy

System Health

Provides Acronis customers with actual information about HDD/SSD health and suggest actions to protect the data

AI Assistant

Chatbot based on DL neural networks to assist Technical Support team to answer frequently asked questions

Deep Find

Semantic search and smart data exploration

System Monitoring

Monitoring system vitals (e.g. CPU load, memory usage) and provide adaptive alerts for abnormal patterns

Stop most threats before they become breaches

Acronis Cyber Protect Cloud

Acronis Active Protection

Anti-ransomware, anti-cryptojacking, AI- and ML-enabled

+

Acronis static AI analyzer

On-access and on-demand detection

Acronis antimalware engine

Any malware (cloud and local detection)

Acronis behavioral engine

On-access detection

Native integration with Windows Security Center

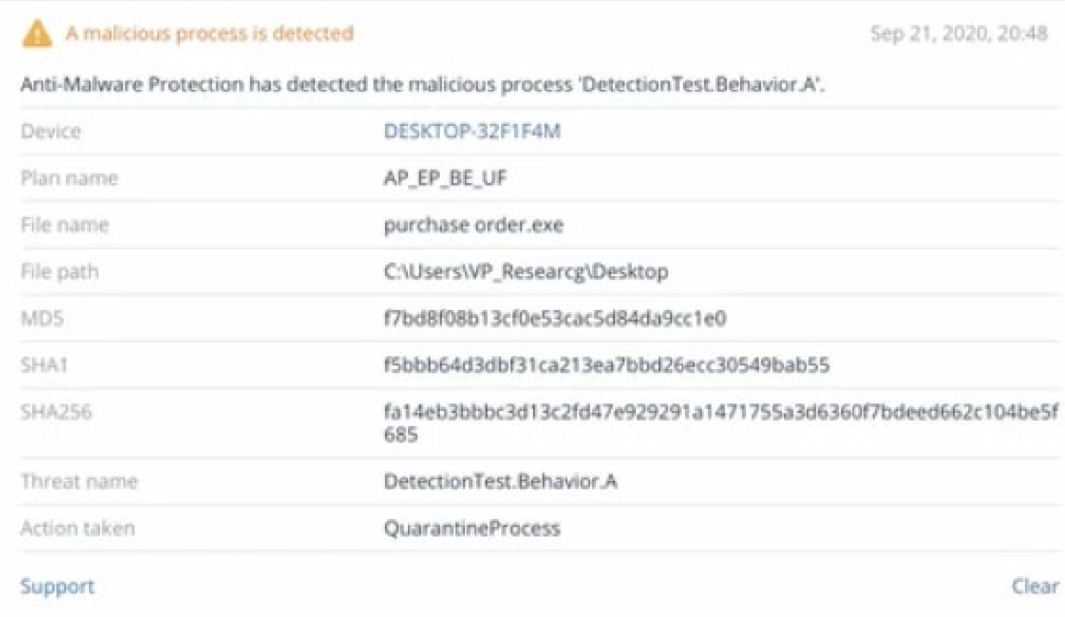
Behavior-based detection

Powerful behavioral heuristics to catch sophisticated threats

Analyze suspicious kernel-level events and all events coming from Windows OS to detect malicious attacks with detection-evasive behavior.

- Effectively dealing with fileless, memory- and script-based attacks (part of APT invasion)
- Dynamic detection rules – catch polymorphic and obfuscated malware
- New malware techniques using symlinks for encrypting files, such as RIPlace, evade detection by most competitive technologies

- Effective detection of unknown, new, and developing threats



A malicious process is detected — Sep 21, 2020, 20:48

Anti-Malware Protection has detected the malicious process 'DetectionTest.Behavior.A'.

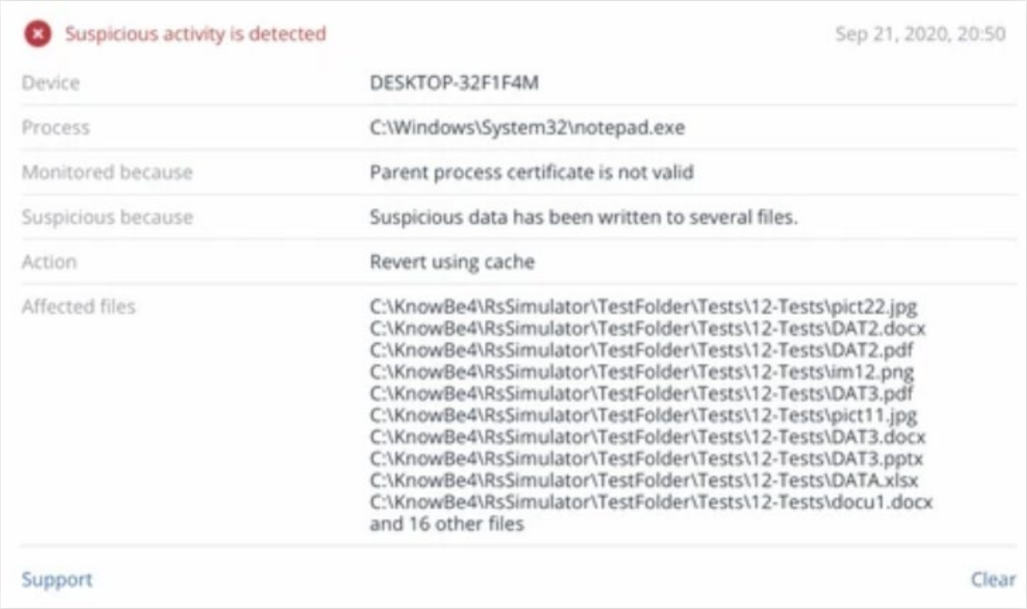
Device	DESKTOP-32F1F4M
Plan name	AP_EP_BE_UF
File name	purchase order.exe
File path	C:\Users\VP_Researcg\Desktop
MD5	f7bd8f08b13cf0e53cac5d84da9cc1e0
SHA1	f5bbb64d3dbf31ca213ea7bbd26ecc30549bab55
SHA256	fa14eb3bbbc3d13c2fd47e929291a1471755a3d6360f7bdeed662c104be5f685
Threat name	DetectionTest.Behavior.A
Action taken	QuarantineProcess

Acronis static AI analyzer

Next-gen static analysis to catch threats before they execute

Examine Windows executables (exe) and dynamic link libraries (DLLs) to determine whether or not a process is malicious prior to execution.

- Machine learning model – trained in Acronis Cloud Brain on millions of malicious and clean files via sandboxes and other security tools
- Proactive layer of protection against malware
- Continuous improvement (new models are trained every hour)



Suspicious activity is detected — Sep 21, 2020, 20:50

Device	DESKTOP-32F1F4M
Process	C:\Windows\System32\notepad.exe
Monitored because	Parent process certificate is not valid
Suspicious because	Suspicious data has been written to several files.
Action	Revert using cache
Affected files	C:\KnowBe4\RsSimulator\TestFolder\Tests\12-Tests\pict22.jpg C:\KnowBe4\RsSimulator\TestFolder\Tests\12-Tests\DAT2.docx C:\KnowBe4\RsSimulator\TestFolder\Tests\12-Tests\DAT2.pdf C:\KnowBe4\RsSimulator\TestFolder\Tests\12-Tests\im12.png C:\KnowBe4\RsSimulator\TestFolder\Tests\12-Tests\DAT3.pdf C:\KnowBe4\RsSimulator\TestFolder\Tests\12-Tests\pict11.jpg C:\KnowBe4\RsSimulator\TestFolder\Tests\12-Tests\DAT3.docx C:\KnowBe4\RsSimulator\TestFolder\Tests\12-Tests\DAT3.pptx C:\KnowBe4\RsSimulator\TestFolder\Tests\12-Tests\DATA.xlsx C:\KnowBe4\RsSimulator\TestFolder\Tests\12-Tests\docu1.docx and 16 other files

Intel TDT: Enhance fileless attack protection

Enhance protection against advanced fileless attacks using Intel GPU offloading

- Leverage Intel Threat Detection Technology (TDT) to **improve protection against polymorphic malware and fileless attacks**
- **Reduce impact on CPU performance** by offloading the advanced memory scanning (AMS) to Intel's integrated graphical controller (GPU)
- **Elevate customer's perception of Acronis** by partnering with Intel

Intel® Threat Detection Technology (Intel® TDT)
intel vPRO PLATFORM BUILT FOR BUSINESS
intel®

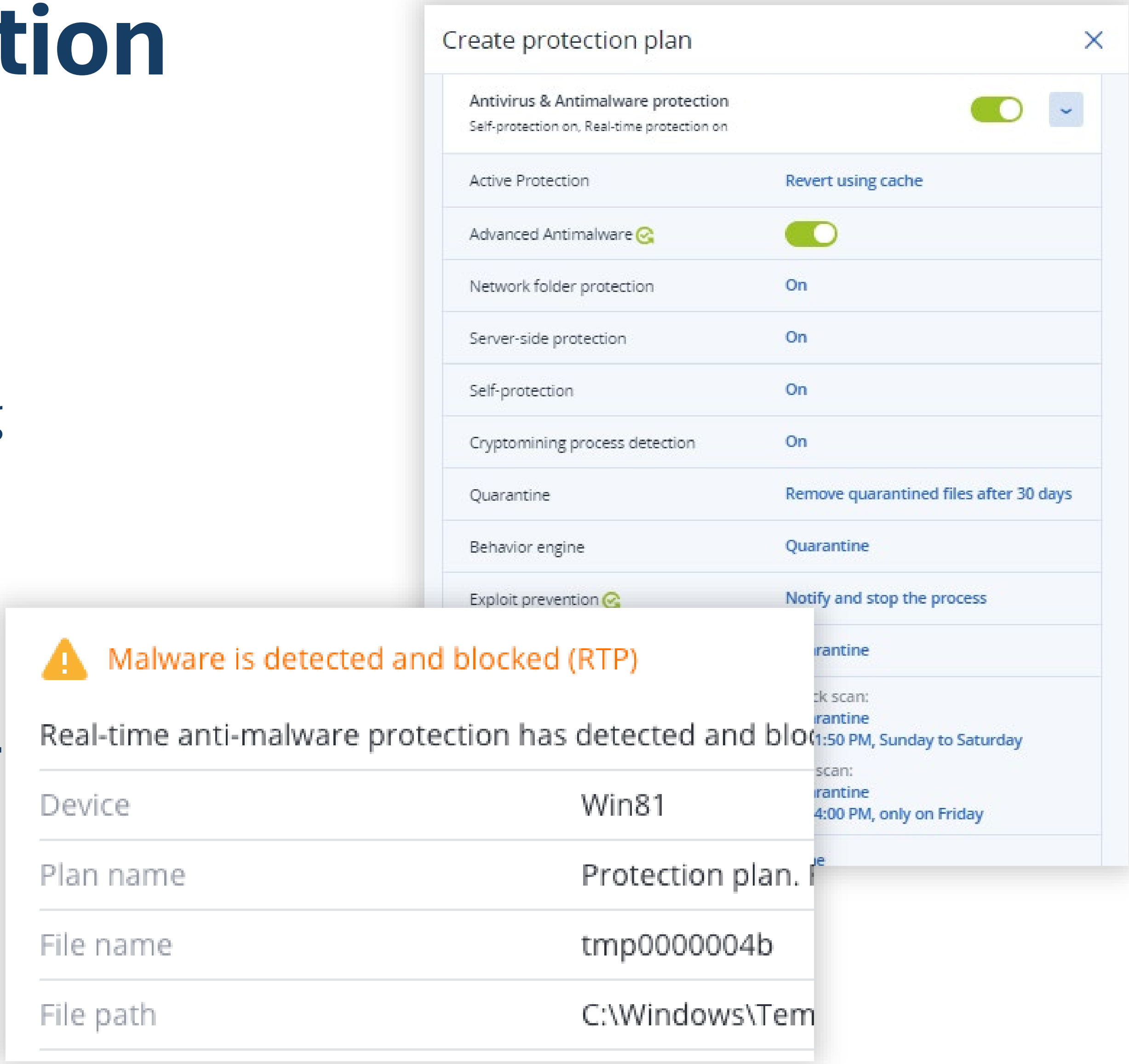
Signature-based detection

Detect and block known threats

Leverage a **database of known malware signatures** to automatically block threats.

When an agent on an endpoint detects something suspicious, it is send to the cloud for additional analysis. A **detection record** is created, which becomes available to all endpoints connected to Acronis Cloud.

Leverage local detection **even in cases with poor internet connections.**



Create protection plan

Antivirus & Antimalware protection
Self-protection on, Real-time protection on

Active Protection	Revert using cache
Advanced Antimalware	
Network folder protection	On
Server-side protection	On
Self-protection	On
Cryptomining process detection	On
Quarantine	Remove quarantined files after 30 days
Behavior engine	Quarantine
Exploit prevention	Notify and stop the process
	rantine
	ck scan: rantine 1:50 PM, Sunday to Saturday scan: rantine 4:00 PM, only on Friday
	e

Malware is detected and blocked (RTP)

Real-time anti-malware protection has detected and bloc

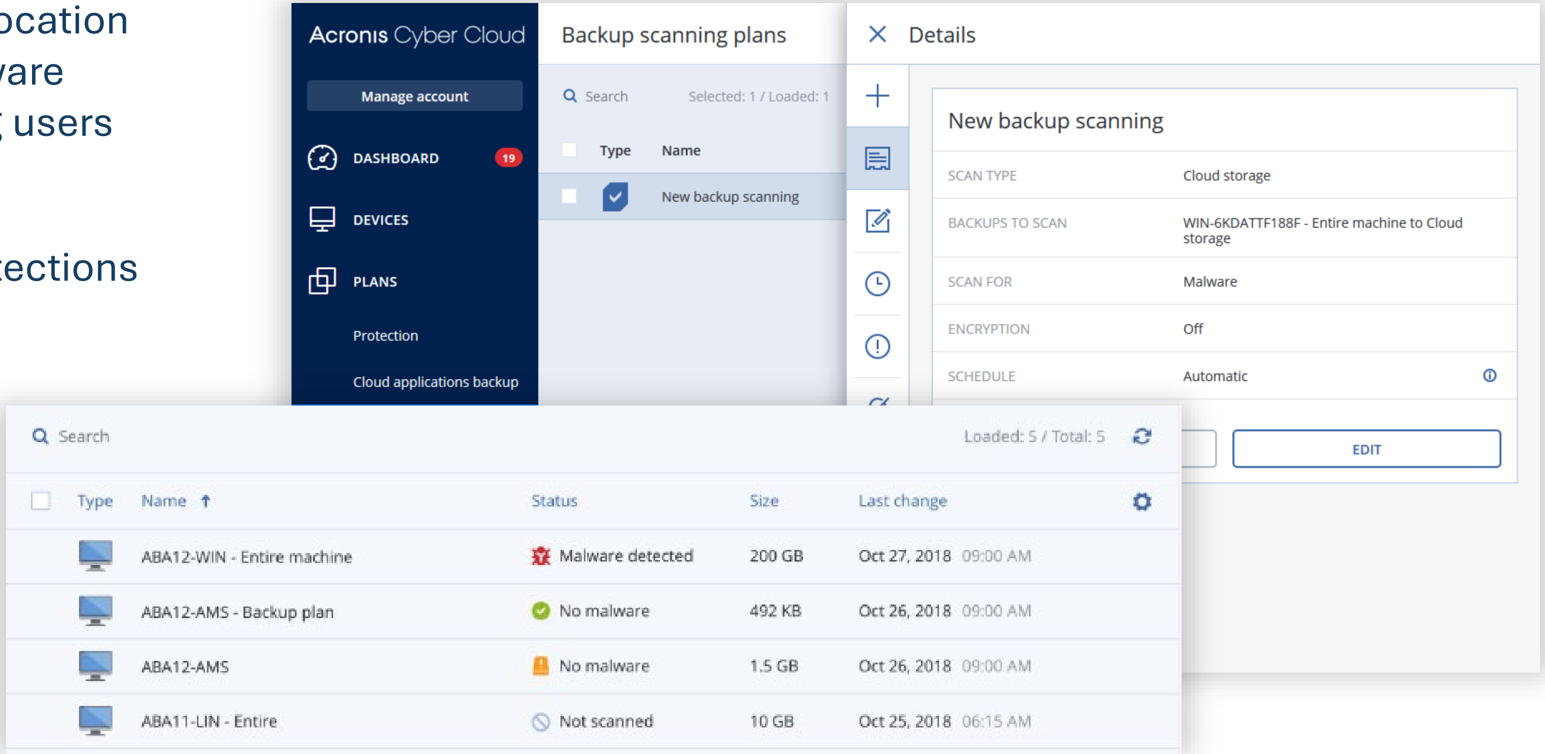
Device	Win81
Plan name	Protection plan. P
File name	tmp0000004b
File path	C:\Windows\Tem

Malware scans of backed up data in Acronis Cloud

Prevent restoring infected files from backups

Scanning full disk backups in a centralized location helps find potential vulnerabilities and malware infections, including ransomware – ensuring users restore a malware-free backup.

- Increases potential rootkit and bootkit detections
- Restores only clean data
- Reduces loads of client endpoints



New backup scanning

SCAN TYPE	Cloud storage
BACKUPS TO SCAN	WIN-6KDATTF188F - Entire machine to Cloud storage
SCAN FOR	Malware
ENCRYPTION	Off
SCHEDULE	Automatic

Type	Name ↑	Status	Size	Last change
	ABA12-WIN - Entire machine	Malware detected	200 GB	Oct 27, 2018 09:00 AM
	ABA12-AMS - Backup plan	No malware	492 KB	Oct 26, 2018 09:00 AM
	ABA12-AMS	No malware	1.5 GB	Oct 26, 2018 09:00 AM
	ABA11-LIN - Entire	Not scanned	10 GB	Oct 25, 2018 06:15 AM

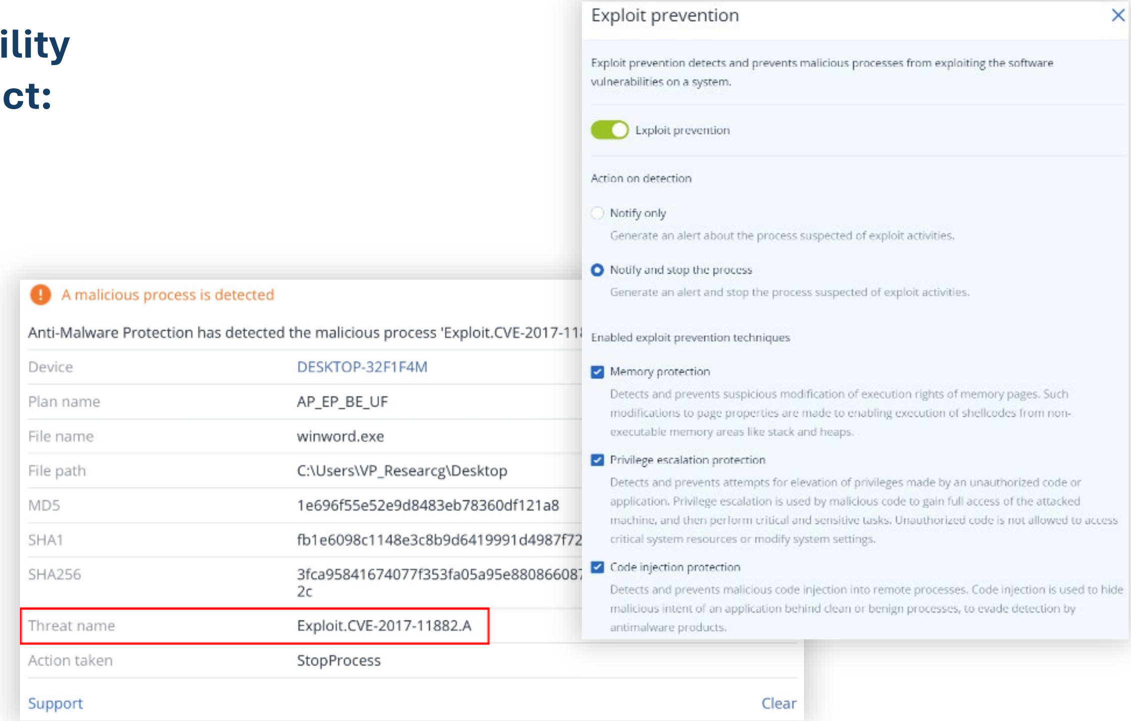
Exploit prevention & runtime protection

Stop malware that attempts to take advantage of software vulnerabilities

Use behavior-based detection heuristics, crafted with vulnerability exploitation in mind and constantly updated by Acronis, to detect:

- Token manipulation
- Stack pivot
- Memory protection (stack)
- Injection detection (Process Hollowing, Remote thread, Process hollowing, APC, Early bird, Reflective DLL)

- Minimize security risks
- Cover unknown vulnerabilities
- Prevent exploits, including memory exploits



A malicious process is detected

Anti-Malware Protection has detected the malicious process 'Exploit.CVE-2017-11

Device	DESKTOP-32F1F4M
Plan name	AP_EP_BE_UF
File name	winword.exe
File path	C:\Users\VP_Researcg\Desktop
MD5	1e696f55e52e9d8483eb78360df121a8
SHA1	fb1e6098c1148e3c8b9d6419991d4987f72
SHA256	3fca95841674077f353fa05a95e88086608 2c
Threat name	Exploit.CVE-2017-11882.A
Action taken	StopProcess

Exploit prevention

Exploit prevention detects and prevents malicious processes from exploiting the software vulnerabilities on a system.

Exploit prevention: on

Action on detection

○ Notify only

Generate an alert about the process suspected of exploit activities.

● Notify and stop the process

Generate an alert and stop the process suspected of exploit activities.

Enabled exploit prevention techniques

☑ Memory protection

Detects and prevents suspicious modification of execution rights of memory pages. Such modifications to page properties are made to enabling execution of shellcodes from non-executable memory areas like stack and heaps.

☑ Privilege escalation protection

Detects and prevents attempts for elevation of privileges made by an unauthorized code or application. Privilege escalation is used by malicious code to gain full access of the attacked machine, and then perform critical and sensitive tasks. Unauthorized code is not allowed to access critical system resources or modify system settings.

☑ Code injection protection

Detects and prevents malicious code injection into remote processes. Code injection is used to hide malicious intent of an application behind clean or benign processes, to evade detection by antimalware products.

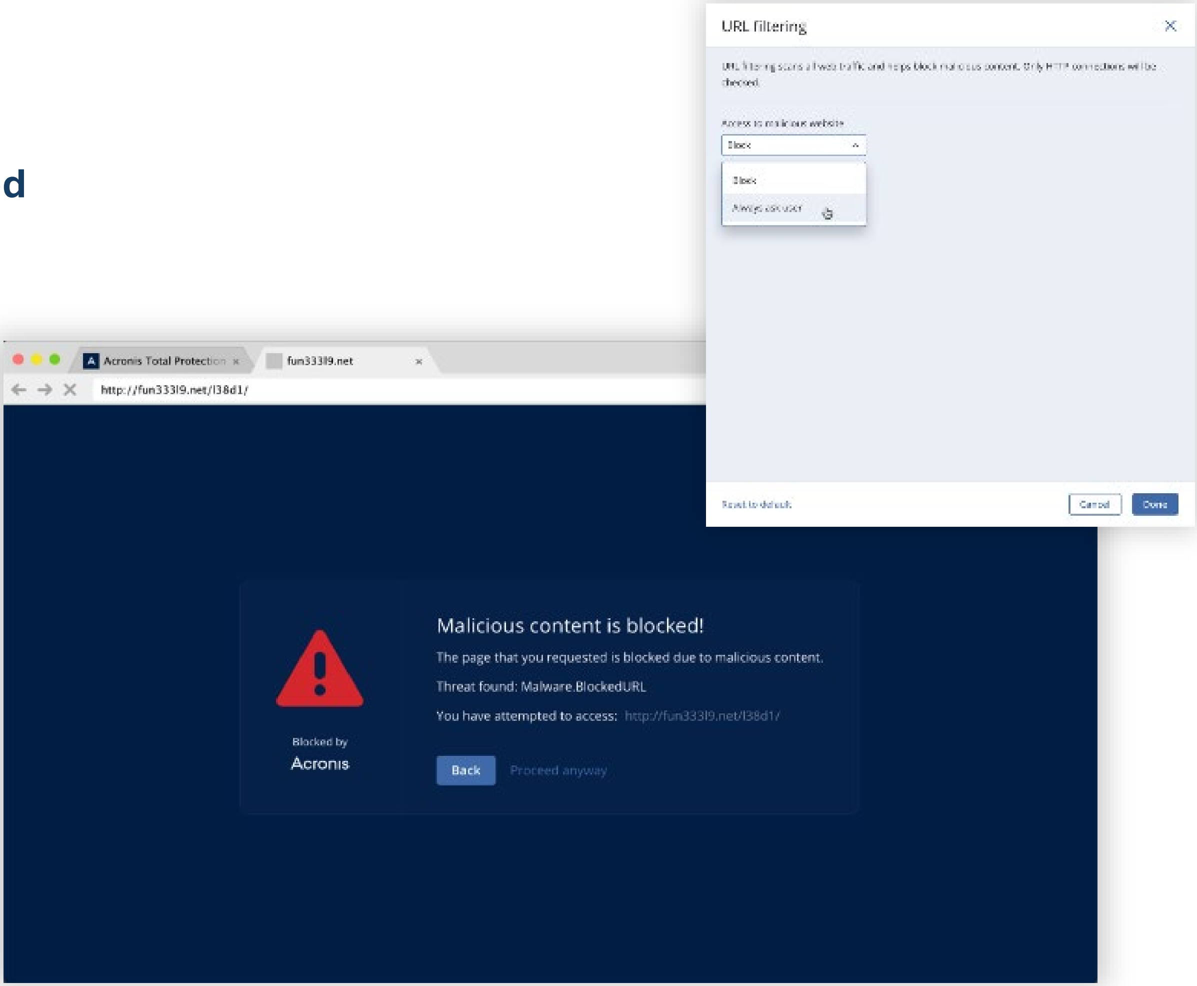
URL filtering

Monitor, control and block internet access to websites based on information contained in a URL list to block malicious or hacked URLs

- HTTP/HTTPS interceptor
- Allowlist/denylist for URLs
- Payload analysis for malicious URLs – analyzes the link and the pages structure

Acronis URL filtering list:

- Acronis own signatures
- AI-based detection
- Licensed signatures and intelligence from partners



URL filtering

URL filtering scans all web traffic and helps block malicious content. Only HTTP connections will be checked.

Access to malicious website: Block

Malicious content is blocked!

The page that you requested is blocked due to malicious content.

Threat found: Malware.BlockedURL

You have attempted to access: http://fun33319.net/l38d1/

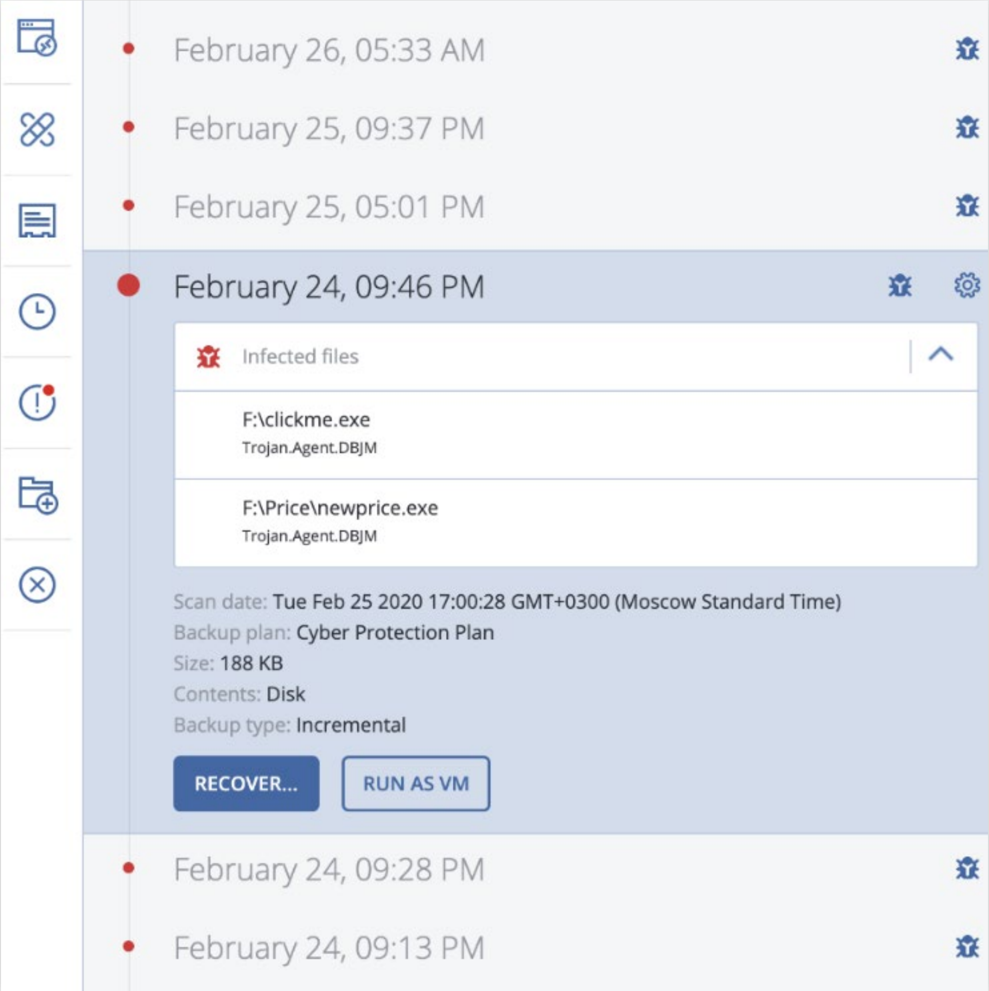
Acronis

Ransomware protection

Protect backups and endpoints from ransomware and ensure automatic rollback

Award-winning anti-ransomware technology

- Ransomware and cryptomining process detection (incl. in local backups)
- Entropy analysis to catch advanced ransomware
- Protect data in network folders
- Server-side protection: Protect the data in shared folders within your network against ransomware
- Automatic recovery of affected data within seconds



February 26, 05:33 AM

February 25, 09:37 PM

February 25, 05:01 PM

February 24, 09:46 PM

Infected files

F:\clickme.exe
Trojan.Agent.DBJM

F:\Price\newprice.exe
Trojan.Agent.DBJM

Scan date: Tue Feb 25 2020 17:00:28 GMT+0300 (Moscow Standard Time)
Backup plan: Cyber Protection Plan
Size: 188 KB
Contents: Disk
Backup type: Incremental

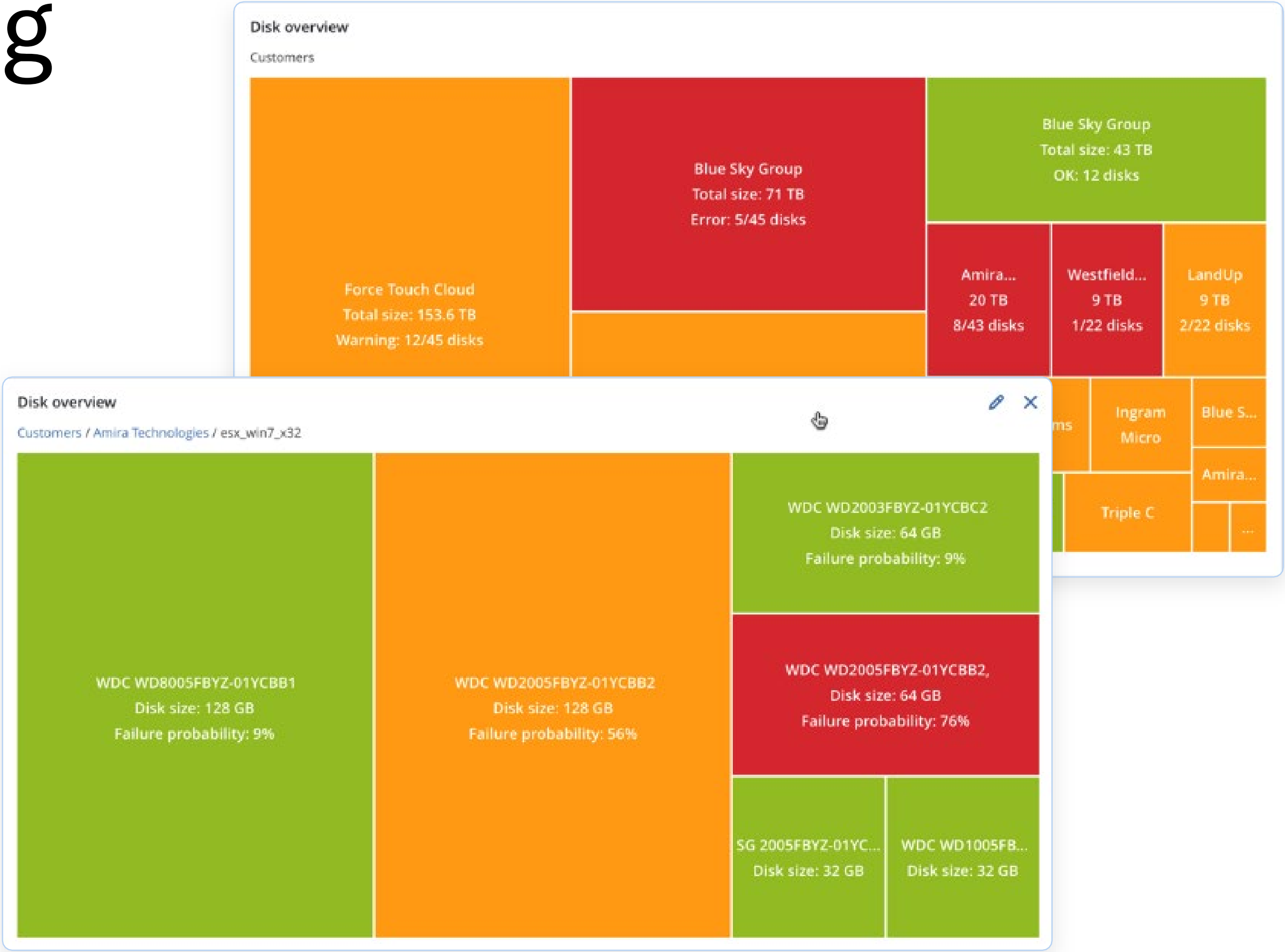
February 24, 09:28 PM

February 24, 09:13 PM

Drive health monitoring

Identify disk issues before they fail

- Uses a combination of machine learning, S.M.A.R.T. reports, drive size, vendor info, etc., to predict HDD / SSD failures
- The machine-learning model allows **98.5%** predictions accuracy (and we keep improving it)
- Once a drive alert is raised, you can take action — such as backing up critical files from the failing drive



Why? Avoid unpredictable downtime or client data loss, plan work more effectively, differentiate your services.

Acronis

ML-based monitoring and smart alerting

Mitigate operational risks and optimize monitoring effort

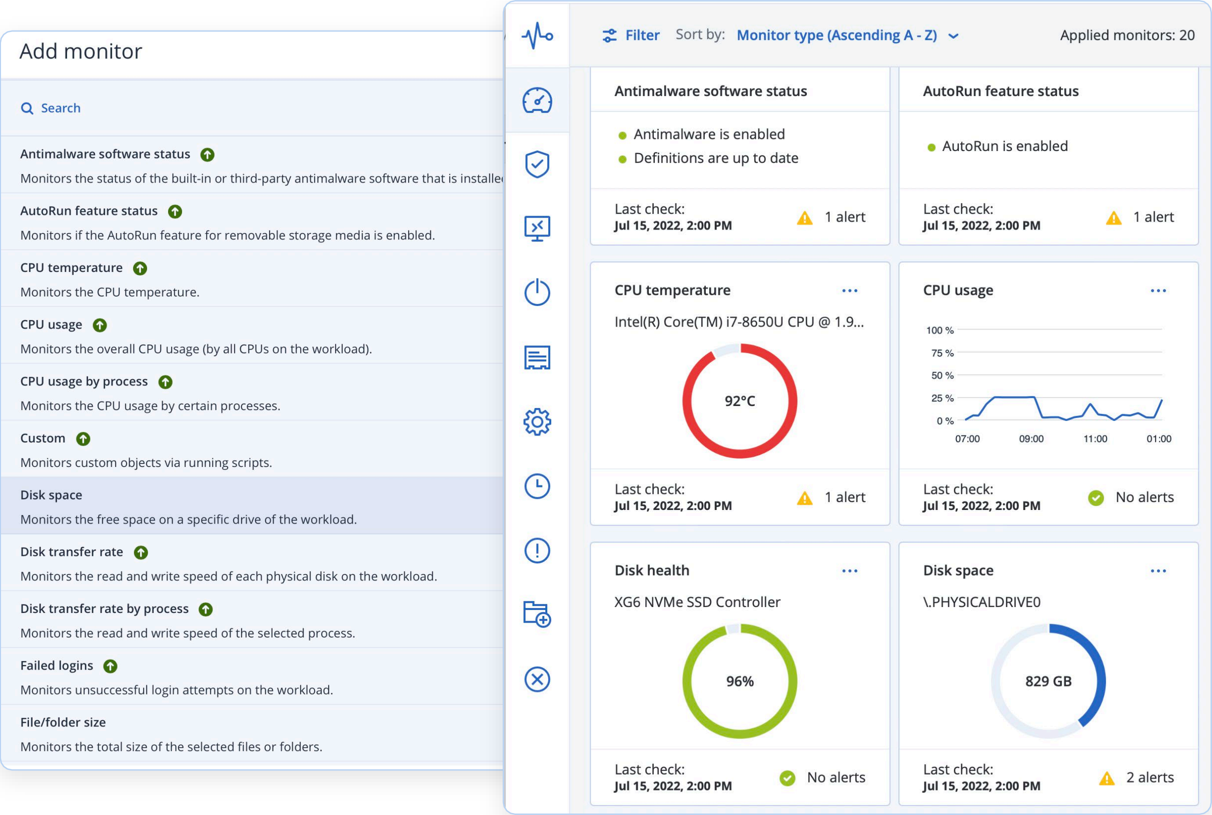
ML-based monitoring and smart alerting increase the efficiency of IT technicians with automatic, fast and precise anomaly detection with auto-response actions.

IT technicians can proactively focus on client protection, understanding machine's performance and reliability, and managing more endpoints with less effort — instead of monitoring lots of alerts, multiple consoles and complex tools.

ML-based monitoring can manage Windows and macOS machines.

Examples of typical tasks:

- Monitor the status of the built-in or third-party anti-malware software
- Monitor the read and write speed of each physical disk
- Monitor the incoming and outgoing traffic for each network adapter



Add monitor

Search

Antimalware software status
Monitors the status of the built-in or third-party antimalware software that is installe

AutoRun feature status
Monitors if the AutoRun feature for removable storage media is enabled.

CPU temperature
Monitors the CPU temperature.

CPU usage
Monitors the overall CPU usage (by all CPUs on the workload).

CPU usage by process
Monitors the CPU usage by certain processes.

Custom
Monitors custom objects via running scripts.

Disk space
Monitors the free space on a specific drive of the workload.

Disk transfer rate
Monitors the read and write speed of each physical disk on the workload.

Disk transfer rate by process
Monitors the read and write speed of the selected process.

Failed logins
Monitors unsuccessful login attempts on the workload.

File/folder size
Monitors the total size of the selected files or folders.

Filter Sort by: Monitor type (Ascending A - Z) Applied monitors: 20

Antimalware software status
- Antimalware is enabled
- Definitions are up to date

Last check: Jul 15, 2022, 2:00 PM ⚠ 1 alert

AutoRun feature status
- AutoRun is enabled

Last check: Jul 15, 2022, 2:00 PM ⚠ 1 alert

CPU temperature
Intel(R) Core(TM) i7-8650U CPU @ 1.9...
92°C
Last check: Jul 15, 2022, 2:00 PM ⚠ 1 alert

CPU usage
Last check: Jul 15, 2022, 2:00 PM ✓ No alerts

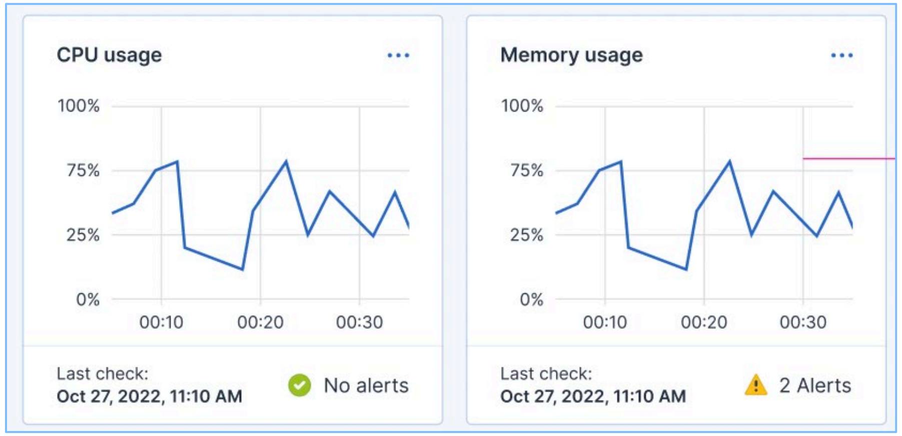
Disk health
XG6 NVMe SSD Controller
96%
Last check: Jul 15, 2022, 2:00 PM ✓ No alerts

Disk space
\.PHYSICALDRIVE0
829 GB
Last check: Jul 15, 2022, 2:00 PM ⚠ 2 alerts

Why? Partners can reduce the number of generated alerts and perform automatic remediation.

AI-Based Endpoint Monitoring & Remediation

- **Tracks key endpoint parameters:**
  - CPU, disk, memory usage
  - Anti-malware status, installed software
  - Network usage, alarm severity, alert message
  - Threshold conditions



CPU usage

Last check:
Oct 27, 2022, 11:10 AM

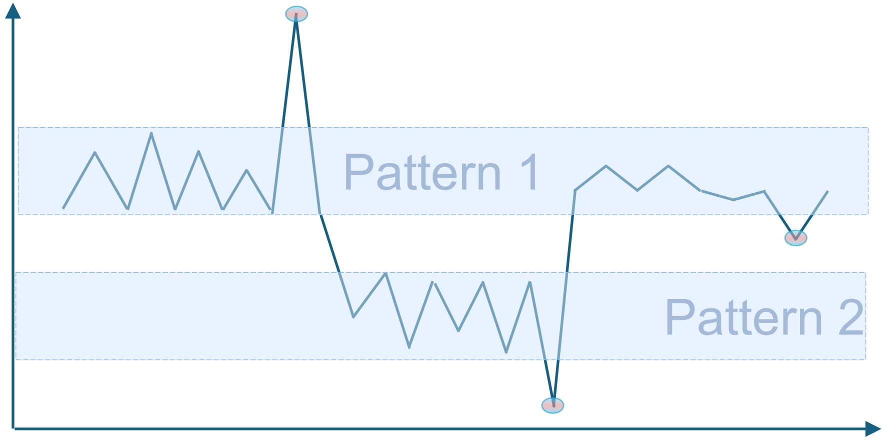
✓ No alerts

Memory usage

Last check:
Oct 27, 2022, 11:10 AM

⚠ 2 Alerts

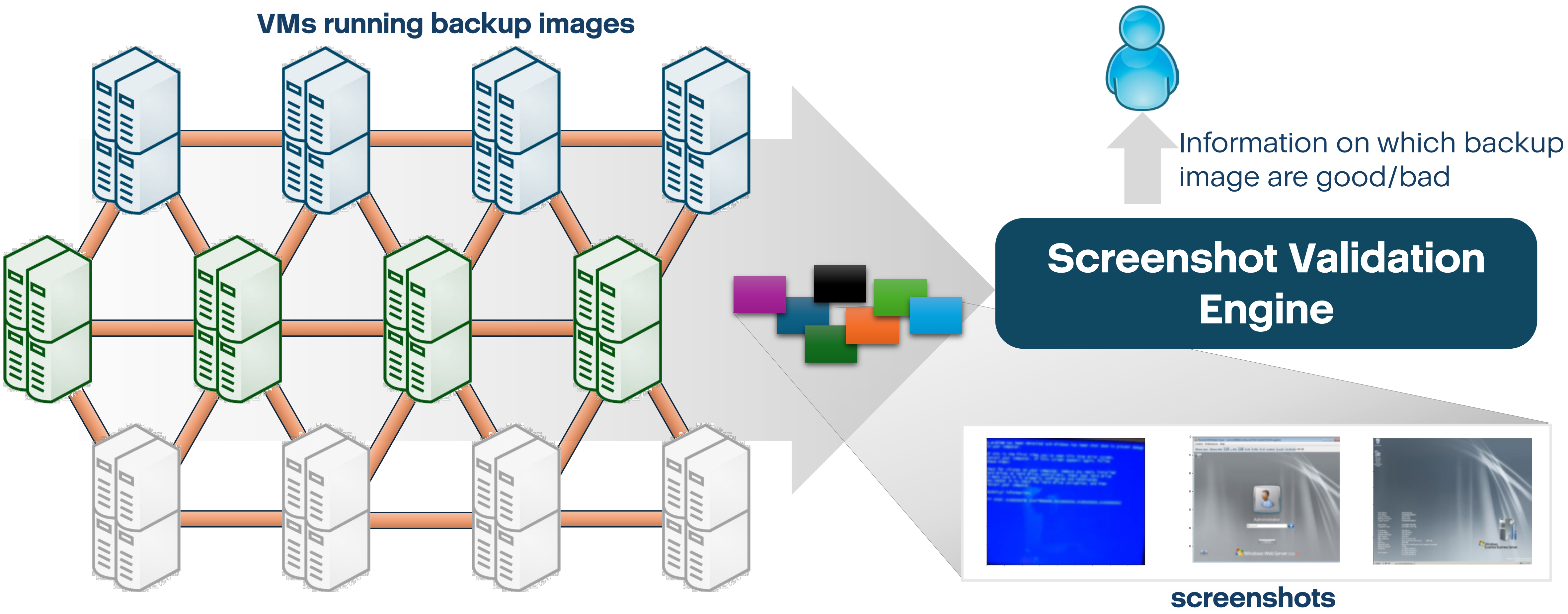
- **Proactively detects anomalies in the workload and fixes the problem automatically**
  - Hard to set specific threshold for some metrics
  - Prevents problems from affecting users.
  - User doesn't need to open a ticket
  - Technician doesn't need to diagnose the problem - applies a predefined script to address it



Screenshot Validations of VMs

Validation of OS bootability by taking screenshots of machine mounted as VM from backup

Value of AI: Detect Failed Reboot, eliminates manual inspection



VMs running backup images

Information on which backup image are good/bad

Screenshot Validation Engine

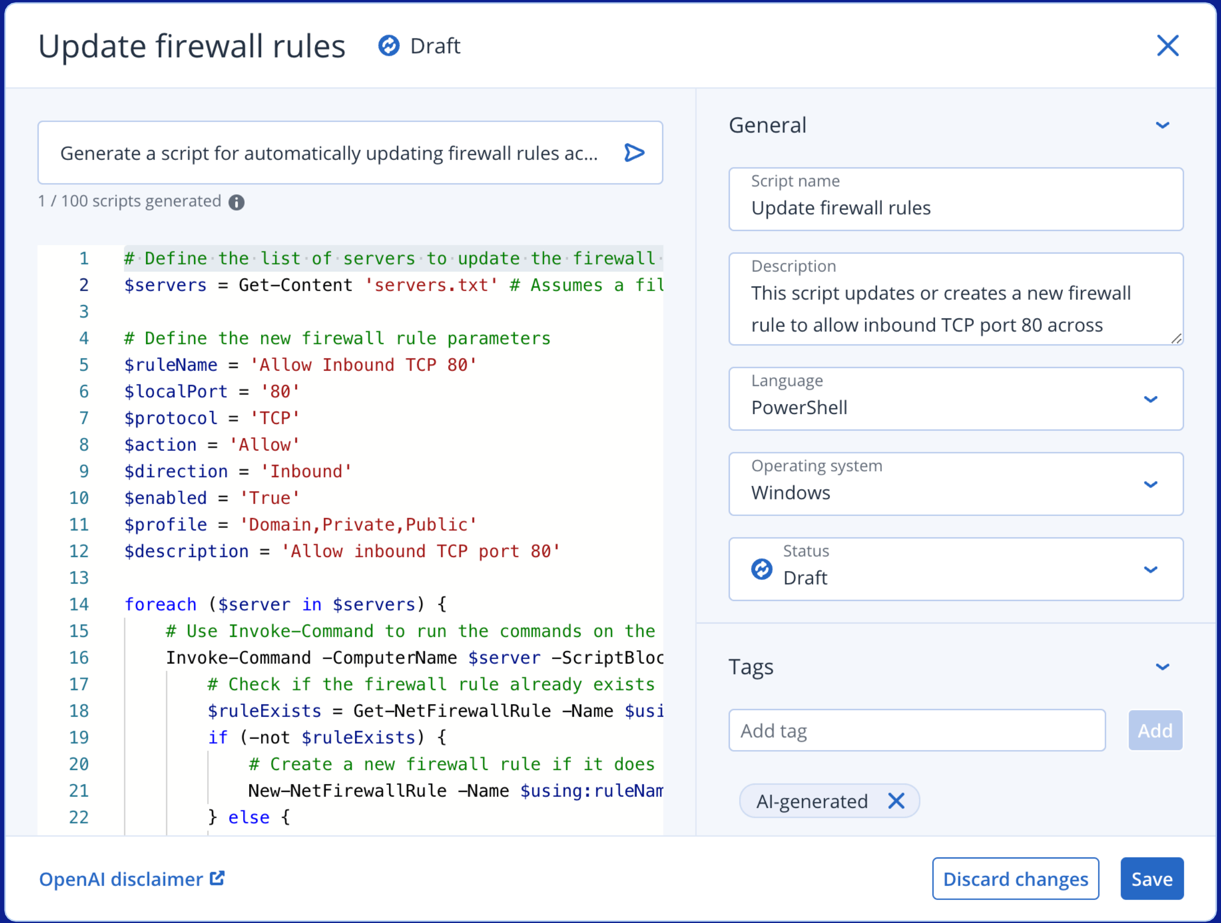
screenshots

AI-based script generation

Integrated with OpenAI to generate powerful scripts in seconds

Leverage generative AI to create powerful PowerShell and Bash scripts, enhancing efficiency and reducing human error even further.

- User-friendly interface simplifies script creation.
- Faster completion of complex tasks, such as software installations, configurations and security mitigations — reducing human error.
- Accelerate productivity while enhancing security.
- Compatible with both Windows and macOS.
- Powered by OpenAI’s GPT-4 model.



Update firewall rules Draft

Generate a script for automatically updating firewall rules ac...

1 / 100 scripts generated

```
# Define the list of servers to update the firewall
$servers = Get-Content 'servers.txt' # Assumes a fil

# Define the new firewall rule parameters
$ruleName = 'Allow Inbound TCP 80'
$localPort = '80'
$protocol = 'TCP'
$action = 'Allow'
$direction = 'Inbound'
$enabled = 'True'
$profile = 'Domain,Private,Public'
$description = 'Allow inbound TCP port 80'

foreach ($server in $servers) {
    # Use Invoke-Command to run the commands on the
    Invoke-Command -ComputerName $server -ScriptBloc
        # Check if the firewall rule already exists
        $ruleExists = Get-NetFirewallRule -Name $usi
        if (-not $ruleExists) {
            # Create a new firewall rule if it does
            New-NetFirewallRule -Name $using:ruleNam
        } else {
```

General

Script name: Update firewall rules

Description: This script updates or creates a new firewall rule to allow inbound TCP port 80 across

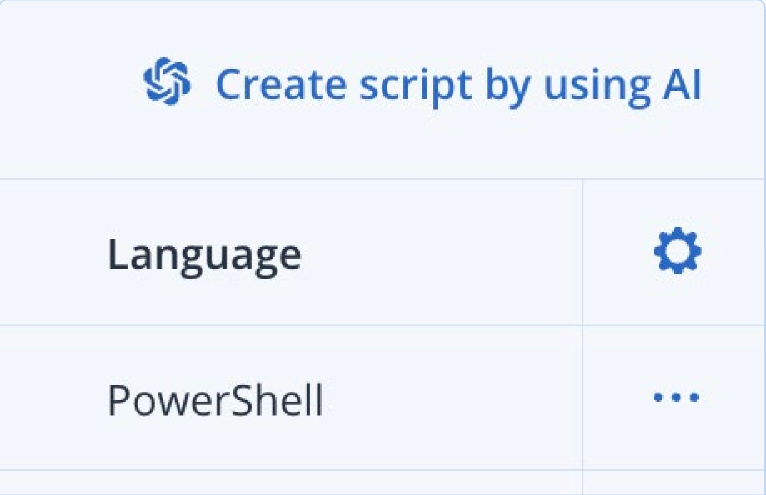
Language: PowerShell

Operating system: Windows

Status: Draft

Tags

AI-based scripting

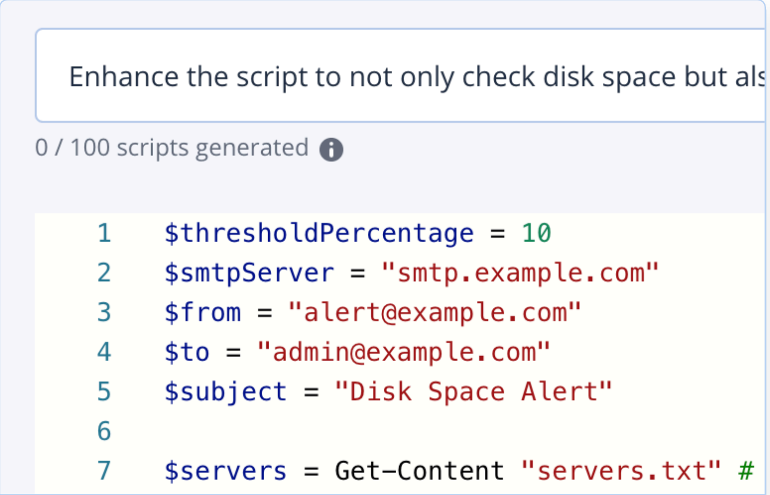


Language

PowerShell

AI-powered script generation

Intuitive interface caters to all levels of technical expertise. Users can input a set of instructions, and the AI generates a custom script tailored to those requirements.



Enhance the script to not only check disk space but als

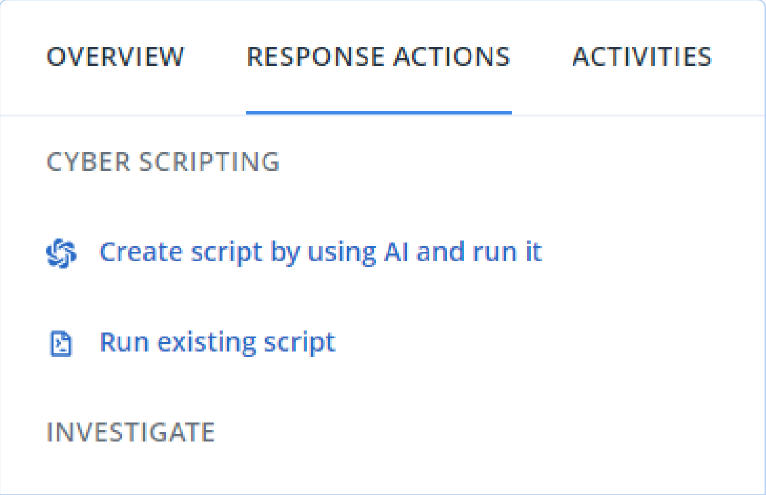
0 / 100 scripts generated

```
$thresholdPercentage = 10
$smtpServer = "smtp.example.com"
$from = "alert@example.com"
$to = "admin@example.com"
$subject = "Disk Space Alert"

$servers = Get-Content "servers.txt" #
```

Pre-existing script enhancements

For more complex requirements, where partial scripts already exist, it completes these scripts according to prompt instructions. Additionally, includes in-line comments for accurate script translation.



Integration with Advanced Security + EDR

In the event of a security incident, technicians can swiftly generate scripts via AI right from the Advanced Security + EDR console to take immediate mitigation actions.

Meet multiple cyber insurance & compliance requirements with a single platform

99% of insurance claims come from small & medium businesses

What cyber insurers expect of insured entities:

- Stringent policies around authentication (MFA) and authorization (least privilege management) Deliver with Acronis
- Vulnerability assessment and patch management Deliver with Acronis
- Behavioral anti-malware Deliver with Acronis
- EDR Deliver with Acronis
- Programmatic backup and a DR plan Deliver with Acronis
- Incident response plan Deliver with Acronis
- Encryption of sensitive data Encryption of backups
- Security awareness training Deliver with Acronis

How Acronis helps organizations comply with regulations:

- Protection of sensitive data against loss & leakage
- Storage of sensitive data within compliant geo locations
- Comprehensive visibility across incidents – analyze & report with ease and confidence
- Immutable backups & Disaster recovery

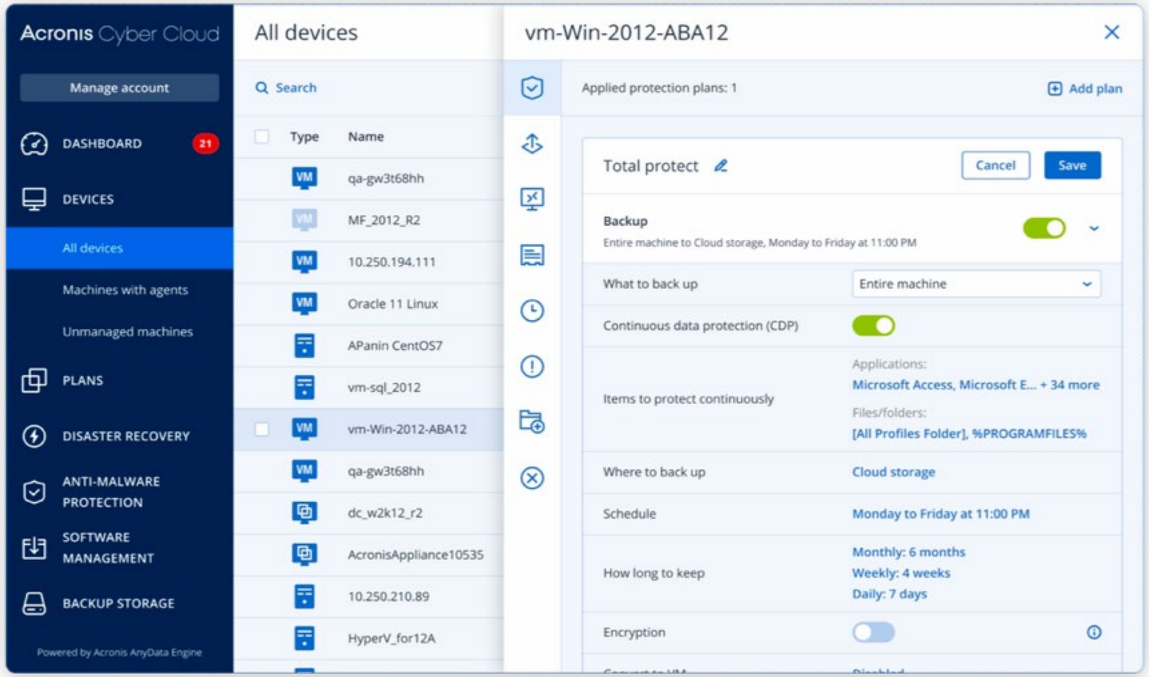
Sources: NetDiligence reports, 2023

And this is how simple it is

And this is how simple it is

Advanced technology that's simple to deploy and manage

An integrated interface allows SPs to deploy Backup, DR, Security and IT Management functionality with just **one click**.



Type	Name
VM	qa-gw3t68hh
VM	MF_2012_R2
VM	10.250.194.111
VM	Oracle 11 Linux
	APanin CentOS7
	vm-sql_2012
VM	vm-Win-2012-ABA12
VM	qa-gw3t68hh
	dc_w2k12_r2
	AcronisAppliance10535
	10.250.210.89
	HyperV_for12A

vm-Win-2012-ABA12

Applied protection plans: 1

Total protect

Backup
Entire machine to Cloud storage, Monday to Friday at 11:00 PM

What to back up: Entire machine

Continuous data protection (CDP)

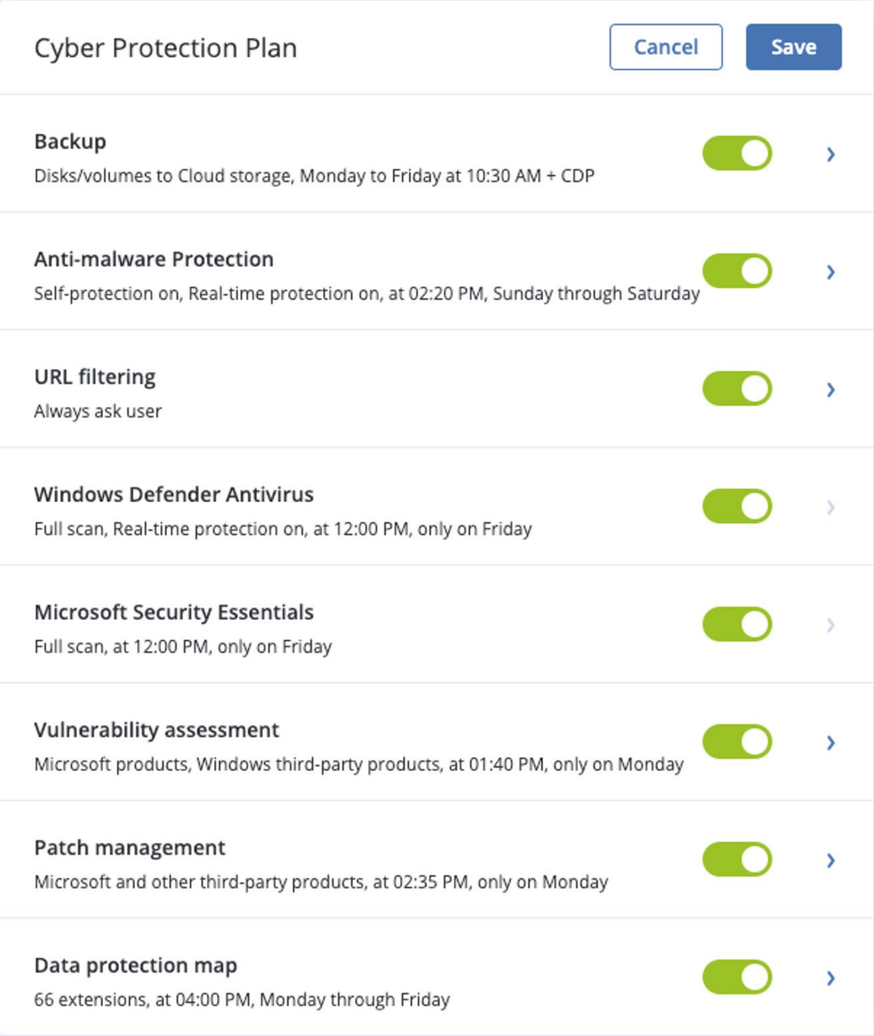
Items to protect continuously: Applications: Microsoft Access, Microsoft E... + 34 more; Files/folders: [All Profiles Folder], %PROGRAMFILES%

Where to back up: Cloud storage

Schedule: Monday to Friday at 11:00 PM

How long to keep: Monthly: 6 months; Weekly: 4 weeks; Daily: 7 days

Encryption



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, only on Friday

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

Vulnerability assessment
Microsoft products, Windows third-party products, at 01:40 PM, only on Monday

Patch management
Microsoft and other third-party products, at 02:35 PM, only on Monday

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

Acronis

Protection for 30+ workload types from a single console

Microsoft

- Azure
- Windows Server
- Windows PC
- Exchange
- SQL Server
- Share Point
- Active Directory
- Hyper-V
- Microsoft 365
- Google Workspace

- Amazon EC2
- Linux Server
- Mac
- iPhone
- iPad
- Android
- SAP HANA
- MariaDB
- MySQL

- VMware vSphere
- Oracle x86 VM Server
- Oracle Database
- Red Hat Virtualization
- Linux KVM
- Citrix XenServer
- Virtuozzo
- Nutanix
- Synology

Streamline delivery of cyber protection using just one solution

Acronis

Flexible storage options

Meet data sovereignty or cost requirements

Cloud storage

Google Cloud Platform

Acronis Cyber Cloud Storage

Azure

Three turnkey cloud storage options

Alibaba Cloud

aws

IBM Cloud

IIJ

wasabi

Other public clouds *(via Acronis Backup Gateway)*

Your own or third-party cloud storage

On-premises storage

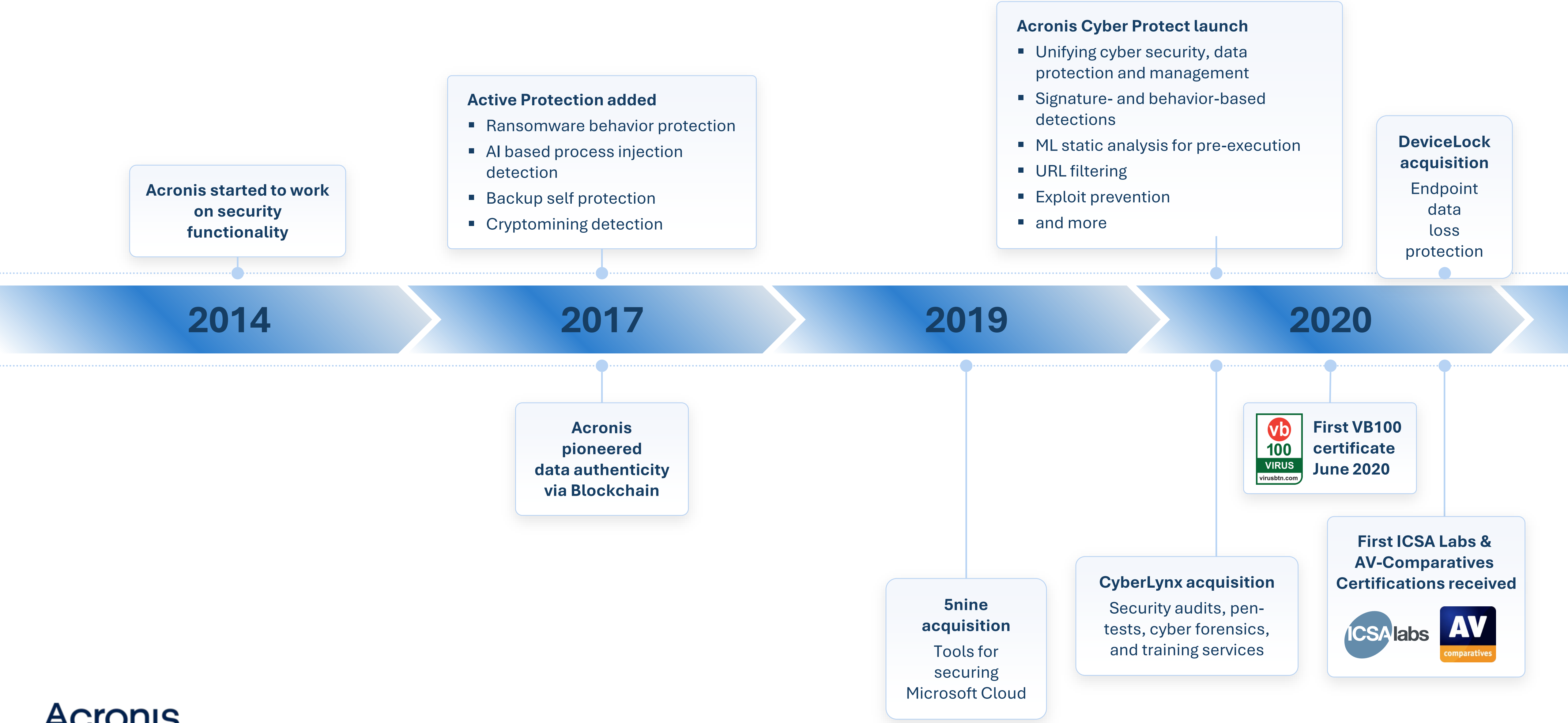
Local disks

SMB/CIFS/DFS and NFS shares

On-premises Acronis Storage

> Other solutions shoehorned us into a situation where we had to tell our customers they couldn’t do certain things. **With Acronis we have complete flexibility**, and this allows us to offer the best user experience.
>
> **Jason Amato,**
> Marketing Manager at
> Centorrino Technologies

Acronis cybersecurity evolution



2014

Acronis started to work on security functionality

2017

Active Protection added

- Ransomware behavior protection
- AI based process injection detection
- Backup self protection
- Cryptomining detection

Acronis pioneered data authenticity via Blockchain

2019

5nine acquisition

Tools for securing Microsoft Cloud

Acronis Cyber Protect launch

- Unifying cyber security, data protection and management
- Signature- and behavior-based detections
- ML static analysis for pre-execution
- URL filtering
- Exploit prevention
- and more

CyberLynx acquisition

Security audits, pen-tests, cyber forensics, and training services

2020

DeviceLock acquisition

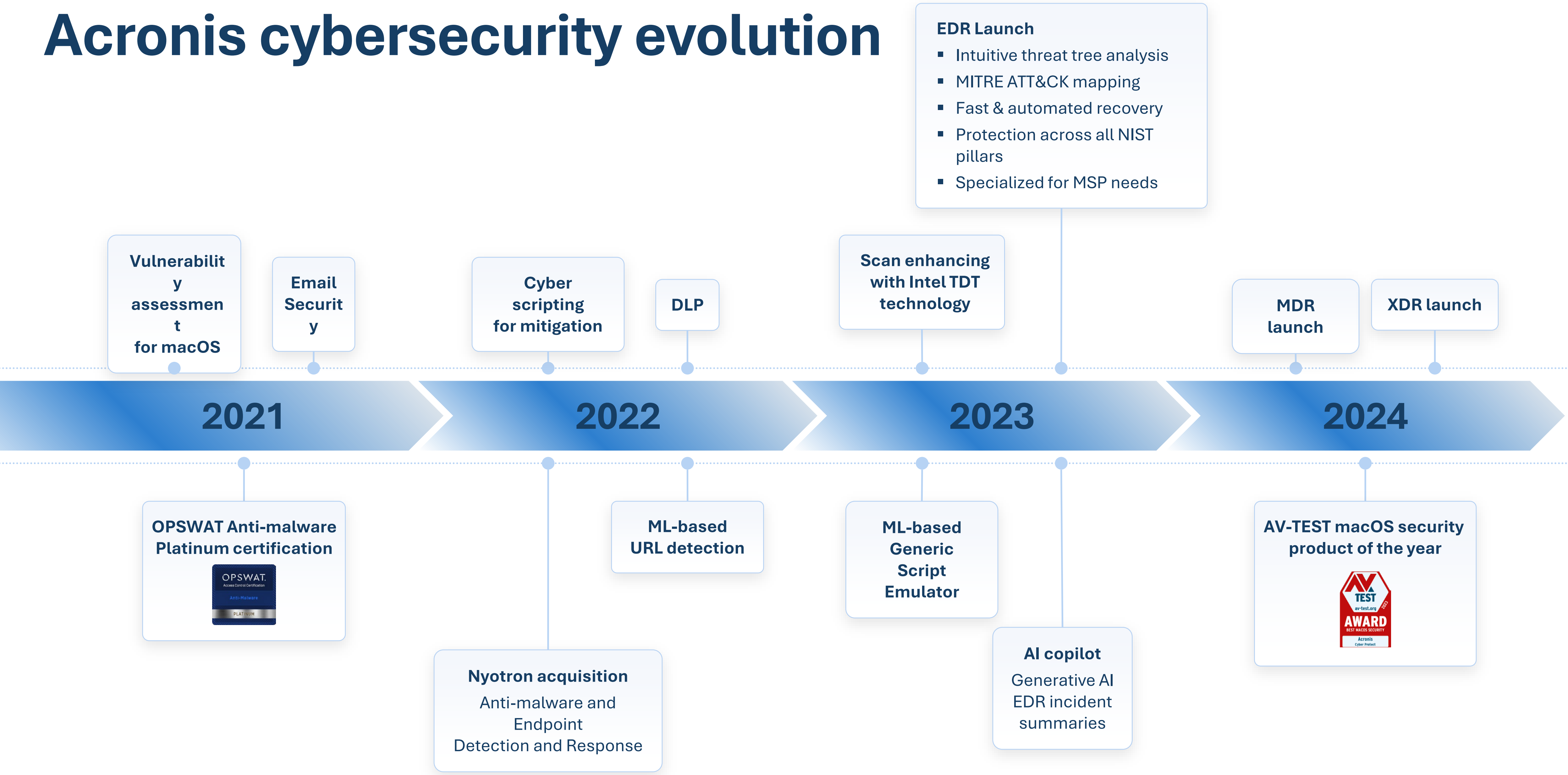
Endpoint data loss protection

First VB100 certificate June 2020

First ICSA Labs & AV-Comparatives Certifications received

Acronis

Acronis cybersecurity evolution



2021

- Vulnerability assessment for macOS
- Email Security
- OPSWAT Anti-malware Platinum certification

2022

- Cyber scripting for mitigation
- DLP
- Nyotron acquisition
  Anti-malware and Endpoint Detection and Response
- ML-based URL detection

2023

- Scan enhancing with Intel TDT technology
- EDR Launch
  - Intuitive threat tree analysis
  - MITRE ATT&CK mapping
  - Fast & automated recovery
  - Protection across all NIST pillars
  - Specialized for MSP needs
- ML-based Generic Script Emulator
- AI copilot
  Generative AI EDR incident summaries

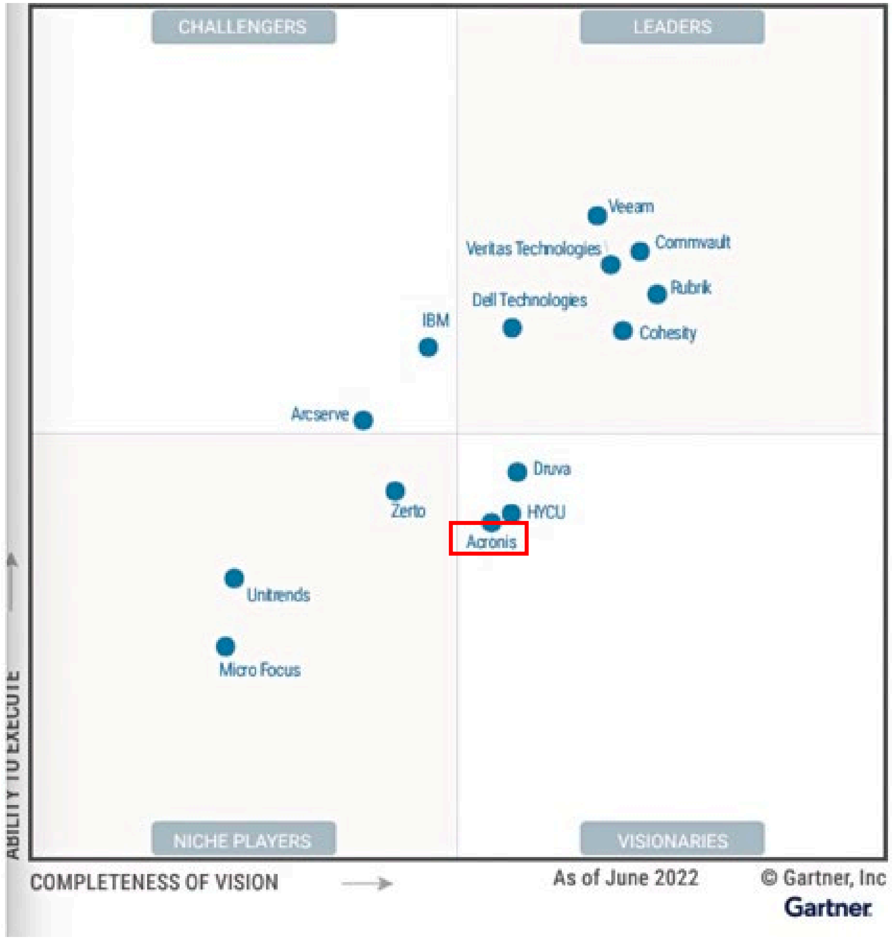
2024

- MDR launch
- XDR launch
- AV-TEST macOS security product of the year

Gartner: Visionary Leader in Cyber Protection

Acronis named Visionary in 2022 Gartner Magic Quadrant

- Acronis is recognized by Gartner **as a leader in cyber protection**.
- Acronis' platform **addresses challenges of separate security systems**.
- **A unified security approach is key** for partners selling Acronis solutions.



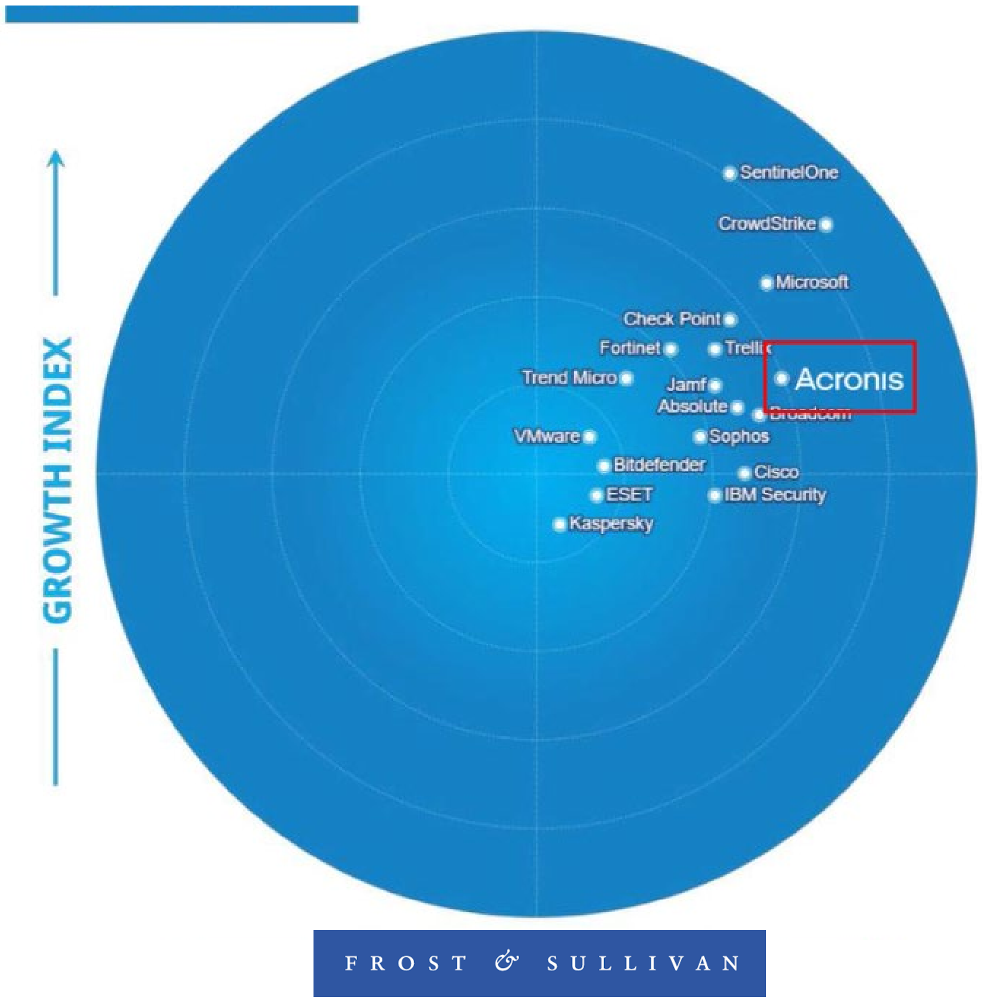
Gartner

Acronis

Frost & Sullivan: Leader in EPP/EDR Innovation

Frost & Sullivan EPP/EDR report named Acronis as a leader in 2023

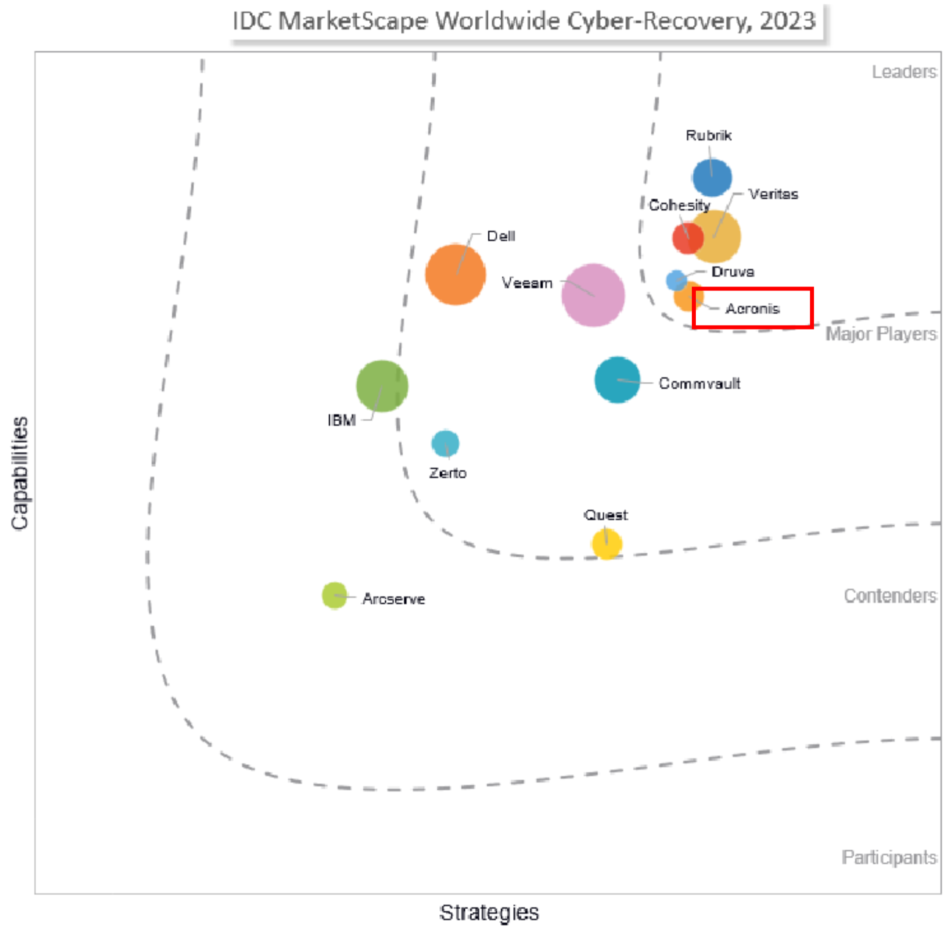
- **Acronis named a Leader** in the 2023 EPP/EDR report by Frost & Sullivan.
- **Positioned as a top innovator** in endpoint security.
- **Traditional MSP platform vendors not included** in this evaluation.



IDC: Leader in Cyber Recovery, Aligns with NIST

IDC MarketScape report 2023 named Acronis as a leader on Cyber Recovery

- **IDC aligns with Acronis' Cyber Protection approach,** emphasizing the NIST framework.
- **IDC excludes traditional MSP platform vendors** from its evaluation, highlighting specialized solutions.
- According to IDC, **Acronis meets MSPs' needs for comprehensive cyber protection** and recovery.
- IDC notes the **simplicity in implementing and managing Acronis solutions**, beneficial for MSPs.
- **Acronis's robust global infrastructure and unique technology** for data protection are recognized by IDC.
- Report acknowledges **Acronis's data classification capabilities**, supporting compliance with GDPR, HIPAA, and PII.



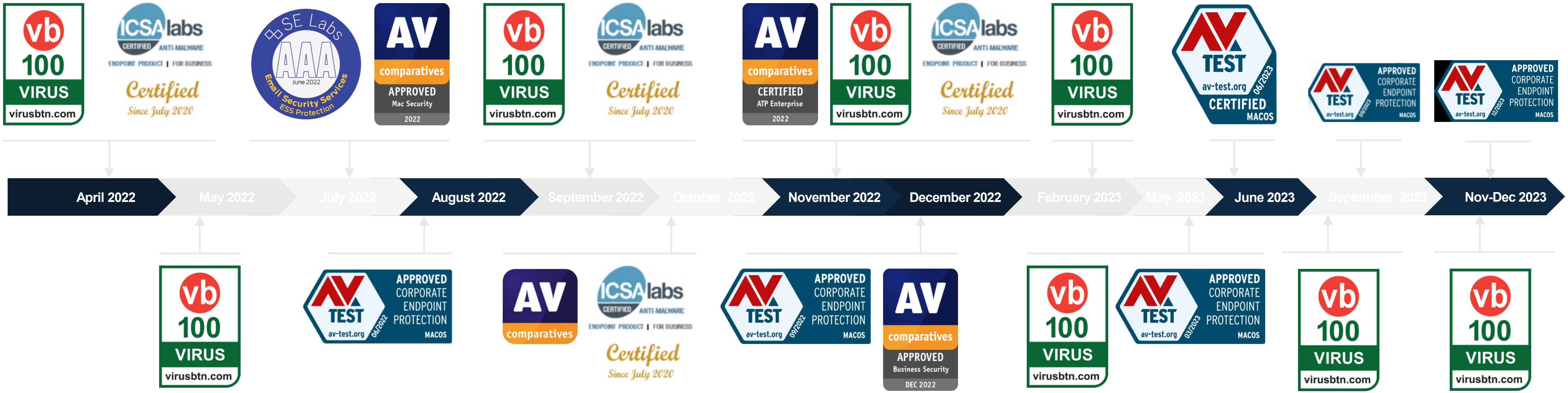
IDC MarketScape Worldwide Cyber-Recovery, 2023

G2: #2 Ranking in Email Security

- **Acronis ranked #2** out of 82 in G2's email security category, ahead of major competitors.
- G2 reviews praise Acronis for **superior functionality over competitors**.
- **Over 350 positive**, mostly 5-star, reviews highlight the effectiveness of Acronis email security.
- **Real-world user endorsements** are invaluable for partners promoting Acronis.

Proven by the security experts

Tests, certifications, alliances and memberships

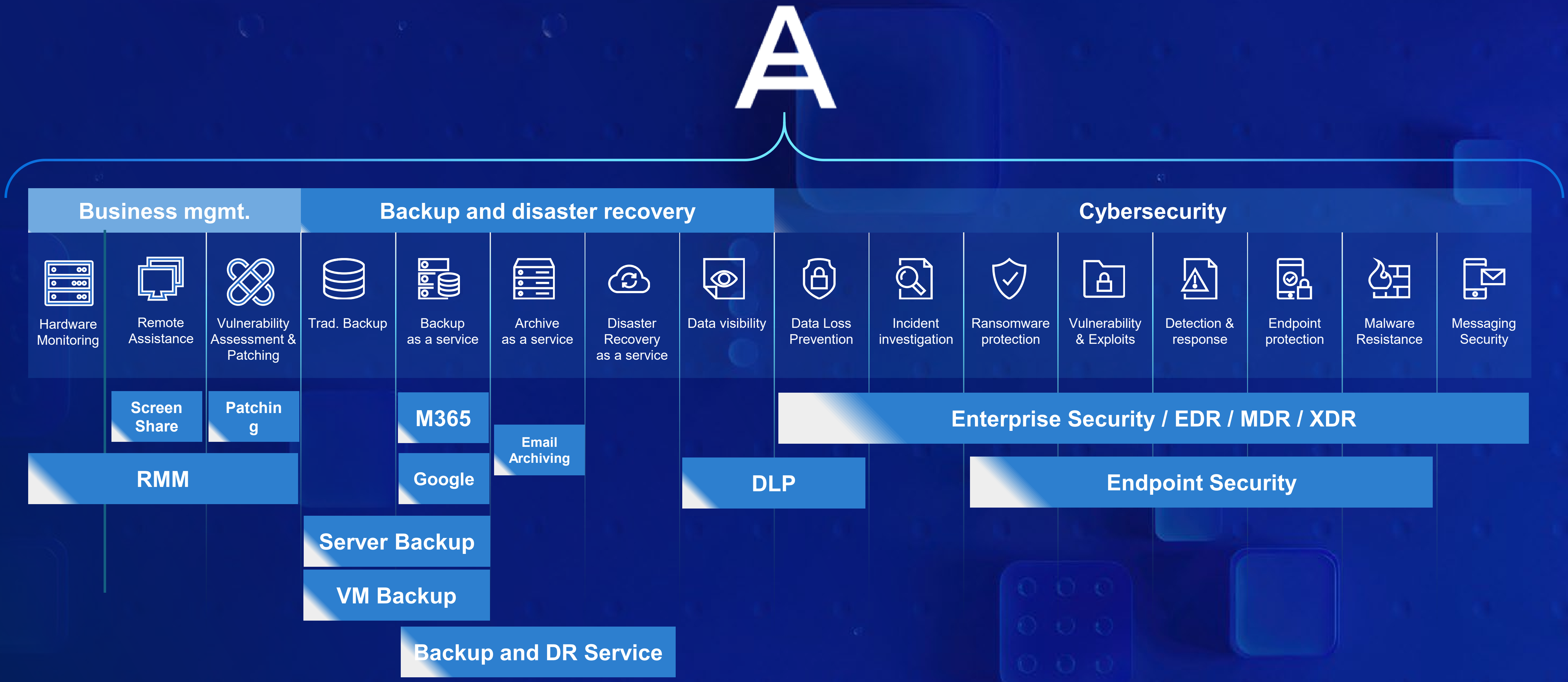


April 2022 · May 2022 · July 2022 · August 2022 · September 2022 · October 2022 · November 2022 · December 2022 · February 2023 · May 2023 · June 2023 · September 2023 · Nov-Dec 2023

vb 100 VIRUS virusbtn.com
ICSA labs CERTIFIED ANTI-MALWARE ENDPOINT PRODUCT | FOR BUSINESS Certified Since July 2020
SE Labs AAA June 2022 Email Security Services ESS Protection
AV comparatives APPROVED Mac Security 2022
AV comparatives CERTIFIED ATP Enterprise 2022
AV TEST av-test.org 06/2023 CERTIFIED MACOS
AV TEST av-test.org 09/2023 APPROVED CORPORATE ENDPOINT PROTECTION MACOS
AV TEST av-test.org 12/2023 APPROVED CORPORATE ENDPOINT PROTECTION MACOS
AV TEST av-test.org 06/2022 APPROVED CORPORATE ENDPOINT PROTECTION MACOS
AV comparatives
AV TEST av-test.org 09/2022 APPROVED CORPORATE ENDPOINT PROTECTION MACOS
AV comparatives APPROVED Business Security DEC 2022
AV TEST av-test.org 03/2023 APPROVED CORPORATE ENDPOINT PROTECTION MACOS

Acronis

Security and Data Protection in one place!



Business mgmt.

Backup and disaster recovery

Cybersecurity

Hardware Monitoring

Remote Assistance

Vulnerability Assessment & Patching

Trad. Backup

Backup as a service

Archive as a service

Disaster Recovery as a service

Data visibility

Data Loss Prevention

Incident investigation

Ransomware protection

Vulnerability & Exploits

Detection & response

Endpoint protection

Malware Resistance

Messaging Security

Screen Share

Patchin g

RMM

M365

Google

Email Archiving

Server Backup

VM Backup

Backup and DR Service

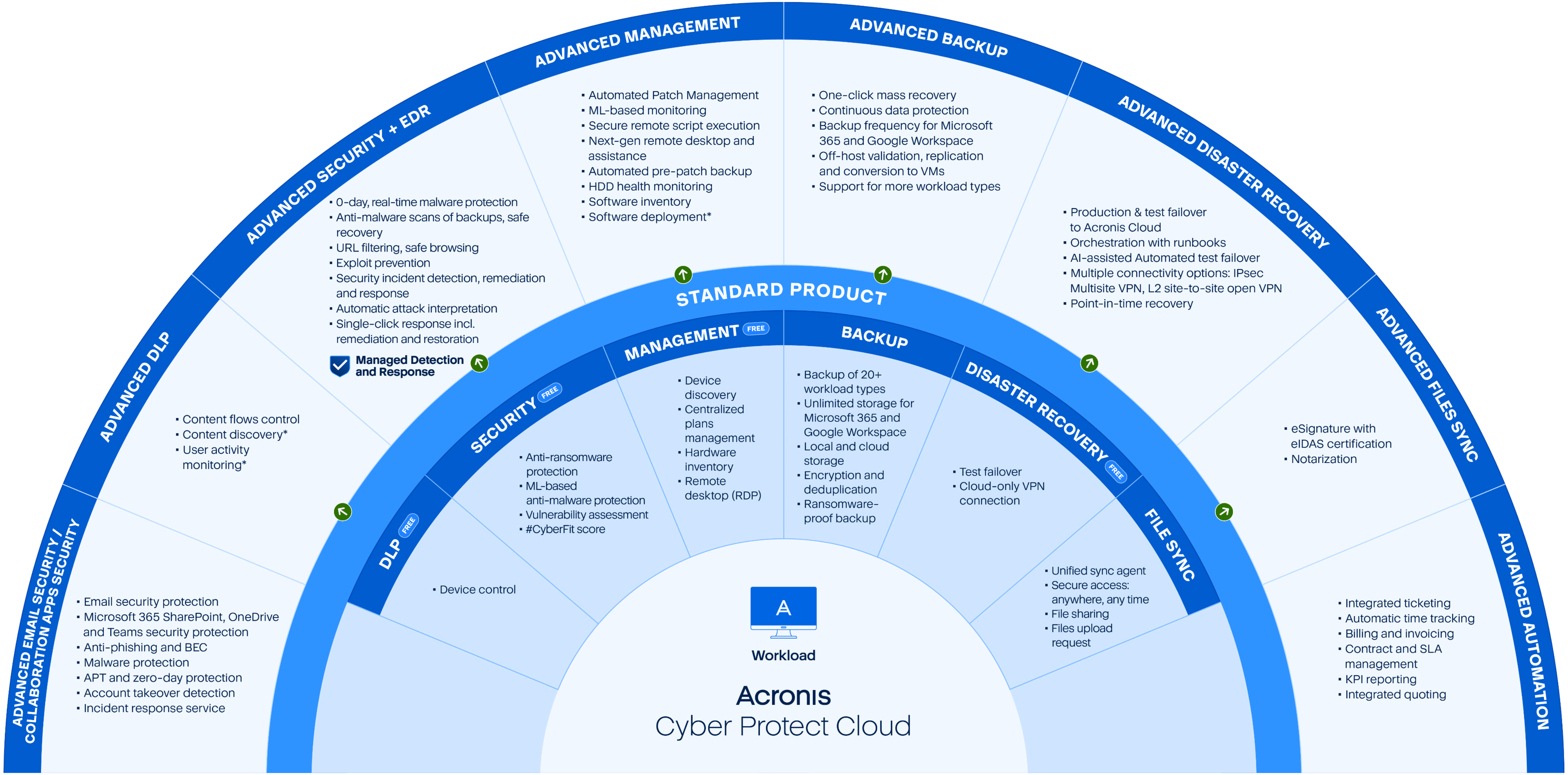
DLP

Enterprise Security / EDR / MDR / XDR

Endpoint Security

Acronis

Source: Gartner, IDC, McKinsey Cyber Market Map



ADVANCED EMAIL SECURITY / COLLABORATION APPS SECURITY

- Email security protection
- Microsoft 365 SharePoint, OneDrive and Teams security protection
- Anti-phishing and BEC
- Malware protection
- APT and zero-day protection
- Account takeover detection
- Incident response service

ADVANCED DLP

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

ADVANCED SECURITY + EDR

- 0-day, real-time malware protection
- Anti-malware scans of backups, safe recovery
- URL filtering, safe browsing
- Exploit prevention
- Security incident detection, remediation and response
- Automatic attack interpretation
- Single-click response incl. remediation and restoration

Managed Detection and Response

ADVANCED MANAGEMENT

- Automated Patch Management
- ML-based monitoring
- Secure remote script execution
- Next-gen remote desktop and assistance
- Automated pre-patch backup
- HDD health monitoring
- Software inventory
- Software deployment*

ADVANCED BACKUP

- One-click mass recovery
- Continuous data protection
- Backup frequency for Microsoft 365 and Google Workspace
- Off-host validation, replication and conversion to VMs
- Support for more workload types

ADVANCED DISASTER RECOVERY

- Production & test failover to Acronis Cloud
- Orchestration with runbooks
- AI-assisted Automated test failover
- Multiple connectivity options: IPsec Multisite VPN, L2 site-to-site open VPN
- Point-in-time recovery

ADVANCED FILES SYNC

- eSignature with eIDAS certification
- Notarization

ADVANCED AUTOMATION

- Integrated ticketing
- Automatic time tracking
- Billing and invoicing
- Contract and SLA management
- KPI reporting
- Integrated quoting

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

- Backup of 20+ workload types
- Unlimited storage for Microsoft 365 and Google Workspace
- Local and cloud storage
- Encryption and deduplication
- Ransomware-proof backup

DISASTER RECOVERY FREE

- Test failover
- Cloud-only VPN connection

FILE SYNC

- Unified sync agent
- Secure access: anywhere, any time
- File sharing
- Files upload request

Acronis Cyber Protect Cloud

Optimize for every workload

Rapidly launch services

Consolidate Solution

Acronis

Acronis

Cyber Foundation

Program

Transforming lives through education

Let's work together to create new knowledge, putting our diverse experiences and strengths towards a brighter future!

Join us!