MANAGED ENDPOINT DETECTION & RESPONSE

DIGITAL Trust.
Mastering business security

PROTECTING THE ENDPOINT

ARE TRADITIONAL AV SOLUTIONS STILL EFFECTIVE?

NEW CHALLENGES

- Vendor update lists are often large and unwieldy. Not all updates can be pushed out, some end up being missed.
- Traditional AV solutions are reliant on deployment to an endpoint, if the endpoint is not under management, an update cannot be deployed
- Traditional pattern-based approach to identify malware is often unable to manage variation and complexity of more sophisticated Malware.
- If traditional AV doesn’t detect malware it can’t report it.
- Heuristic static analysis employed by traditional AV is vendor specific so can miss new malware if not on vendor radar.

RETAINED BENEFITS

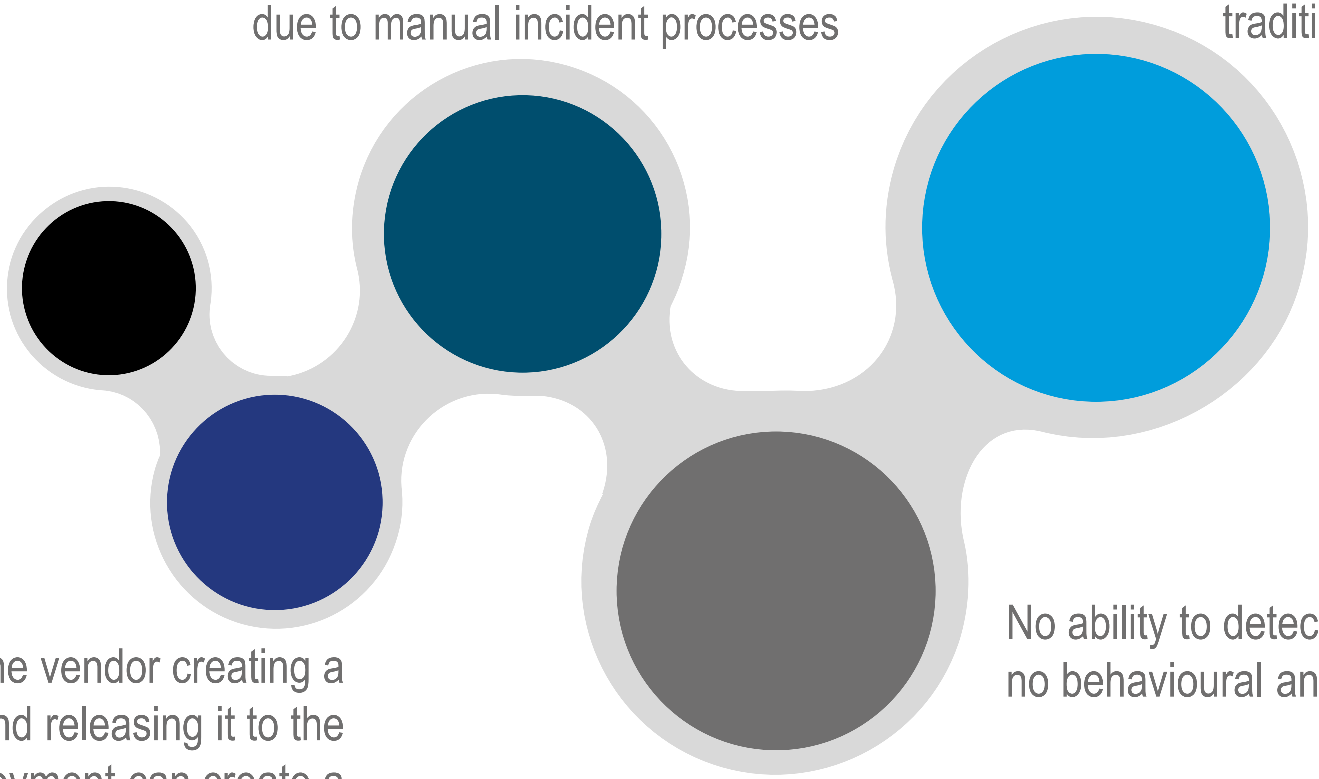
✓ TRADITIONAL AV CAN STILL DETECT AND QUARANTINE MALICIOUS CODE

✓ VENDORS CONSTANTLY LOOK FOR NEW THREATS

✓ AV TOOLING PROVIDES REPORTING OF DETECTED INFECTIONS

PROTECTING THE ENDPOINT

BUSINESS IMPACT IF CONTINUING TO USE ONLY TRADITIONAL AV



Lack of tooling to do anything once it is established that an infection cannot be remediated by traditional AV service

Delays between the vendor creating a new signature and releasing it to the customer for deployment can create a significant risk window.

Security teams unable to react quickly due to manual incident processes

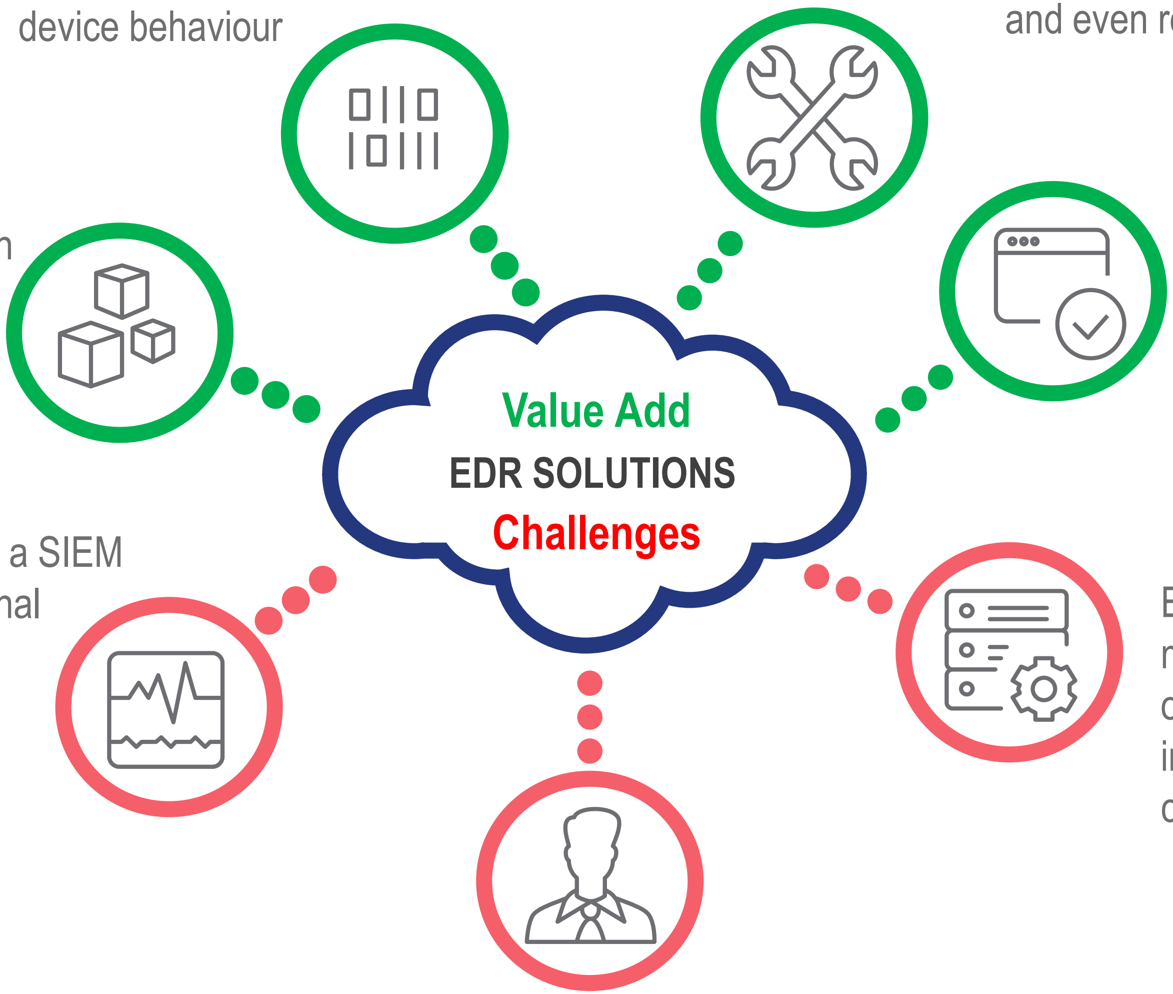
No ability to detect zero-day threats and no behavioural analytics

Lack of detailed information provided by traditional AV to the SOC

DIGITAL Trust
Mastering business security

IS EDR THE ANSWER?

…..IF IT IS, WHAT ARE ITS CHALLENGES?



Value Add

EDR SOLUTIONS

Challenges

More comprehensive analysis of device behaviour

EDR incorporate tools with which to contain and even remove infections.

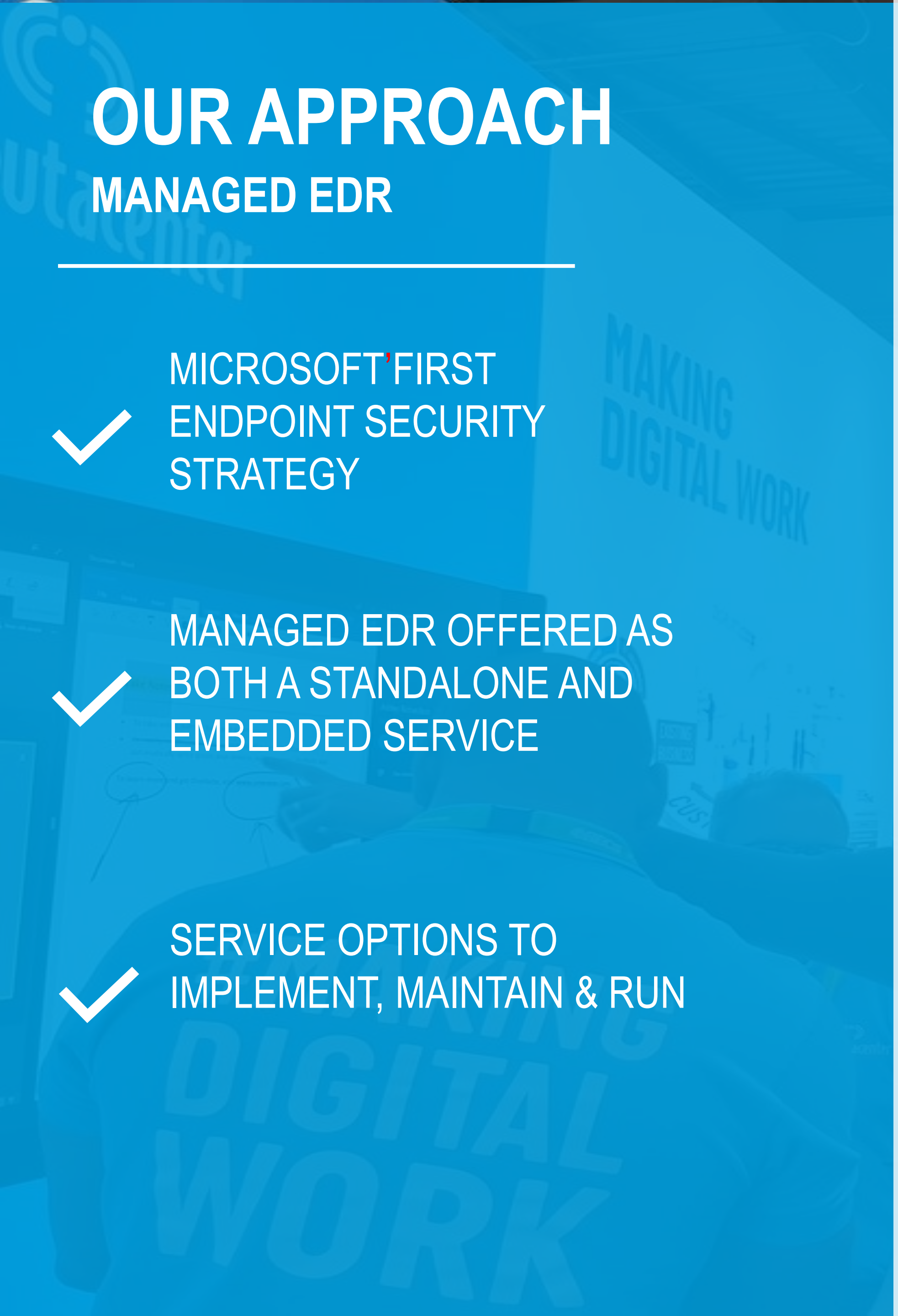
Uses machine learning to undertake malware Identification rather than pattern based.

Gives security analysts a single pane of glass with which to view and respond to any cyber threats

Integrating EDR data to a SIEM to give the SOC additional insight can be difficult

EDR is a complex solution that needs to maintained and managed, and only operates effectively if the telemetry data ingested and analysed is configured correctly

Many organisations lack the in-house skills and scale in their security teams to operate EDR effectively



OUR APPROACH

MANAGED EDR

✓ MICROSOFT’FIRST ENDPOINT SECURITY STRATEGY

✓ MANAGED EDR OFFERED AS BOTH A STANDALONE AND EMBEDDED SERVICE

✓ SERVICE OPTIONS TO IMPLEMENT, MAINTAIN & RUN

- Help our customers take advantage of the inbuilt capability within Microsoft’s E5 licencing
- Embed EDR services within our broader Endpoint Security Managed service
- Operate as an interface between our customers security teams and the Microsoft Defender for Endpoint Console
- Filter security alerts identified by Microsoft Defender for Endpoint, logging only actual security issues to the customer
- Adding optional diagnostic and triage activity as agreed with the customer
- Utilising pre-defined operational runbooks to streamline diagnostic assessment
- Utilising in-built automation and machine learning within the Microsoft platform to perform agreed levels of triage

SERVICE DETAIL

MANAGED EDR

MONITORING

- Monitoring of security alerts and security incidents shown by the Microsoft Defender Security Center console.

RUN BOOKS

- Responding to Security incidents using predefined run books
- Development of additional runbooks and update or amendment of existing runbooks

TROUBLE SHOOTING

- Troubleshooting in relation to Defender for Endpoint service performance issues and helping to manage service outages identified by the Customer or by the Computacenter Managed EDR team

REVIEW OF DATA SOURCE EFFICACY

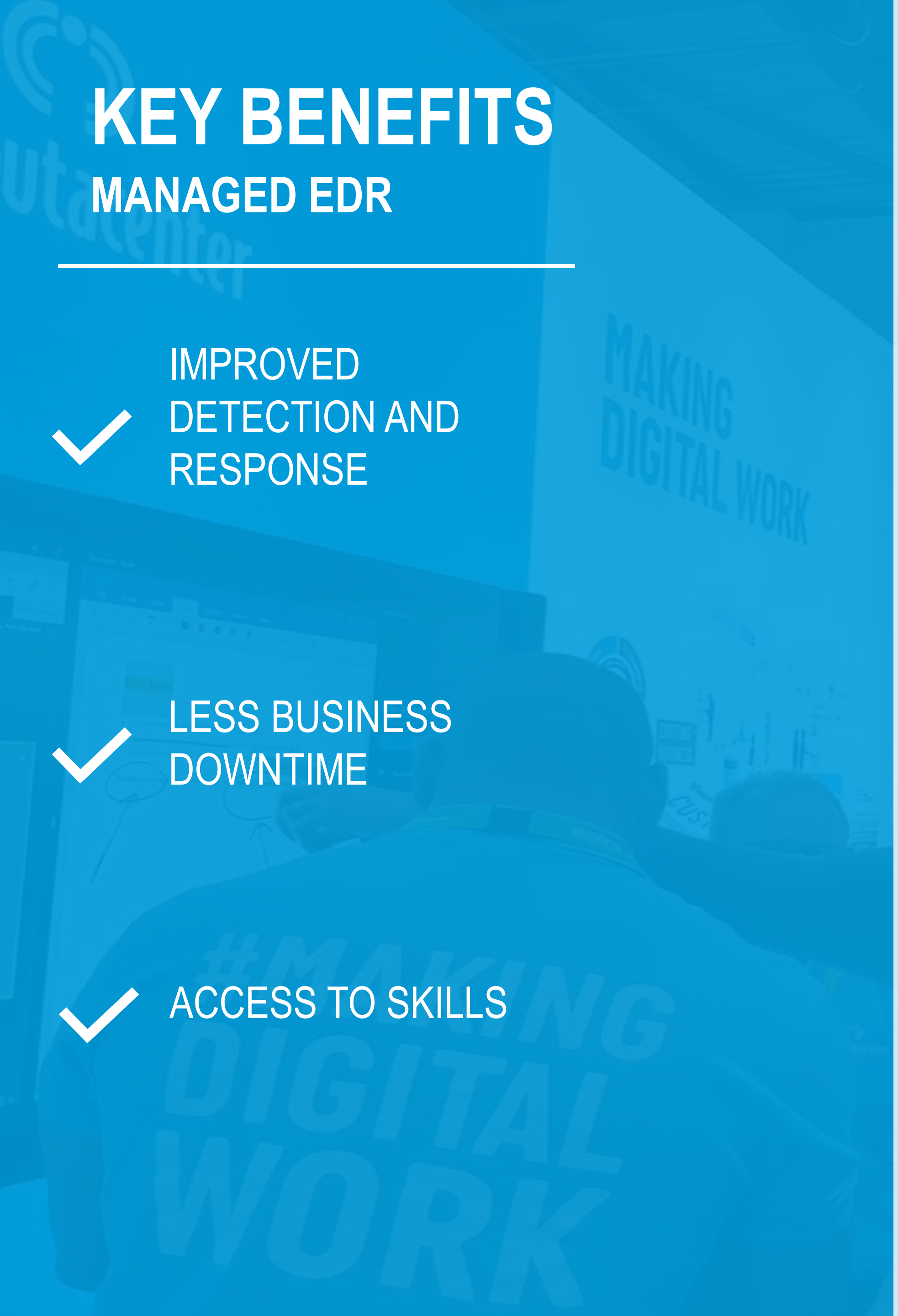
- Are all devices running Microsoft Defender as intended?
- Are all devices that are running Microsoft Defender contributing data to the Defender for Endpoint solution?

TUNING OF DETECTION ALGORITHMS

- Provide insight and guidance as to which detections are adding the most value
- Understand which detections are creating unnecessary “white noise”, to enable the customer to consider additional detections deployment

SLA & TREND REPORTING

- Monthly summary of the volume and type of incidents identified and passed to the customers support teams
- Insight to any overarching trends in incident type and cause



KEY BENEFITS

MANAGED EDR

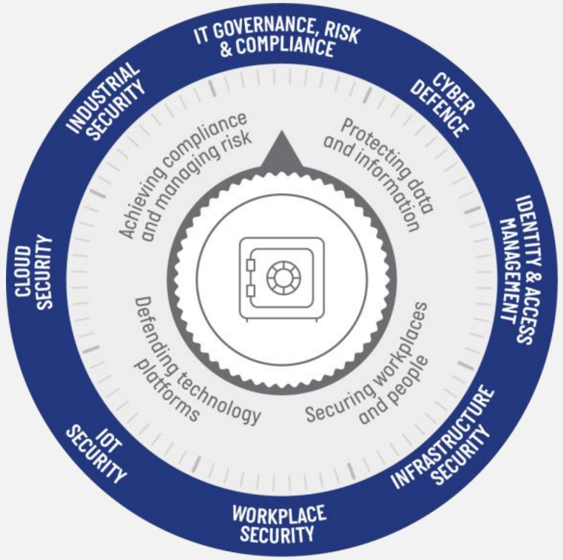
✓ IMPROVED DETECTION AND RESPONSE

✓ LESS BUSINESS DOWNTIME

✓ ACCESS TO SKILLS

- Acceleration of both Mean Time to Detection and Mean Time to Response as remediation can be conducted remotely by the detection team.
- Enhance real-time prevention against malicious activity 24*7, with much quicker reaction to detected issues.
- Increasing the productivity of Customer security teams by freeing them to focus on other security priorities.
- Offsetting the risk of recruiting, training and retaining limited, high value, high demand security analytics skills.
- Leverage Microsoft E5 licencing investment.

WHY COMPUTACENTER ?


IT GOVERNANCE, RISK & COMPLIANCE
CYBER DEFENCE
IDENTITY & ACCESS MANAGEMENT
INFRASTRUCTURE SECURITY
WORKPLACE SECURITY
IOT SECURITY
CLOUD SECURITY
INDUSTRIAL SECURITY
Achieving compliance and managing risk
Protecting data and information
Securing workplaces and people
Defending technology platforms

DIGITAL Trust
Mastering business security

DIGITAL Power
Cloud accelerating business

DIGITAL Connect
Enabling connected business outcomes

DIGITAL me
Workplace designed for people, engineered for business

End to End capability – Source, Transform & Manage

2020 Leader for both 'Strategic Security Services' and 'Technical Security Services'

40 years of experience in enterprise IT, and 20 years in information security

300+ Dedicated security personnel

We blend the speed of a boutique security shop with the size and presence of international security solutions

Computacenter holds over 200 security vendor accreditations

PROTECTING DATA & INFORMATION

ACHIEVING IT COMPLIANCE & MANAGING IT RISK

DIGITAL Trust.

Mastering business security

SECURING WORKPLACES & PEOPLE

DEFENDING TECHNOLOGY PLATFORMS