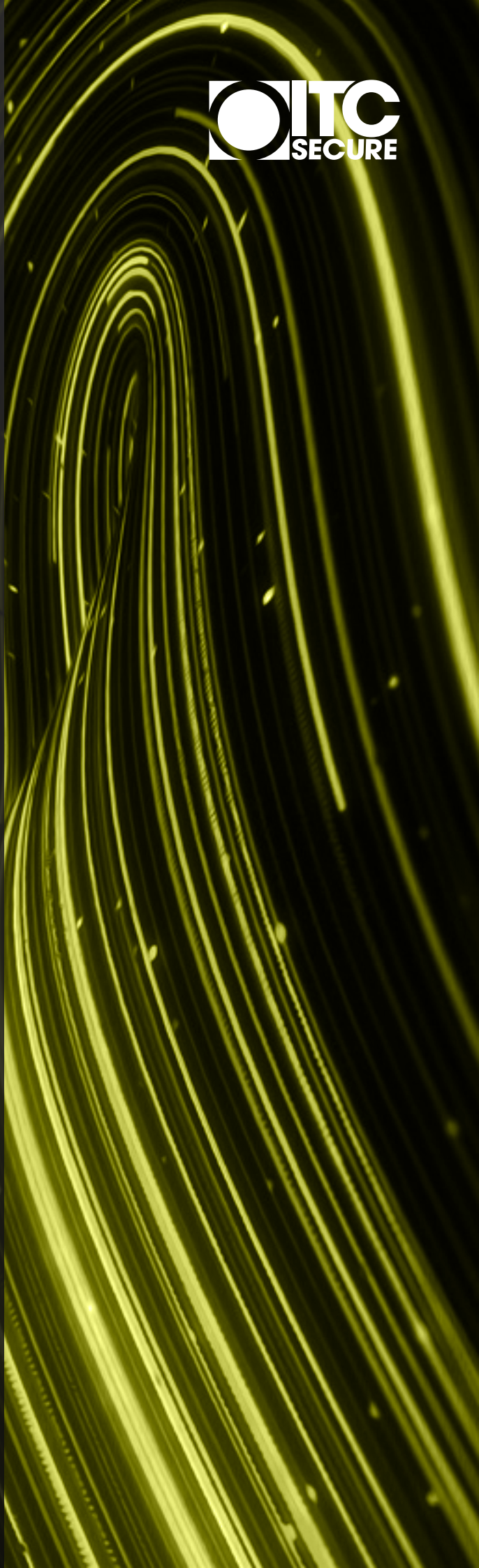
RISK.TRANSFORMED.

BALANCING COMPLEXITY AND SIMPLICITY IN CYBER SECURITY

How do you select the right Managed Extended Detection & Response (MXDR) for your business?

Read this guide to find out.

TABLE OF CONTENTS



Section one

EXECUTIVE SUMMARY

We live in an age where virtually every type of cross-border business transaction has a digital component. The possibilities for new relationships with customers and partners are endless, all thanks to technology.

But this accelerated digital transformation can be a double-edged sword, bringing both opportunities and threats in equal measures. The more we connect to the outside world, the greater the risk. Every time another device or capability is added within your business, you also add a vulnerability of project failure, of a data breach, or worse.

We've gone from having between 50,000 to 500,000 endpoints in a corporate network and today we have millions or even tens of millions with the advent of the Internet of Things (IoT). Whilst the number of endpoints has grown exponentially, many of the older devices are no longer adequately secured or maintained by their manufacturers, which poses significant risk when using them in your business environment today.

It is predicted that by 2030, as many as 500 billion devices will be connected to the Internet worldwide, with many of them outside corporate control. Already, smart cars and homes have been exploited by malware being used in distributed denial-of service attacks, while billions of chips are at risk from Meltdown and Spectre weaknesses. This is further compounded with limited in-house resources, a cyber security skills gap, and rapid growth in the number and sophistication of threats; this has overwhelmed many security teams who are typically understaffed and unable to keep up.

In this new reality, a data breach or network intrusion is all but inevitable when it comes to reaping the benefits of digital transformation.

But it can be challenging to establish a truly integrated cyber security approach due to a lack of resources and technology, increasing regulatory and operational pressures, system compromises, and ever-expanding attack surfaces and vulnerabilities.

The question then becomes what can businesses do about it? This guide answers this question.

Section two

CREATE A STRONGER CYBER SECURITY POSTURE WITH MXDR

Staying ahead of the threat landscape curve has become increasingly difficult.

Alert triage can simply overwhelm security teams, particularly those that are understaffed.

Research shows that Security Operation Centre (SOC) teams can be overwhelmed with an average of over 10,000 alerts per day, and too often the doors are wide open for attackers.[1]

The price tag resulting from inadequate defences is significant and affects both the top and bottom line. On average, the cost of a data breach reached $4.35m USD in 2022 – an increase of 12.7% in comparison to 2021.[2]

To combat the significant growth in attacks, Managed Extended Detection & Response (MXDR) is emerging as a solution to note when it comes to supplementing in-house efforts and provide comprehensive, consolidated cyber security to companies that cannot maintain their own security operations. In fact, organisations that have deployed MXDR experience an average lower cost of data breaches than the organisations that haven't deployed it.[2]

What is MXDR?

MXDR is the most advanced threat detection and response available today. It builds on previous generations (like MDR and XDR) to increase protection across your attack surface, covering a broad range of risk scenario, integrated as a single service.

Leveraging human and machine analysis, it provides 24x7 monitoring and detection, prevention, remediation, and expert threat identification and hunting - across IT and operational technology (OT) assets—from the cloud to the ground to the edge

+10,000
The average number of alerts SOC teams deal with every day.
- Enterprise Management Institute

$4.35m
The average cost of a data breach.
- 2022 Cost of Data Breach report, IBM

287 days
The average time it takes an organisation to identify and contain a breach.
- 2022 State of Detection and Response report, IBM

Section three

WHY ORGANISATIONS NEED MXDR

The need for MXDR is dictated by three challenges that

01. BUSINESS PRESSURES

Thirty years of history has shown us that cyber risk is difficult to understand, problematic to hedge, only likely to grow, and characterised by continually changing business pressures.

Today, it's no longer enough to be insured for cyber security without proactive measures in place that can make the difference between premiums, policies and coverage. Additionally, investors are placing increased priority on cyber security within their investment decisions, compounded by the fact that regulation is increasingly making cyber security mandatory by placing greater obligations on companies – it's no wonder that all of these elements are creating increasing business pressures for company leaders to navigate and manage.

02. RISING COMPLEXITY

The reality of cyber security today is that business leaders are having to contend with a high degree of complexity, from accelerated digital transformation and cloud adoption in support of an agile workforce to the dissolution of the traditional secure perimeter.

This has been further compounded by a legacy network sprawl and an unmanageable volume of tools and providers to choose from when implementing a cyber security strategy.

As a result, complexity has driven cyber risks and associated costs to dangerous new heights and has made the implementation of effective security mechanisms increasingly difficult.

03. CYBER SKILLS GAPS

59% of organisations indicated that they would find it challenging to respond to a security incident due to a shortage of skills.[3]

Many organisations make the mistake of buying top-of-the-line cyber security technologies but then lack the skills, expertise, and resources to configure and use them to their full advantage – an issue compounded by the cyber skills gap of more than 2.7 million professionals globally[4].

With companies averaging 43 separate IT security and management tools in its infrastructure[5] , the reality is that deploying more tools is not the solution when there aren't enough skilled people to support them.

Section four

THE ADVANTAGES OF MXDR

The market is growing in response to the need for organisations to protect their business around the clock. MDXR enables companies to expand capabilities beyond in-house resources.

The advantages of MXDR services include:

01.
GREATER EXPERTISE

MXDR providers give you access to seasoned cyber security specialists who have the requisite skills and expertise to serve as dedicated team members and understand their customers' particular business needs.

02.
BETTER TECHNOLOGY

MXDR providers use advanced technology and a comprehensive suite of tools.

03.
REDUCED COMPLEXITY

A framework that integrates threat detection, prevention and remediation capability, and vulnerability assessment enables you to manage risks more efficiently from both known and unknown threats.

04.
HIGHER VALUE

The technology and 24x7 coverage of a SOC are cost prohibitive for many organisations, while an MXDR solution acts as a force multiplier that is easier on your budget.

MXDR: Putting the X-factor in MDR:

Building off MDR, MXDR is a next-gen advanced protection and response cloud platform, where the "X" is extending beyond traditional technology.

It's a simplified and consolidated approach that focuses on the entire business environment and provides critical supplemental technology and cyber security skills.

It integrates with your existing infrastructure, offering correlation of real-time threat detection, prevention, remediation and incident validation.

Always on, MXDR monitors and detects threats while automating response and remediation across all endpoints, infrastructure and beyond: a critical speed factor.

Supportive SOC services offer rapid incident response to threats, including mitigation and remediation assistance.

Section five

MXDR FEATURES AND CAPABILITIES

01.
24X7, REAL-TIME THREAT PROTECTION

A security incident can unfold at any time. You need a team of security analysts and engineers who monitor and triage alerts, and actively respond to indicators of compromise when they occur – 24x7.

The best MXDR providers enable you to gain deeper visibility, which is consolidated across endpoints, infrastructure and beyond, supported by a dedicated team of security experts, 24x7, to deliver the best outcome for your business.

02.
THREAT INTELLIGENCE INTEGRATION

To reduce the risk of advanced threats, you need the latest threat intelligence from multiple sources.

MXDR solutions, which integrate threat intelligence, as well as behavioural analytics, are much better positioned to analyse data in the right context to detect advanced, unknown threats.

03.
ADVANCED ANALYTICS

Leveraging machine learning, threat intelligence, and big data, advanced analytics is a critical MXDR component that enables real-time threat detection.

Top MXDR providers invest heavily in analytics platforms and other tools to analyse data in context, as well as the ability to correlate events across the entire business environment.

04.
INCIDENT RESPONSE

The longer your dwell time, the more expensive your remediation becomes. The average time to identify a breach is 287 days— but companies that identify a breach in less than 100 days and contain it within 30 days can save $1m USD.[2]

MXDR providers include different degrees of incident response as part of their base fee, along with crisis support.

05.
THREAT HUNTING

Defences based on point-in-time scanning or signatures can no longer keep up with today's stealthy threats like fileless malware. Proactive threat hunting goes beyond scanning files that enter your environment.

MXDR providers rely on a combination of automated tools and human analysts to track activity and identify suspicious behaviour across IT and operational technology (OT) assets—from the cloud to the ground to the edge.

Section six

TOP CRITERIA WHEN EVALUATING AN MXDR PROVIDER

Effectively detecting, preventing and remediating today's advanced threats requires a sophisticated mix of people, process, and technology: one that enables businesses to take a proactive, holistic approach to cyber security.

Knowing what to look for in an MXDR provider will help organisations get the value they seek from their cyber security programme:

01. INTEGRATED DELIVERY

Threat detection needs to go far beyond an organisation's endpoints given accelerated cloud adoption and the shift to hybrid working. A MXDR provider should be experienced with a comprehensive portfolio of cyber security solutions that protect networks, endpoints, cloud environments and identity: bringing together threat telemetry and forensic data from the organisation's broader infrastructure as an easy-to-consume service.

02. BROADER PROTECTION

Threat hunting is without doubt one of the many important aspects of cyber security. It needs to involve proactively, while exploring and interrogating systems for their current state as well as historical data – combining both human-led threat hunting with 24×7 monitoring and real-time analysis and investigations, and specialist tools for specific business systems in order to effectively detect, prevent and remediate.

03. ACTIONABLE INTELLIGENCE

The right level of intelligence is often the foundation for effective detection and threat hunting. Look for an MSSP that can curate multi-signal inputs with expert guidance that result in less 'noise' and improved intel where the action required is built into their workflow (rather than manual reporting)– enabling better decision making to allow for faster responses to threats to your business.

04. ACCELERATED RESPONSE

Look for a provider that goes beyond just notifying and alerting. Your provider should have the ability to respond to threats by containing them and keeping them from spreading further and be able to act remotely on your organisation's endpoints, within the network, or the cloud, with actionable mitigation guidance and automated response actions tailored to your environment.

05. CULTURE FIT

Culture fit is an important but often overlooked aspect. Consider their operating model and how they will work with your business in terms of service-delivery experience and capabilities. Questions to consider: are they credible, and do they have a good reputation in the industry? Do they have the right balance of strategic thinking and operational excellence to be a long-term partner? Do they understand your broader business objectives and how to make security a strategic enabler for your business?

A good cyber security provider will take a holistic approach to and consider all aspects of your business in order to implement a comprehensive strategy that includes both technical and non-technical measures; all the while, they will work closely with you to keep you up to date with the latest trends and threats and ensure that your business is always one step ahead.

Section seven

THE ITC APPROACH: ITC MXDR POWERED BY PULSE

We believe that cyber security is an enabler to support every business' digital transformation objective.

ITC's MXDR service powered by Pulse delivers intelligent detection and optimal protection at scale for organisations looking to secure their digital transformation journey and accelerate business performance, without the complexity traditionally associated with cyber security.

Through a combination of leading technology and deep expertise in cyber security, ITC's MXDR service delivers a consolidated, modular set of threat hunting, detection, response and remediation capabilities, simplifies the complexity by being easy to consume and reduces risk 24x7 while helping to improve your overall cyber security posture.

ITC's MXDR is powered by Pulse, the company's service delivery platform, an industrialised operating model that combines human-in-the loop expertise, best-in-class methodologies and automated processes that drives an unrivalled experience and enables intelligent detection and optimal protection for businesses at scale.

The NIST framework centres around five core functions: **identify**, **protect**, **detect**, **respond**, and **recover**. When you're evaluating cloud security solutions, consider how well they score on these five functions.

Section seven

THE ITC APPROACH: ITC MXDR POWERED BY PULSE

BROADER PROTECTION	ACTIONABLE INTELLIGENCE	ACCELERATED RESPONSE
Gain deeper visibility consolidated across endpoints, infrastructure and beyond supported by the best minds in security from ITC.	Curated threat intelligence together with expert guidance for better decision making that enables faster response to threats to your business.	Proactive guidance, remediation and automated response actions to advanced threats, tailored to your environment.
GREATER VISIBILITY Profiling your assets and collecting data and security event observations from multiple-signal inputs across endpoints, networks, systems and applications, tailored to your environment.	**CONTINUOUS INTEL** Ability to scale with automated continuous information gathering and analytics to provide high-quality indications of attack for further analysis, reducing dwell time.	**CUSTOMISED RESPONSE** Tailored response actions for each environment by enriching security-event notifications with additional data prior to acting to mitigate the threat.
24X7 MONITORING Monitoring of your environment 24x7 combining automation and human intelligence necessary to effectively manage todays threats and emerging risks.	**CREDIBLE REPORTING** Delivery of credible, accessible reporting, which enables better decision making, to improve your security posture.	**TECHNICAL ANALYSIS AND HUMAN INSIGHT** Aggregated intelligence through our platform, with a team of experts who know how to augment and contextualise them and deliver actionable mitigation responses.

ANCHORED BY MICROSOFT'S CYBER SECURITY PORTFOLIO SUPPORTED BY OTHER BEST-OF-BREED SECURITY PARTNERS

Microsoft awarded Solutions Partner: one of only 40 specialised managed partners in the UK&I, and one of only 10 SCI/MSSP managed partners*

FULLY MANAGED AND DELIVERED BY OUR TEAM OF CYBER SECURITY EXPERTS

25+ years experience delivering business critical services to over 300 blue-chip organisations

**This information is accurate to the best of ITC's knowledge and is subject to change.*

Section eight

FINAL THOUGHTS

It is no secret that the cyber security industry has multiple challenges. If technology alone were the answer, the problem would already have been solved. Yet 63% of organisations reported a breach in the last year.[6]

Many organisations make the mistake of buying top-of-the-line cyber security technologies but then lack the skills, expertise, and resources to configure and use them to their full advantage – an issue compounded by the cyber skills gap of more than 2.7 million professionals globally.[4]

The reality is that the time, effort and expertise needed to establish 24×7 detection, prevention and remediation capabilities in- house can be overwhelming. Many organisations try to protect their data by implementing security technologies such as XDR and SIEM platforms across a large number of endpoints, network, and cloud environments. However, these technologies can be difficult to deploy, configure, and maintain and often take too long for an organisation's in-house resources to gain expertise on them due to other business priorities that limit their time.

For most companies, developing and maintaining the necessary expertise and technological capabilities to remove the burden of deploying, configuring, and managing their security across multiple environments can be hard, if not impossible. In order to stay ahead of the curve, it is essential for businesses to take a holistic approach to cyber security that goes beyond just pure technology.

The key is to find a provider that understands your business and can provide the right blend of skills, technology, and governance to make security a strategic enabler for your business, giving you the confidence and agility you need to stay ahead of emerging threats and reap the benefits of digital transformation, improving your cyber posture by keeping complexity at bay so that you can focus on what matters to you the most: your business.

About ITC Secure

ITC Secure (ITC) is an advisory-led cyber security services provider and a Microsoft Solutions Partner with designations in Security, Modern Work, and Infrastructure..

The company has a 25+ year track record of delivering business-critical services to over 300 global blue-chip organisations, bringing together the best minds in security, a relentless focus on customer service, and advanced technological expertise to help businesses succeed.

With its integrated delivery model, 24×7 fully managed state-of-the-art Security Operations Centre, and customer-first mindset, ITC works as an extension of its customers' teams to accelerate their cyber maturity – safeguarding their digital ecosystem and securing their business and reputation.

ITC serves global organisations from its locations in the UK and US with a world-class team of cyber consultants, technical designers, and cyber experts.

The company is a certified Great Place to Work® employer, active member of the Microsoft Intelligent Security Association (MISA) and winner of the Best Security Company of the Year 2021, Best Workplaces™ in Tech, and Best Workplaces™ for Wellbeing 2022.

W: **www.itcsecure.com** | E: **enquiries@itcsecure.com**

Sources : 1. Enterprise Management Institute | 2. IBM | 3. World Economic Forum | 4. (ISC)² | 5. The Foundry | 6. Forrester