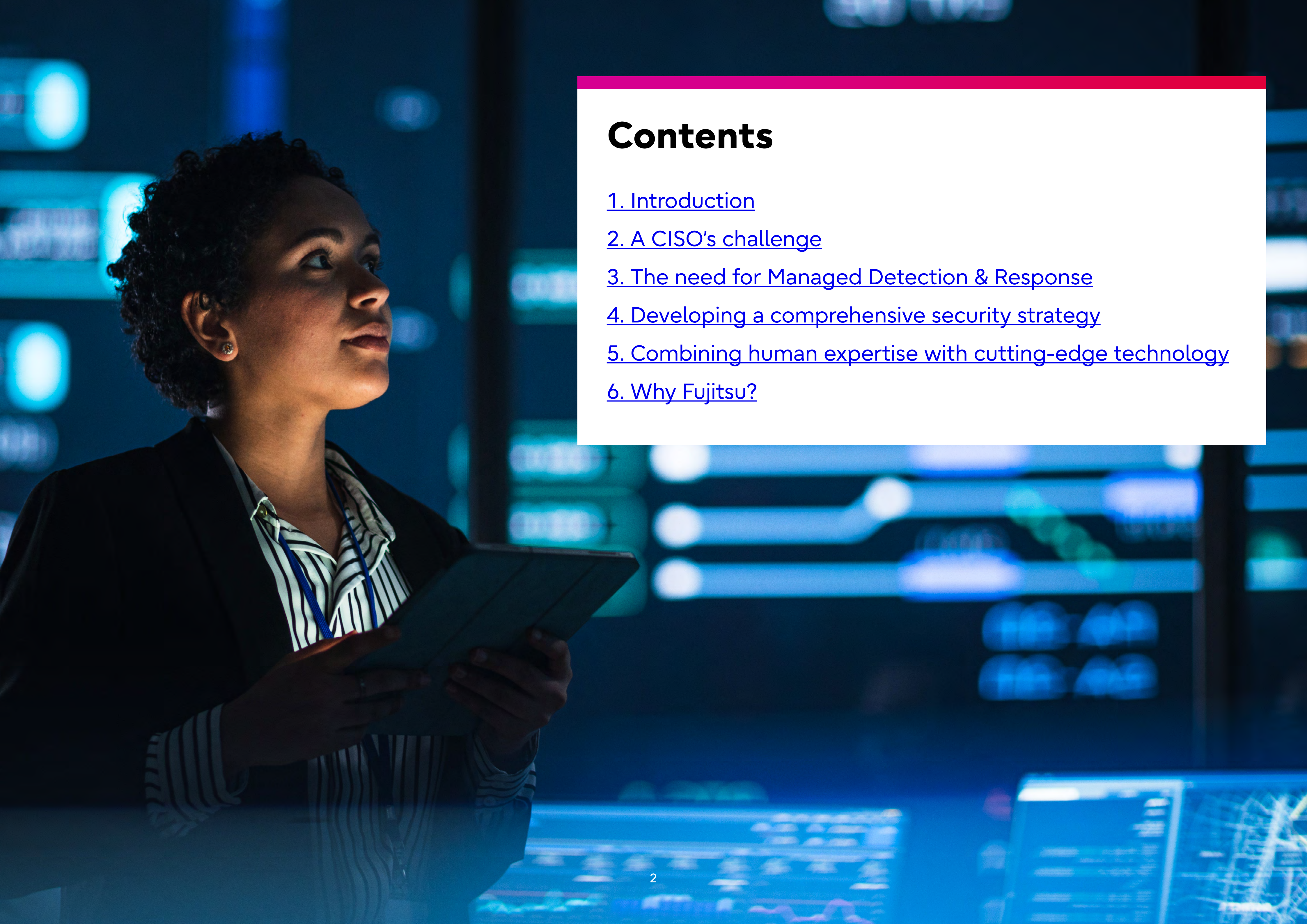
Managed Detection and Response

Accelerating security response and mitigating business risks with Fujitsu

Solution guide



Contents

> *"Security leaders are increasingly cognizant that reducing the time to detect a threat is meaningless without a corresponding reduction in the time to respond to a threat to enable a return to a known good state."*
>
> Gartner Research Market Guide for Managed Detection and Response Services

1. Introduction

The threat landscape continues to grow in velocity and complexity. Organizations are navigating a landscape fraught with security threats, including sophisticated phishing attempts, ransomware and frequent exploitation of application and network vulnerabilities. These threats pose significant risk to the daily operation of businesses and present formidable challenges that must be addressed to not only detect but adequately respond.

For any business, effectively managing and responding to these threats is crucial. Without a centralized and dynamic approach to handling these security challenges, the capacity to prevent breaches across the digital enterprise is markedly diminished.

2. A CISO's challenge

Imagine a Chief Information Security Officer (CISO) with a mission – protecting the organization from the ever-present dangers of cyber attacks.

The burden of a CISO

The job of a CISO is a fine balancing act of managing risk, resources and often with budget constraints. The CISO and Security Operations team are inundated with alerts with a necessity to identify and respond to true positives. There is an abundance of manual tasks, daily checks and a requirement to manage multiple and disparate security tools. As such, the stakes are high – any oversight could lead to breaches, significant regulatory fines with unwanted exposure and reputational damage.

Where the CISO stands

- Past security incidents linger as stark reminders of the potential consequences of a breach.
- Alarm fatigue is a daily reality, with an overwhelming volume of security events to handle.
- Ensuring technologies are properly configured, maintained, and patched is a continuous task, vital for security integrity.
- Tuning and configuring rules to counter sophisticated threats require expertise which is hard to come by.
- Monitoring security alerts is a continual effort, but another huge challenge is how to respond effectively and in a timely manner.

A new dawn

Resources drained by ineffective incident triage and false positives should be a thing of the past. A CISO needs a real-time, transparent view of their organization's security posture with increased visibility in a dynamic and proactive manner. Threat enrichment ensures they can zoom in, respond and mitigate genuine threats.

A CISO needs confidence their approach will maintain pace with the evolving threat landscape. This ensures the organization can operate safely and securely with a threat response strategy that adapts and responds just as quickly as the threats it's designed to counter.

3. The need for Managed Detection and Response

Managed Detection and Response (MDR) extends beyond traditional and disparate security services such as Security Information and Event Management (SIEM). It is a centralized, dynamic service that can identify true positives through enrichment and correlation achieving a proactive and optimal response.

Sending logs to a SIEM platform and waiting for alarms to fire is simply no longer fit for purpose. Rules must be created dynamically with high fidelity to detect the latest threats. Data must be enriched and tagged with up-to-date threat intelligence and where possible responses must be handled as efficiently as possible with elements of automation.

Frameworks like MITRE ATT&CK are also increasingly important in order to assist in identifying the type of attack and technique being used. Correlating this across other security events allows for a holistic and enriched analytical view.

This should be coupled with proactive hunting of threats and not waiting for alarms to fire. This doesn't have to be exhaustive but analysis of telemetry on a daily basis should be a key element of any MDR service.

Customers demand a consistent and standard service, monthly reports detailing SLA's and device uptime are still necessary. It is vital that all incidents are reported and analyzed in as near real-time as possible, demonstrating efficient response and ensuring confidence there are no breaches of the network or exfiltration of data.

Meet Jane, a CISO mastering cyber security challenges

Watch this video to discover how Fujitsu Managed Detection and Response service transforms her team's efficiency with automated, cutting-edge technology.

Click the link below to watch the video.
youtube.com/watch?v=x2Nlp-96GYY

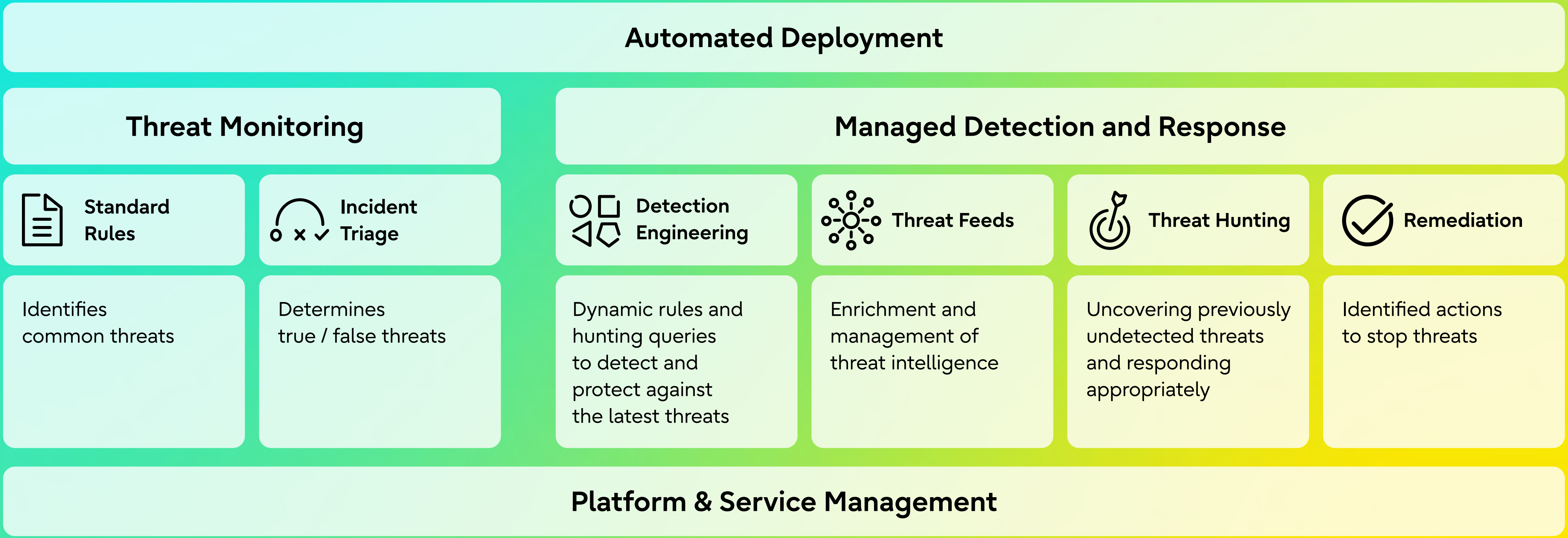
4. Developing a comprehensive security strategy

Our MDR service, underpinned by Microsoft Sentinel, is supported by our experienced team of security professionals across the globe. Our teams have significant depths of knowledge across critical domains such as Threat Intelligence, Detection Engineering, Security Orchestration, Automation & Response (SOAR), Threat Hunting and Incident Response.

We are committed to the continual improvement of your security posture, with a laser focus on timely response to true security incidents, whilst reducing false positives. In the face of emerging threats and stringent compliance requirements, our service delivers swift and confident response.

Our MDR service will reinforce and elevate your organization's security. With a key focus on the Microsoft stack via Microsoft Sentinel, we configure and implement analytic rules and enrich IP data for a thorough contextual understanding of incidents.

Our delivery model is tailored to specific needs, with MDR services executed from our Global Delivery Centers (GDCs), whilst regional security teams provide localized, on-the-ground support and expertise. This blended approach ensures that each aspect of the service is delivered effectively, matching the unique requirements of your organization.



Automated Deployment

Threat Monitoring

Standard Rules

Identifies common threats

Incident Triage

Determines true / false threats

Managed Detection and Response

Detection Engineering

Dynamic rules and hunting queries to detect and protect against the latest threats

Threat Feeds

Enrichment and management of threat intelligence

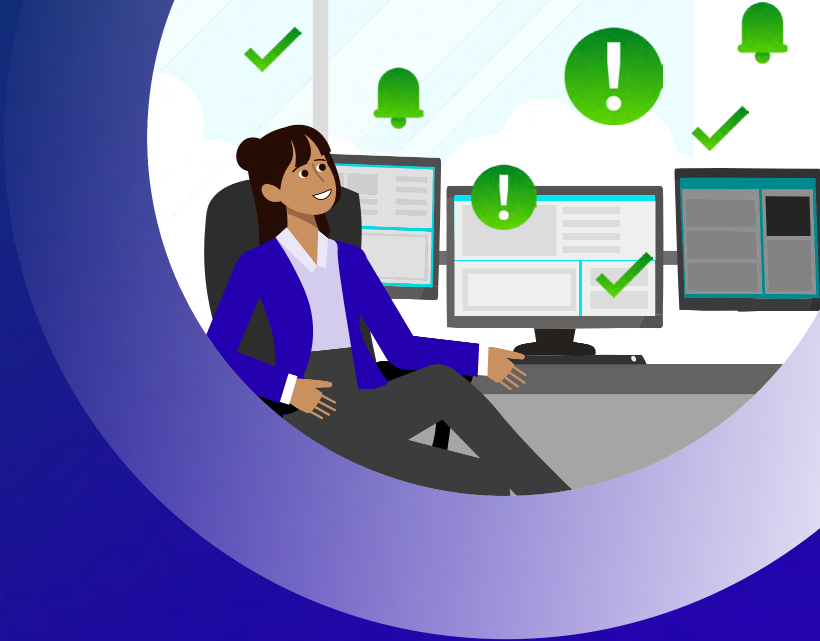
Threat Hunting

Uncovering previously undetected threats and responding appropriately

Remediation

Identified actions to stop threats

Platform & Service Management



5. Combining human expertise with cutting-edge technology

Our MDR service is engineered to enhance the security of organizations by providing investigative analysis that not only identifies threats, but also disrupts and contains them effectively.

Key customer benefits of Fujitsu MDR service:

Increased visibility

Our MDR service provides a comprehensive understanding of your organization's security landscape. It ensures that critical threats are promptly identified and addressed.

Optimized intelligence

With a centralized and consolidated view of security threats, we enrich incidents and reduce the "noise" to bring core threats to the forefront.

Automated deployment

We streamline the deployment process meaning the heavy lifting has already been done. This significantly reduces the time and effort required to get started and ensures the service is cost competitive.

Rapid response capabilities

Our dynamic service is designed for agility, enabling quick and decisive actions. This responsiveness is critical in minimizing potential damage and maintaining operational security.

In the pursuit of a secure organization, the true measure of success lies in the ability for your business to thrive without the distraction of security threats. With Fujitsu MDR service taking the helm of day-to-day threat management, your teams are free to focus on strategic business initiatives and stakeholder communications. This means less time spent in the trenches of cyber defense and more time driving business value, growth, and innovation.

6. Why Fujitsu?

Fujitsu stands out by offering global expertise across security services. Our strategic partnerships across academia, public and private sectors ensure we stay at the forefront of industry demands.

Global reach with a local touch

Our extensive network of Global Delivery Centers (GDCs) is complimented by local expertise. Ensuring that expert assistance is readily available no matter your location, we deliver standardized services with predictable costs. We provide you with the expertise you need, exactly when and where you need it.

Rapid, ready-to-deploy solution

Deployed as code, our MDR service is not only data-ready but also designed to return early actionable alerts. This rapid deployment capability is critical for organizations that need to respond swiftly to evolving security threats.

Seamless technological integration

Fujitsu has a long-standing partnership with world-class security technology partners including Microsoft and others.

Sustainability at the forefront

Our commitment to sustainability is woven into the fabric of our services. We prioritize eco-friendly practices in our service delivery, reflecting our dedication to not just securing digital assets but also preserving our planet.

Accelerate your security response with Fujitsu

Are you facing cyber security challenges that seem insurmountable? Whether you're grappling with the complexities of threat detection or streamlining your incident response, Fujitsu is here to elevate your security strategy while helping you mitigate business risks.

From initial assessment, a 30-day proof-of-value exercise, to full-scale deployment, our experts are ready to tailor a solution that fortifies your defenses and aligns with your unique security needs.

Connect with Fujitsu today to discover how our global expertise, cutting-edge solutions and dedicated teams can contribute to your cyber security success.

Visit us at fujitsu.com/global/mdr