Manuals+

☰

Contents [hide]

FUJITSU

FUJITSU Continuous Threat Exposure Management

Specifications:

- Product Name: Continuous Threat Exposure Management
- Manufacturer: FUJITSU
- Framework: Gartner-defined CTEM
- Features: Continuous discovery, risk prioritization, decisivere mediation

Empowering resilient enterprise security through continuous discovery, risk prioritization, and decisive remediation

Enterprises today are confronted with a complex set of cyber security challenges. Digital transformation has expanded attack surfaces, cloud complexity has grown, and attackers have become increasingly sophisticated. Fujitsu, as the only global system integrator providing a fully managed Continuous Threat Exposure Management (CTEM) service, addresses these challenging security dynamics head-on. This distinct service, owned and delivered by Fujitsu and powered by XM Cyber Attack Graph Analysis™, ensures continuous visibility, precise prioritization, and decisive action. Our approach helps CISOs, Security Operations leaders, IT directors, and board-level stakeholders shift from reactive defense to proactive resilience.

Why CTEM matters now

Given the rapidity at which cyber threats take root across enterprise IT environments, traditional vulnerability management no longer provides sufficient protection. The Fujitsu CTEM managed service – powered by XM Cyber's industry-leading analytics – delivers immediate, tangible results across four critical dimensions of enterprise security.

Defining CTEM

CTEM is a strategic, Gartner-defined framework that goes beyond traditional, reactive vulnerability management. Rather than focusing exclusively on common vulnerabilities and exposures (CVEs), CTEM offers a holistic, attacker-centric approach designed to identify and remediate exposures that present genuine risks to critical business assets.

According to Gartner's Top Strategic Technology Trends 2024: "A Continuous Threat Exposure Management (CTEM) program is a set of processes and capabilities that allow enterprises to continually and consistently evaluate the accessibility, exposure, and exploitability of an enterprise's digital and physical assets." CTEM thus transforms security operations from reactive, siloed, and fragmented activities into a continuous, coherent, and strategic risk management program.

Risk reduction

Enterprises struggle daily with thousands of vulnerabilities and security alerts – often making it hard to pinpoint where the real threats lie. The Fujitsu CTEM managed service provides continuous, real-time visibility across your entire hybrid environment, delivering a clear, holistic understanding of your most urgent risks. By identifying choke points – specific points of exposure where multiple attack paths converge – the managed service drastically simplifies risk management. Through continuous scanning and advanced analytics, our CTEM service then enables your security team to concentrate on precisely those issues that pose the greatest danger, eliminating critical lateral-movement risks and ultimately reducing breach likelihood and associated costs. "2% of exposures reside on choke points – key attack-path junctures – that adversaries leverage to escalate and propagate attacks towards critical assets."
XM Cyber's 2024 State of Exposure Management Report

Consider a Payment Card Industry (PCI) environment with hundreds – or even thousands – of potential attack paths. Rather than addressing every vulnerability equally, the CTEM service pinpoints two strategic choke points. By focusing on these choke points, the organization can fix multiple vulnerabilities simultaneously, eliminating up to 80% of the associated risk. This targeted approach dramatically enhances security effectiveness and ensures optimal use of resources.
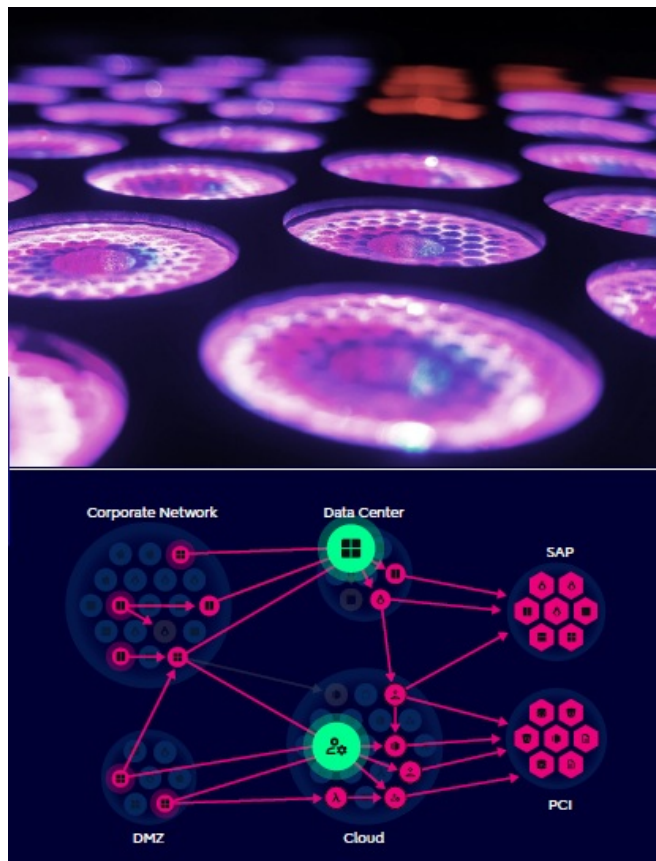
Operational efficiency

Security teams often grapple with resource overload, struggling to differentiate between critical risks and insignificant alerts. The Fujitsu CTEM managed service enables teams to focus their efforts effectively, reducing patch workloads and accelerating remediation timelines. "We've seen teams cut patch workloads dramatically once they identify which issues pose real risk." Matthew Rhodes, GSI & MSSP Sales Manager, XM Cyber

By highlighting only the most exploitable exposures, Fujitsu helps your team reduce unnecessary patches, perform quicker triage, and significantly lower the reliance on repeated penetration testing.

Executive-level visibility

The Fujitsu CTEM managed service delivers clear, board-level security metrics. By translating technical findings into meaningful business insights, the service empowers CISOs and IT directors to articulate risk management clearly and convincingly to senior leadership.

Key board-level metrics include:

- Number of critical assets at risk

- Potential exposures identified and mitigated
- Month-over-month risk posture improvements

These metrics not only support better executive understanding but also clearly demonstrate security ROI, bridging the gap between technical operations and business objectives.
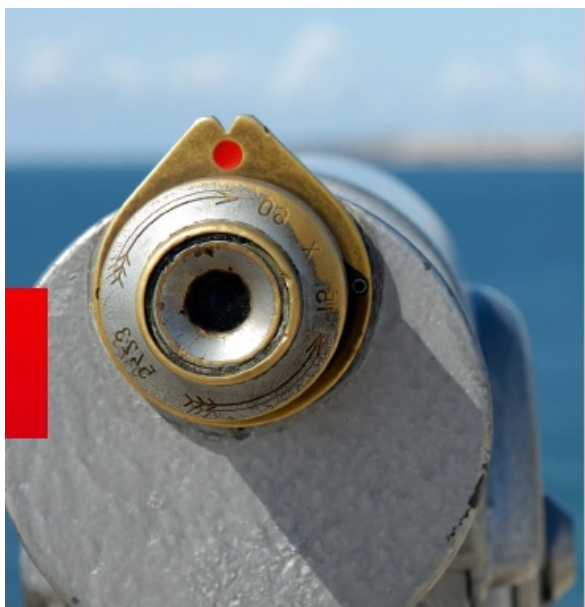
Compliance enablement

Regulatory compliance audits (PCI, GDPR, NIS-2) often strain organizational resources due to the complexity and scale of data needed. The CTEM managed service streamlines the compliance process by providing continuous, comprehensive visibility into your security posture. The service leverages XM Cyber Attack Graph Analysis™ to clearly illustrate the steps taken to mitigate critical exposures, significantly easing compliance reporting and audit readiness.

The new security reality

Modern enterprises operate in complex, hybrid environments that blend on-premises infrastructure with multi-cloud ecosystems. This complexity, combined with the relentless pace of digital transformation, has introduced unprecedented cyber security challenges. The reality of modern security is starkly different from traditional assumptions, necessitating a shift from reactive patching to a proactive, continuous threat management approach.

Overstretched defenders

Security teams today face a relentless wave of exposures, yet their resources remain limited. With an ongoing shortage of cyber security talent, organizations must continually achieve more with fewer resources. This imbalance increases the likelihood of critical threats slipping through unnoticed.

"82% of enterprises report a widening gap between identified exposures and their remediation capabilities." XM Cyber's 2024 State of Security Posture Report

This "remediation gap" – the difference between discovered vulnerabilities and the capability to fix them – is unsustainable and puts business-critical assets at heightened risk.

Siloed tools

Traditional security tools operate in silos: one for cloud misconfigurations, another for Active Directory vulnerabilities, yet another for software patching. This fragmented view obscures the bigger picture of security posture, enabling attackers to exploit minor gaps across different layers of the environment. Attackers rarely exploit a single vulnerability; instead, they chain smaller exposures together to escalate their access to critical assets. Unfortunately, most security teams cannot see these chains clearly because each tool operates independently.

"75% of discovered exposures are dead ends; focusing on the 25% that genuinely lead

to critical compromise provides maximum security ROI." XM Cyber 2024 State of Exposure Management report

Why "patch everything" fails
The traditional approach of attempting to patch every identified vulnerability is neither practical nor effective. Organizations quickly become overwhelmed, exhausting valuable resources without significantly reducing their actual risk exposure. This approach disrupts business operations and still leaves critical attack paths undiscovered and unaddressed.

Moreover, not every vulnerability represents a genuine business risk. Many identified exposures are "dead ends", meaning that while they may be technically exploitable, they do not lead attackers directly to critical systems or sensitive data – such as customer records, HR information, or industry-specific databases. CTEM explicitly deprioritizes these low-impact vulnerabilities, enabling teams to focus their limited resources on fixing high-impact exposures at critical choke points.

The need for a holistic, continuous approach
Organizations must move beyond reactive vulnerability management toward an attacker-centric, always-on model of exposure management. CTEM is exactly this framework, providing a structured way to continuously identify, prioritize, and address security risks.

By focusing on the attacker's perspective – how adversaries chain together vulnerabilities, misconfigurations, identity weaknesses, and other gaps – CTEM provides clarity on real-world risks, enabling teams to disrupt potential attack paths before exploitation occurs.

The CTEM framework – What you need to know

Core principles of CTEM

CTEM is built around four foundational principles:

1. **Attacker perspective**

   CTEM models real-world attack scenarios, identifying how attackers combine vulnerabilities, misconfigurations, and identity flaws into exploitable pathways toward business-critical assets. By taking the attacker's viewpoint, organizations can see risks clearly and take pre-emptive action.

2. **Risk-based prioritization**

   CTEM takes a predictive, proactive approach to security. Instead of reacting after incidents occur, it continuously identifies and evaluates potential attack paths toward critical business assets. By concentrating efforts where the potential impact is highest, organizations achieve better security outcomes with less strain on resources, delivering measurable improvements in resilience.

3. **Continuous improvement**

   Unlike periodic vulnerability assessments or penetration tests, CTEM continuously discovers, validates, and remediates exposures as the business and threat landscape evolve. This ongoing cycle helps maintain a dynamic, real-time view of the organization's true risk posture.

4. **Business alignment**

   The CTEM framework directly connects security activities to business outcomes by clearly illustrating how potential cyber attacks can impact critical assets, data, and

operations. This alignment enables CISOs and security leaders to clearly communicate the value and impact of security investments in terms that resonate with executive stakeholders.

CTEM vs. traditional security approaches

Traditional vulnerability management programs typically rely heavily on identifying and patching known CVEs. However, XM Cyber's 2024 report highlights a crucial insight: "Only about 1% of monthly exposures in a typical enterprise are traditional CVEs; the remaining 99% involve identity, configuration, and other exposures."
Fujitsu articulates the difference:

"Organizations often chase thousands of alerts without knowing which ones are truly exploitable. CTEM changes that by mapping real attacker pathways and clearly identifying the few exposures that genuinely matter."
James Frith, Global CTEM Service Owner, Fujitsu

CTEM's continuous and proactive approach addresses the critical shortcoming of traditional vulnerability management – namely, its inability to prioritize effectively. CTEM goes far beyond telling teams what's theoretically vulnerable; it shows them what's genuinely exploitable and urgent.

"XM Cyber provides the automated, continuous vantage point. Fujitsu ensures that vantage translates into real remediation and meaningful business risk reduction."
Matthew Rhodes, GSI & MSSP Sales Manager, XM Cyber

Meet Jane, a CISO under relentless pressure to shield her organization from advanced cyber threats. Discover how the Fujitsu CTEM managed service empowers Jane and her team to stay one step ahead – focusing on what matters most to protect the organization's crown jewels.
Click the link below to watch the video. https://youtu.be/CBch5iYo3TE

Operationalizing the five-stage

CTEM framework with Fujitsu

The Fujitsu CTEM managed service operationalizes Gartner's CTEM framework into five clear, actionable stages. By combining Fujitsu's global managed service expertise with XM Cyber's market-leading technology, each stage seamlessly flows into the next, driving continuous security improvement.
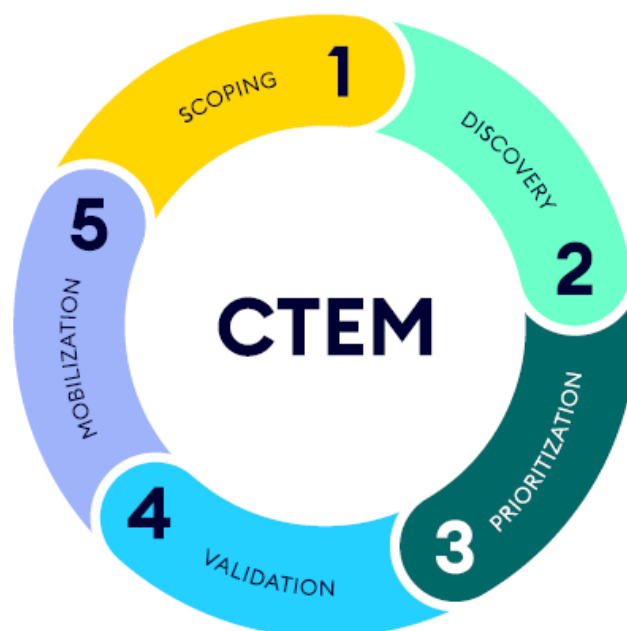
1. **Scoping**

   Clearly identify the data, systems, and assets most critical to your business, establishing what matters most and where your security efforts should be directed.

Getting started

Key foundational acivities include:

- Stakeholder interviews (IT, security, compliance, line-of-business leaders).
- Asset inventory focusing on critical business systems (payment platforms, ERP, intellectual property).
- Establish risk tolerance and business impact thresholds
-

"Scoping is absolutely critical. Without knowing the 'crown jewels,' you end up trying to fix everything at once." Matthew Rhodes, GSI & MSSP Sales Manager, XM Cyber

- Fujitsu's expert consultants lead tailored scoping workshops, clarify business objectives, establish clear prioritization criteria, and create a focused, actionable scope

for the CTEM initiative.

Discovery

Provide continuous visibility into vulnerabilities, misconfigurations, identity issues, and potential exposures across hybrid environments – on-premises, cloud, and Active Directory.

Creating a digital replica

XM Cyber safely replicates environment metadata to create a continuously updated digital twin, running 24/7 attack simulations without impacting live production systems. Attackers exploit identity exposures, cloud misconfigurations, and traditional vulnerabilities interchangeably. Only holistic visibility across all these dimensions can reveal true attack paths. Fujitsu ensures seamless integration between XM Cyber's platform and existing security tools (vulnerability scanners, CSPM, AD scanning), maintaining consistent visibility across all environments.

Prioritization

Identify and prioritize exposures that present genuine, real-world threats by mapping complete attack paths to critical business assets.

Making prioritization actionable

Fujitsu CTEM engineers leverage XM Cyber Attack Graph Analysis™ to pinpoint exposures that truly threaten critical business data, such as customer information, intellectual property, or operational systems. Analysts don't just provide a list of problems, but clearly communicate prioritized risks and provide actionable remediation recommendations tailored to your organization's risk tolerance and business impact

thresholds. As a result, your security and IT teams can confidently allocate resources to activities with tangible business outcomes, improving efficiency and effectiveness – conforming these fixes actually work.

Validation

Confirm actual exploitability of identified exposures and test how effectively existing security controls (EDR, SIEM) detect or prevent the potential attack in real time.

Continuous simulations

XM Cyber continuously executes safe, simulated attacks against the digital twin environment every few hours, significantly reducing false positives and focusing remediation efforts effectively. Validation ensures remediation resources focus exclusively on genuinely exploitable threats, maximizing security ROI and reducing the burden on resource-constrained security teams. Fujitsu oversees the validation process, interpreting results, confirming the efficacy of existing controls, and clearly outlining feasible remediation strategies to customers.
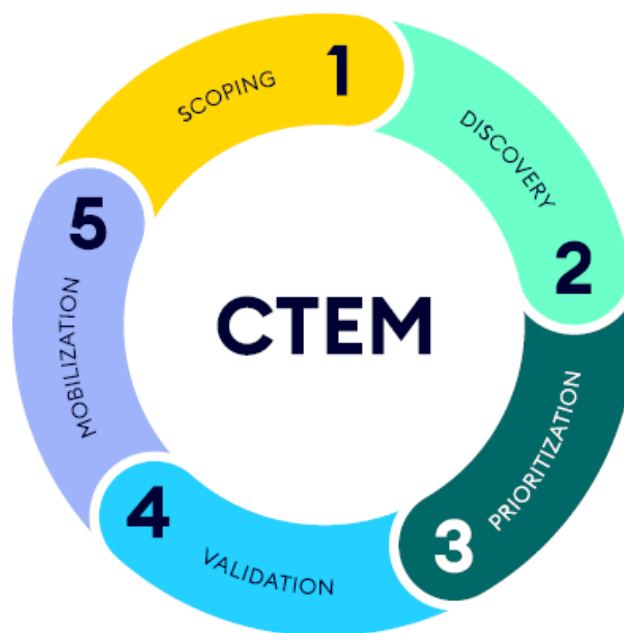
Mobilization

Ensure timely and effective remediation by improving communication, collaboration, and accountability among security, IT, and DevOps teams.

The role of Fujitsu CTEM engineers

Fujitsu CTEM engineers facilitate effective mobilization by:

- Clearly translating security priorities into actionable tasks for IT and DevOps teams.
- Integrating with existing workflow systems (ServiceNow, Jira) to track remediation tickets and monitor their progress.
- Providing clear guidance and verifying that remediations have effectively reduced identified risks.
- Delivering concise, insightful monthly or quarterly security posture reports, clearly demonstrating ongoing improvements in your security resilience.

Why Fujitsu + XM Cyber

The partnership between Fujitsu and XM Cyber uniquely positions enterprises to address modern cyber security challenges through a proven, cohesive approach. By merging XM Cyber's platform with Fujitsu's global managed service excellence, organizations benefit from end-to-end security management that combines cutting-edge technology with operational expertise. A key differentiator of this service is the breadth of exposure detection, encompassing vulnerabilities, misconfigurations, identity and credential issues, cloud security risks, and Active Directory weaknesses. This comprehensive visibility across hybrid environments ensures no exposure type is overlooked, providing a robust defense against attackers who exploit multiple exposure types simultaneously.

Best-in-class technology
XM Cyber delivers industry-leading capabilities through its continuous exposure management platform:

- **Advanced graph analytics**
  XM Cyber Attack Graph Analysis™ provides continuous, real-time visibility of vulnerabilities, misconfigurations, and identity risks across hybrid environments – on-premises, multi-cloud, and Active Directory.
- **Granular identity & configuration insight**
  Beyond traditional CVEs, XM Cyber uncovers critical risks such as overly permissive identities, stored credential issues, and dangerous Active Directory configurations.
- **Secure, auto-updated digital twin**
  XM Cyber's digital twin securely mirrors the organization's hybrid infrastructure, allowing continuous, safe simulation of realistic attack scenarios without disruption to

live environments.

Managed service expertise

Fujitsu brings decades of expertise as the only global systems integrator offering a fully managed CTEM service across North America, EMEA, and Oceania, including:

- **Global scale and reach**
  Fujitsu's global presence ensures consistent, high-quality security management across geographically dispersed operations.
- **Comprehensive consulting and operational delivery**
  From initial business-driven scoping to operational remediation and executive reporting, Fujitsu serves as a single trusted partner across the entire CTEM lifecycle.
- **ROI and resource optimization**
  Fujitsu reduces the frequency and expense of penetration tests and manual security audits. By focusing only on critical exposures, organizations experience less patch fatigue, increased operational efficiency, and optimized resource allocation.

Key differentiators

- **End-to-end coverage**
  Unlike partial solutions, Fujitsu's managed CTEM approach covers the entire exposure management lifecycle – from scoping and discovery to validation, remediation, and mobilization.
- **Adaptability to complex environments**
  CTEM seamlessly handles diverse hybrid environments, supporting scenarios such as multi-cloud, mergers and acquisitions, global supply chains, and operational technology (OT).
- **Ongoing improvement and maturity**
  As an organization's infrastructure evolves, so does the Fujitsu CTEM managed service. It is designed for continuous improvement, never remaining static or relying on one-time assessments.

"Fujitsu has over 40 years of experience designing and delivering large-scale security services for both public and private sector customers. Our CTEM engineers provide consulting, scoping, and ongoing mobilization, using XM Cyber's platform to pinpoint exposures and ensure vulnerabilities actually get fixed. This truly is an end-to-end service." James Frith, Global CTEM Service Owner, Fujitsu

Onboarding the service

The onboarding process is structured around clear milestones and focused deliverables, ensuring you can quickly leverage the full value of the Fujitsu CTEM managed service without overburdening your internal teams.

Onboarding phase	Activities	Outcomes & deliverables
Kick-off & scoping	• Initial stakeholder meetings • Scoping workshops to identify critical assets and establish business priorities	• Defined critical assets and business priorities • Agreed service scope and objectives

Deployment & integration	- Sensor deployment - Integration with existing cyber ecosystems and ticketing systems (e.g., ServiceNow, Jira)	- Platform set-up and operational readiness - Validated integrations
Initial threat assessment & remediation plan	- Attack scenario creation and initial risk analysis - Identify critical exposures and choke points	- Prioritized remediation plan tailored to business- critical assets - Clear, actionable remediation guidance
Validation & operationalization	- Continuous validation of remediation effectiveness - Regular security posture reporting and review	- Confirmed remediation outcomes and measurable risk reduction - Established ongoing operational processes

Conclusion: Fix what matters most and strengthen your security resilience

Enterprises face countless exposures, but not all pose serious risk. The key is to fix what matters most. The Fujitsu CTEM managed service uses an attacker-centric approach to identify, prioritize, and remediate only the exposures that truly threaten your critical assets. This targeted approach delivers measurable risk reduction while maintaining operational efficiency. With clear executive-level metrics and seamless integration into your existing workflows, you gain actionable insights that drive business value and resilience.

Recommended next steps

- Schedule a scoping workshop: Engage Fujitsu's expert team to clearly define your critical business assets, threat posture, and immediate risk reduction opportunities.

- Run a Proof of Value (PoV): Demonstrate immediate operational impact by modeling your most critical risk scenarios, clearly illustrating the CTEM framework's strategic value and return on investment.

Contact us:

- Fujitsu CTEM managed service
- James Frith – Global CTEM Service Owner, Fujitsu
- James.frith@fujitsu.com
- Visit us at www.fujitsu.com/global/ctem

Align your enterprise security strategy to a recognized Gartner framework with immediate operational impact.

FAQ

What makes CTEM different from traditional vulnerability management?

CTEM offers an attacker-centric approach that focuses on genuine risks to critical business assets rather than just common vulnerabilities and exposures (CVEs).

How does CTEM help improve operational efficiency?

By targeting strategic choke points and highlighting exploitable exposures, CTEM helps reduce unnecessary patches, accelerate triage processes, and optimize resource utilization.

Documents / Resources

	[FUJITSU Continuous Threat Exposure Management](#) [[pdf](#)] User Guide Continuous Threat Exposure Management, Threat Exposure Management, Exposure Management, Management

References

- [User Manual](#)

📁 FUJITSU

🏷 Continuous Threat Exposure Management, Exposure Management, FUJITSU, Management, Threat Exposure Management

Leave a comment

Your email address will not be published. Required fields are marked *

Comment *

Name

Email

Website

☐ Save my name, email, and website in this browser for the next time I comment.

Post Comment

Search:

e.g. whirlpool wrf535swhz   **Search**