

Gartner Insights

CISOs Must Focus on the Outcomes of Preemptive Cybersecurity

Charlie Winckless, Craig Lawson, Bryan Haley



CISOs Must Focus on the Outcomes of Preemptive Cybersecurity

5 August 2026 - ID G00859378 - 9 min read

By: Charlie Winckless, Craig Lawson, Bryan Haley

Initiatives: CxO Leadership

The term preemptive cybersecurity is emerging as numerous vendors rebrand existing products as “preemptive,” sometimes only adding simple, additional capabilities. This insight explains what controls and visibility CISOs should be prioritizing to address the emerging threats they face.

Insights at a Glance

Preemptive cybersecurity aligns with existing proactive approaches to cybersecurity. It adds focus beyond prevention, detection, and response and seeks to improve foresight capabilities to limit an attack’s impact early, optimally preventing initial access. Vendors are increasingly pushing this concept, but it faces key challenges:

- Most organizations will need a cultural shift to adopt preemptive approaches, as predicting cyberthreat activity accurately is largely aspirational.
- AI-washing, both as a threat and as a capability, is prevalent in cybersecurity product marketing today.
- Many capabilities promoted as preemptive exist in current platforms. Combining them, however, has the potential to add resilience.

Understanding the reality around preemptive security is important for CISOs who face heightened pressure to distinguish hype from material security value, particularly in the “age of AI,” where both threats and the capabilities of offerings continue to be overstated. While benchmarks and lab experiments around AI attackers are impressive, today, true AI-powered attacks remain very rare in the real world. Rather, adversaries are using AI to scale traditional phishing, automate tasks, and compensate for skill gaps. At the same time, initiatives such as Project Glasswing and Daybreak are employing frontier LLMs and accelerating the scale of vulnerability disclosures that organizations must address. All of this demands a continued focus on ensuring that appropriate cybersecurity controls are implemented and that budgets are targeted where the highest value can be obtained.

Preemptive cybersecurity approaches can be broken into four core domains, often bolstered by managed services directly from the vendor or another partner:

- **Preemptive exposure management:** Simulates real-world attacks to validate control effectiveness and thereby improves visibility into control gaps before they are exploited.
- **Adversary management and threat intelligence:** Provides tactics, techniques- and procedures-driven insight into adversary behavior and helps predict likely attacks. When combined with other controls, this enables more targeted protection.
- **Adversary disruption:** Uses deception, threat hunting, and intelligence-driven controls to slow attackers and generate high-fidelity signals that incidents are occurring.
- **Posture and policy management:** Continuously assesses (and optionally hardens) configurations across cloud, endpoint, and infrastructure, and reduces attack surface amid rising AI-driven vulnerability discovery.

Issue

Preemptive cybersecurity is being applied as a label to both new and existing technologies by vendors. This is particularly true given the vulnerability discovery capabilities of frontier AI models; there is AI-washing both in creating demand for and in labeling these technologies as preemptive. This insight provides guidance on the value of the concepts associated with the term and on existing technologies that can be considered part of such an approach.

AI-washing is common both in marketing the need for preemptive cybersecurity and in describing product delivery. CISOs must focus on the outcomes delivered and whether existing tools support these outcomes, not on the hype around AI.

Preemptive cybersecurity consists of four core domains, each addressing different needs – though these core domains do overlap.

The four domains are:

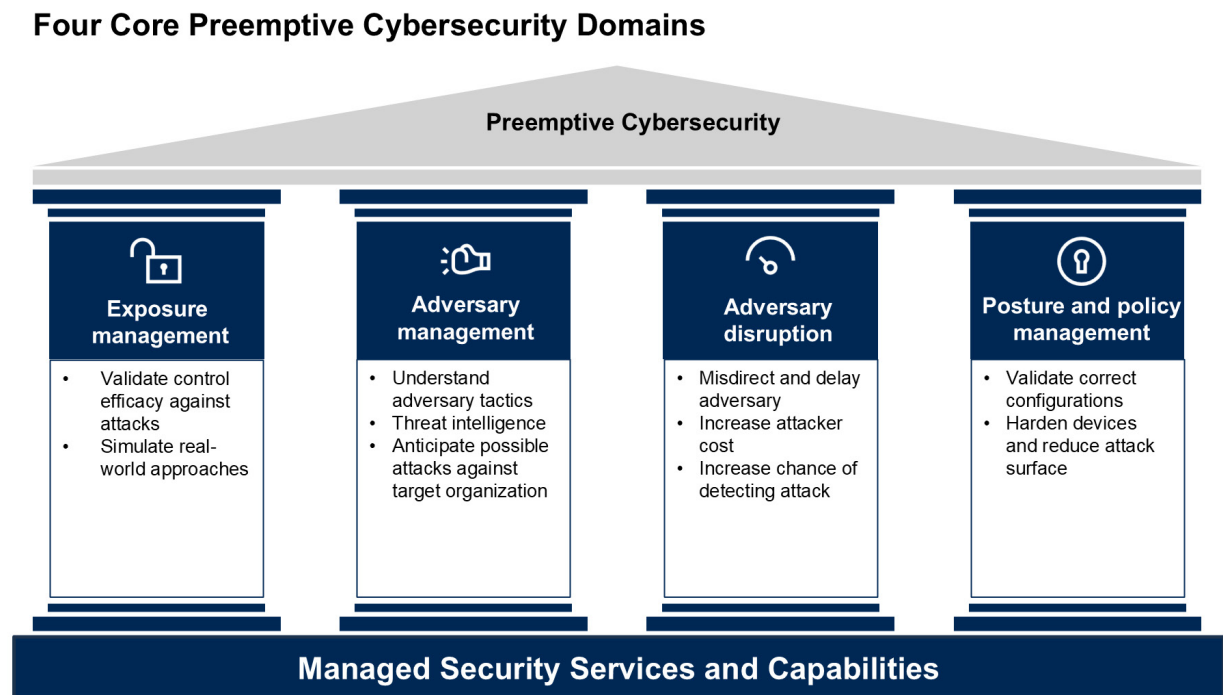
- Preemptive exposure management
- Adversary management and threat intelligence (adversary management)
- Adversary disruption
- Posture and policy management

Many of these domains are covered by technologies that already exist in many organizations. CISOs should clearly understand the additional value that add-on capabilities may provide before investing. Approaches will often include managed services delivered by the vendor to enhance its technology.

Impact

Understanding and decoding hype is critical to assist CISOs in ensuring they invest in the right technologies at the right time to appropriately secure their organizations. This is especially true in the “age of AI,” where many technologies and threats are surrounded by extreme hype. For instance, today, AI-powered attacks are still rare, though attackers are augmenting their approaches by using AI tools. These tools are used to make common attacks, such as phishing, more efficient, to automate and augment attacks, and to offset a lack of knowledge or skill on the part of the attacker. Marketing, however, would have us believe that AI attacks will be dramatically different from what we see today, rather than simply faster, enabling less-skilled adversaries to upskill.

Figure 1: Four Core Preemptive Cybersecurity Domains



Source: Gartner
859378_C

Gartner

Preemptive cybersecurity is being positioned as part of the solution to an increasingly complex and volatile threat landscape. As an approach, it can help proactively defend against all classes of attacks, both making it harder for an attacker to succeed and give defenders more time and a greater chance to detect an attack — an urgency that is magnified as LLM-delivered vulnerability discovery accelerates the number of vulnerabilities that must be managed. However, it is not just a technology investment and will require significant investment in and upskilling of staff, and will be additive to, rather than a replacement for, existing security controls.

More Detail

CISOs considering preemptive cybersecurity solutions must ensure that they do not already have a similar capability being delivered as part of their existing product and service portfolio. These tools must be treated as additive to a well-established and mature program; they are not substitutes or replacements for cyber hygiene, nor do they replace core skills or technology gaps.

Even where a capability does not exist today, a pragmatic evaluation of its utility is essential. For example, it is extremely rare for organizations to be willing to automatically remediate discovered issues due to the concern over potential disruption, and this may limit preemptive cybersecurity offerings to detecting, rather than fixing issues, thereby increasing, rather than reducing overhead.

Without a cultural shift, many CISOs will be unable to fully utilize preemptive cybersecurity approaches due to concerns about their impact on operational stability.

Each of the four pillars shown in Figure 1 will provide different benefits and capabilities. Not all capabilities will be necessary for all organizations or included in all offerings. In particular, many organizations will require vendor- or third-party-led managed services to realize significant value from these offerings unless they have large and high-level security teams.

Preemptive Cybersecurity Technical Domains

Preemptive Exposure Management

What is it?

Preemptive exposure management involves tooling to test for vulnerabilities, assess how they expose your organization to breach activity, and evaluate the security controls you have in place to ascertain their effectiveness. These offerings simulate real-world attacks (ideally derived from data or capabilities around adversary intelligence) against extant security controls. This can be against actual controls, or in some cases, a simulated digital twin to reduce potential impact.

Core Benefit

The result of implementing this is better visibility into how effective the implemented controls are. Where controls are insufficiently effective, it gives visibility into where and why they fail prior to an actual attack.

Adversary Management and Threat Intelligence

What is it?

Adversary management and threat intelligence involve using data and context to understand likely trends from adversaries. These trends will include TTPs that are in use and increasing as well as targets (both technical and operational). On its own, adversary management allows for **scenario planning** and understanding of current situations. It is of most value when combined with one of the other pillars to provide actionable enforcement.

Core Benefit

Use of adversary management and its consumption by other tools provide targeted protection against known current attack techniques. Curating and tuning adversary management to your organization provides more granular protection.

Adversary Disruption

What is it?

Disruption is the approach of accepting that attacks will occur and working to delay or misdirect such attacks. This includes deploying techniques such as deception and honeypots that provide a clear signal of an attack when triggered, conducting proactive threat hunting (often as a service, and tied to effective adversary management), and operationalizing threat intelligence in other controls to give targeted and granular protection.

Core Benefit

Adversary disruption serves three purposes. It may slow down an attack as an attacker spends time (or automated resources) on a target of no value. It also can provide a clear signal of an attack, allowing incident response efforts to be triggered. Lastly, data from disruptive technologies (especially deception technologies) can be taken back into other areas of security and used to feed those controls as attacker TTPs.

Posture and Policy Management

What is it?

Successful attacks often take advantage of failures in the configuration of your environments. This is especially true in the case of cloud environments, but configuration risks have also been exploited in other areas, specifically in campaigns such as Fortbleed.¹ As the number of vulnerabilities organizations have to manage increases due to the effect of LLM-driven vulnerability discovery and the advanced capabilities of frontier AI models, hardening configurations is even more vital than before. Well-hardened devices present a smaller attack surface and will expose fewer vulnerabilities for an attacker to attempt to exploit.

In the sense of preemptive cybersecurity, posture and policy management involves the continuous validation of device configuration. Such an approach is common in hyperscale cloud, where cloud security posture management (and **saas security** posture management), **cloud infrastructure entitlement management** and **cloud native application protection platforms** can take advantage of the open and well-defined APIs from major cloud service providers and evaluate their configurations for security risks. Similarly, unified endpoint management solutions can harden many user endpoints. Traditional network and security infrastructure must also be considered part of your attack surface, however, and may not always be accessible from these controls.

Core Benefit

Ensuring continuous posture assessment (configuration against threats, patching, hardening, etc.) of devices and environments has several benefits. At a minimum, it can show compliance with policy to an auditor. With the right standards and policies, it reduces the attack surface and minimizes the impact of an incident that does compromise a hardened device.

With all preemptive cybersecurity offerings, many organizations will also benefit from a managed or supported service, either from the vendor or a third-party provider.

— *Source: Gartner (August 2026)*

Technologies Aligned With Preemptive Cybersecurity

Table 1 shows current technologies that are aligned with a preemptive approach. Some — in fact many — of these may be extended capabilities within existing platforms.

Table 1: Preemptive Cybersecurity Domains and Current Offerings

(Enlarged table in Appendix)

Preemptive Cybersecurity Domain ↓	Core Current Offerings ↓
Preemptive exposure management	■ Adversarial exposure validation (see: Market Guide for Adversarial Exposure Validation) ■ Breach and attack simulation ■ Automated security control assessment (see: Innovation Insight: Automated Security Control Assessment) ■ Autonomous exposure remediation (see: Hype Cycle for Security Operations, 2026)
Adversary management and threat intelligence	■ Cyberthreat intelligence (see: Magic Quadrant for Cyberthreat Intelligence Technologies) ■ Unified cyber risk intelligence (see: The Evolution of Threat Intelligence Is Unified Cyber Risk Intelligence) ■ Cyberthreat intelligence management platforms (see: Hype Cycle for Security Operations, 2026)
Adversary disruption	■ Deception (see: Guide to Network Security Concepts) ■ Firewalls (with threat intelligence integration) (see: Magic Quadrant for Hybrid Mesh Firewall) ■ NDR (with threat intelligence integration) (see: Magic Quadrant for Network Detection and Response) ■ Threat hunting ■ Detection engineering
Posture and policy management	■ Cloud native application protection platforms (see: Market Overview for Cloud-Native Application Protection Platforms) ■ Cloud security posture management ■ Cloud infrastructure entitlement management ■ Kubernetes security posture management ■ AI security posture management ■ Data security posture management (see: Market Overview for Data Security Posture Management) ■ Network security posture management ■ Unified endpoint management (see: Market Overview for Endpoint Management Tools) ■ Endpoint protection platforms (see: Magic Quadrant for Endpoint Protection)

Source: Gartner (August 2026)

Contributors

Pete Shoard

Evidence

¹ CSA Research Note: FortiBleed Default Credentials, Cloud Security Alliance.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

[Emerging Tech Impact Radar: Preemptive Cybersecurity](#)

Preemptive Cybersecurity: Creating the Next Wave of Cybersecurity Growth Opportunities Hype Cycle for Security Operations, 2026

© 2026 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's Business and Technology Insights Organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner insights may address legal and financial issues, Gartner does not provide legal or investment advice and its insights should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its insights is produced independently by its Business and Technology Insights Organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)." Gartner insights may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.

Table 1: Preemptive Cybersecurity Domains and Current Offerings

<i>Preemptive Cybersecurity Domain</i> ↓	<i>Core Current Offerings</i> ↓
Preemptive exposure management	■ Adversarial exposure validation (see: Market Guide for Adversarial Exposure Validation) ■ Breach and attack simulation ■ Automated security control assessment (see: Innovation Insight: Automated Security Control Assessment) ■ Autonomous exposure remediation (see: Hype Cycle for Security Operations, 2026)
Adversary management and threat intelligence	■ Cyberthreat intelligence (see: Magic Quadrant for Cyberthreat Intelligence Technologies) ■ Unified cyber risk intelligence (see: The Evolution of Threat Intelligence Is Unified Cyber Risk Intelligence) ■ Cyberthreat intelligence management platforms (see: Hype Cycle for Security Operations, 2026)
Adversary disruption	■ Deception (see: Guide to Network Security Concepts) ■ Firewalls (with threat intelligence integration) (see: Magic Quadrant for Hybrid Mesh Firewall)

Preemptive Cybersecurity Domain ↓	Core Current Offerings ↓
	■ NDR (with threat intelligence integration) (see: Magic Quadrant for Network Detection and Response) ■ Threat hunting ■ Detection engineering
Posture and policy management	■ Cloud native application protection platforms (see: Market Overview for Cloud-Native Application Protection Platforms) ■ Cloud security posture management ■ Cloud infrastructure entitlement management ■ Kubernetes security posture management ■ AI security posture management ■ Data security posture management (see: Market Overview for Data Security Posture Management) ■ Network security posture management ■ Unified endpoint management (see: Market Overview for Endpoint Management Tools) ■ Endpoint protection platforms (see: Magic Quadrant for Endpoint Protection)

Source: Gartner (August 2026)

Actionable, objective insights

Position your organization for success. Explore these additional complimentary resources and tools for CIOs:

Article



Don't Delay in Building Preemptive Cybersecurity Solutions

Learn how to proactively defend against AI-powered cyberthreats.

[Read Now](#)

Hub Page



Gartner AI Hub

Discover practical AI insights for confident decision making.

[Learn More](#)

Virtual Briefing



IT 2030: Empowerment or Chaos? CIO's Role in AI-Powered Democratization

Learn how CIOs can enable AI innovation while managing risk.

[Watch Now](#)

Tool



Gartner AI Maturity Assessment

Assess your AI maturity and build a roadmap to scale impact.

[Explore Tool](#)

Already a client? Get access to even more resources in your client portal.

[Log In ↗](#)

Connect with us

Get actionable, objective business and technology insights that drive smarter decisions and stronger performance on your mission-critical priorities.

Contact us to become a client:

U.S.: 1 855 322 5484

International: +44 (0) 3300 296 946

[Become a Client](#)

Learn more about Gartner for CIOs
gartner.com/chief-information-officer

Stay connected to the latest insights



Attend a Gartner conference
[View Conference](#)