Talos が読み解くサイバー脅威の転換期、Cisco のフロンティア AI への対応

武田 貴寛
Talos, Threat Inteligence Interdiction, Outreach Team, Security Research Engineer

寺下 健一
CxO Advisor, Office of the CTO

July 2026

Project Glasswing

Securing critical software for the AI era

cisco

Daybreak

Frontier AI for defenders.

Start scan with Codex Security plugin | Contact Cyber sales

Building the future of cyber defense

accenture · Akamai · ncc group · Capgemini · CATO NETWORKS · CHECK POINT

CISCO · CLOUDFLARE · cognizant · CROWDSTRIKE · DARKTRACE · elastic

EY · FORTINET · GUIDEPOINT SECURITY · IBM · KPMG · okta

Palantir · paloalto NETWORKS · proofpoint · pwc · SentinelOne · SoftBank

SOPHOS · SPECTEROPS · tenable · TrendAI · WIZ · zscaler

cisco

Claude Mythos のインパクト

271個

当時最新の
Firefoxバージョンに対して
発見された脆弱性の数

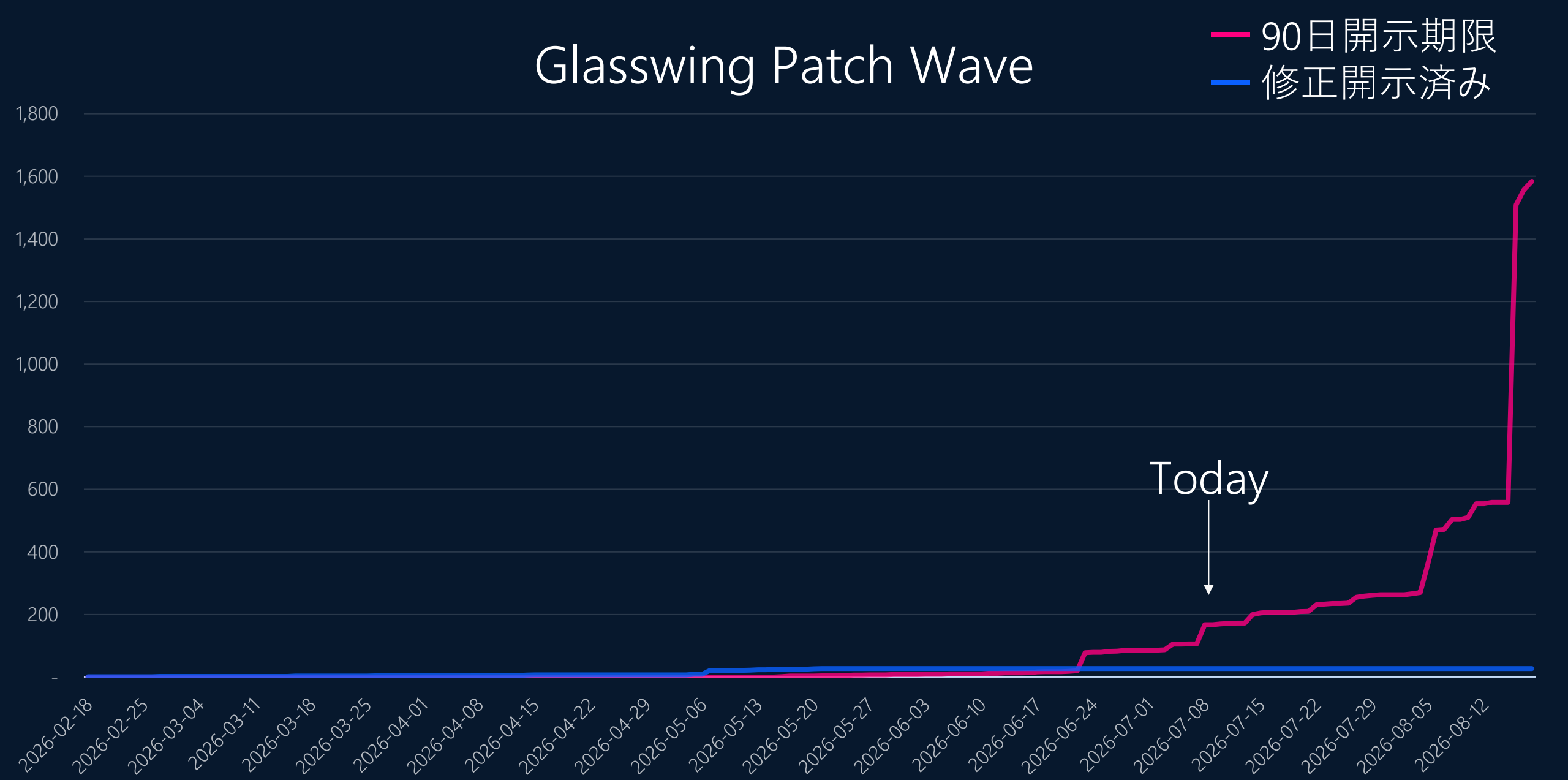
27年

発見されたOpenBSDの
脆弱性がこれまで
存在していた年月

23,000個

1,000以上のOSSを
対象にした検査で
発見された脆弱性の数

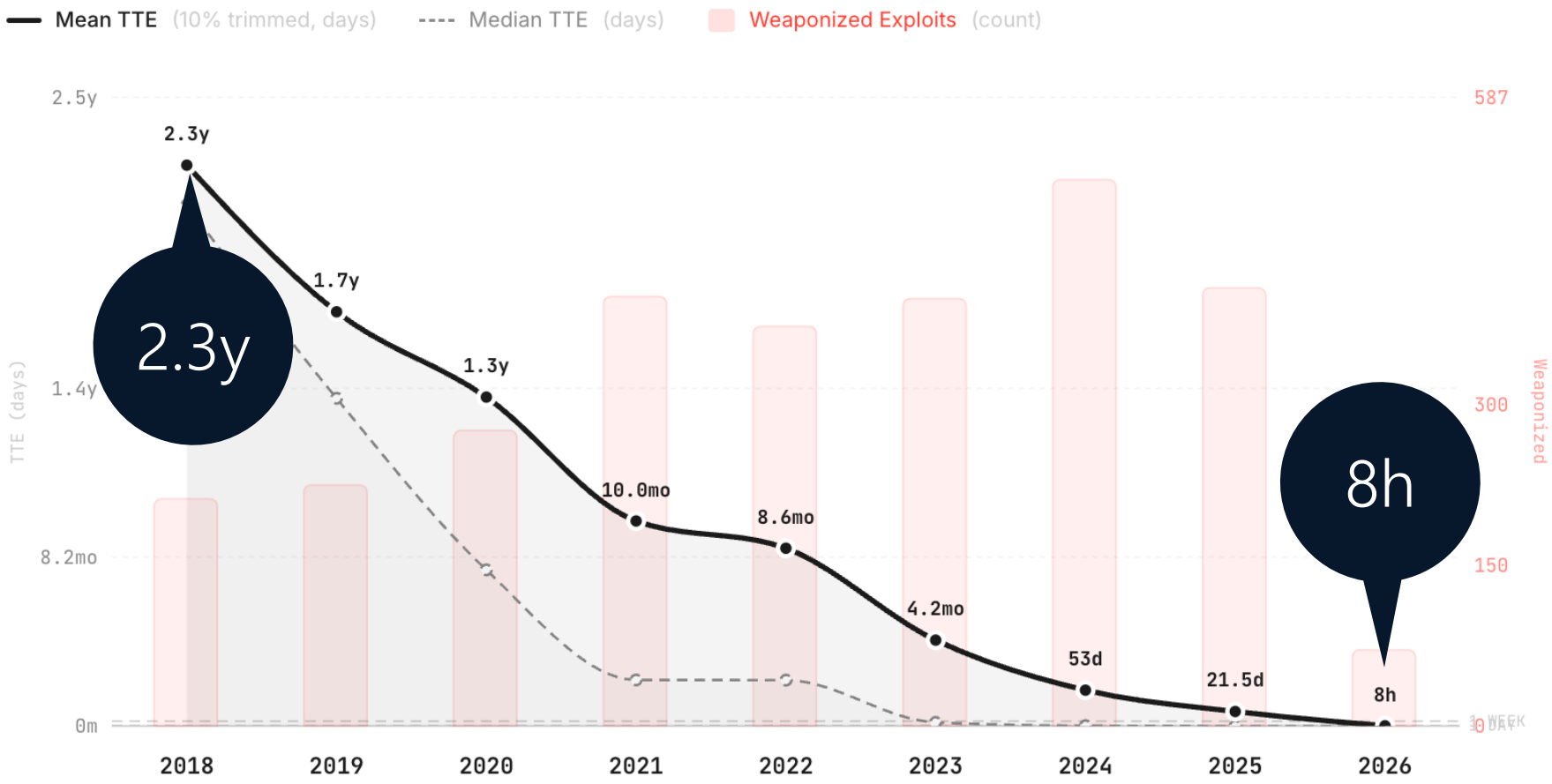
Glasswing Patch Wave

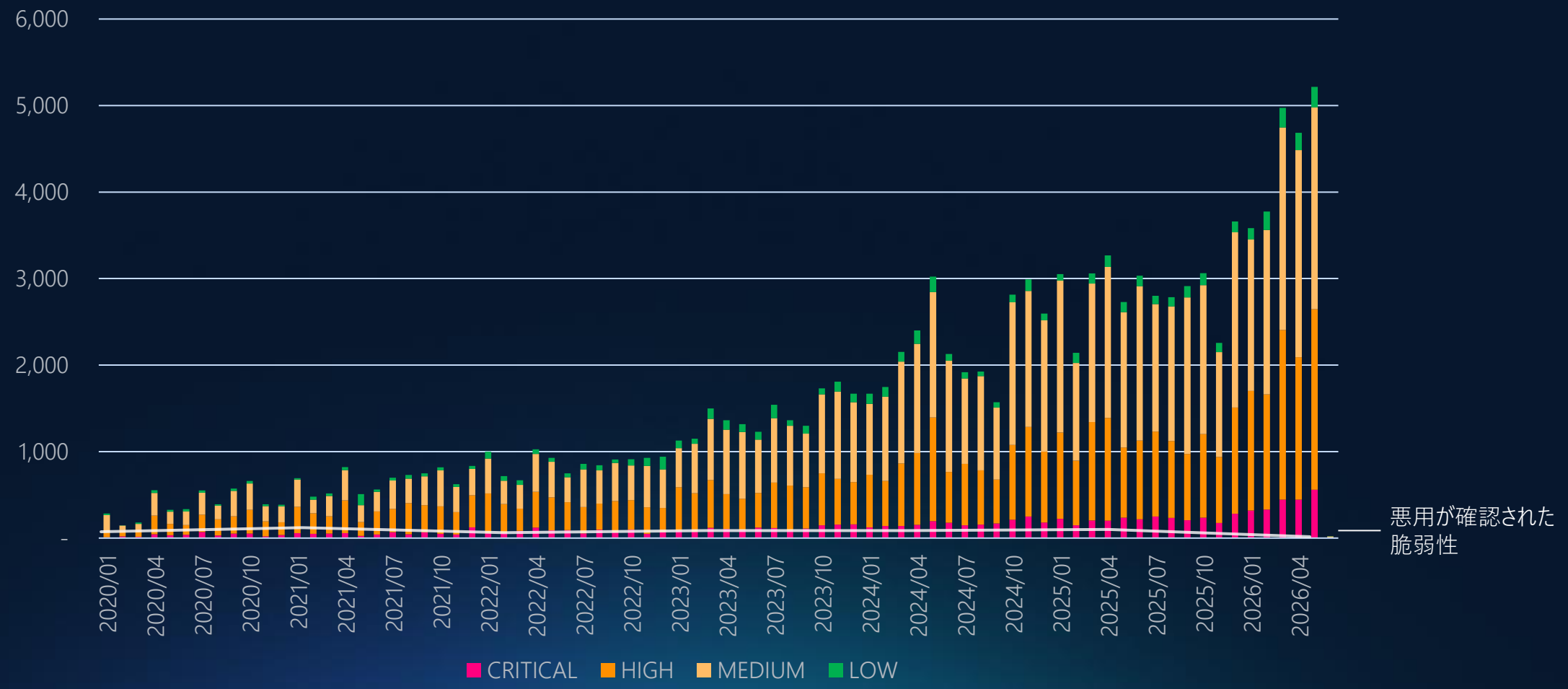


As of June 26

From Vulnerability to Exploitation

TTE measures the gap between CVE public disclosure and first confirmed in-the-wild exploitation. Zero = same-day.





悪用された脆弱性は、全体の1%未満

NIST. "CVE"
CISA. "KEV Catalog"

米国政府は、4つのリスク変数に基づくセキュリティパッチの優先順位付けを実装するためのガイダンスを発表

CISA. (2026). "BOD 26-04: Prioritizing Security Updates Based on Risk"

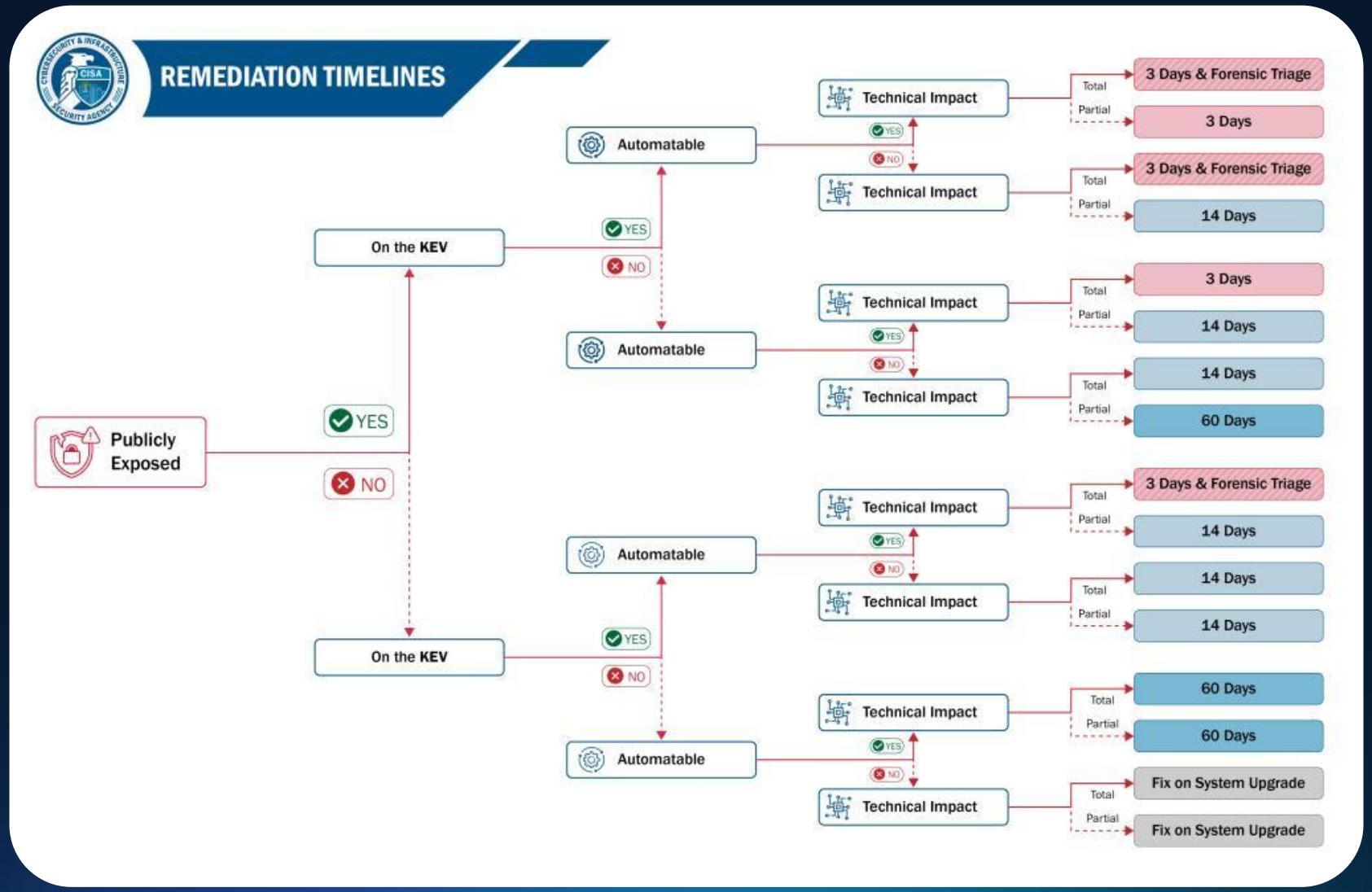
リスクを決定する変数

アセットの露出
悪用のエビデンス
悪用の自動化
技術的影響範囲

対応タイムラインの動的設定

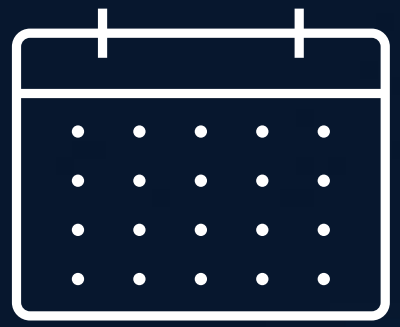
最短で3日以内の修正と、
システム侵害を確認する
フォレンジックが義務付けられる。

CISA. (2026). "BOD 26-04: Prioritizing Security Updates Based on Risk"

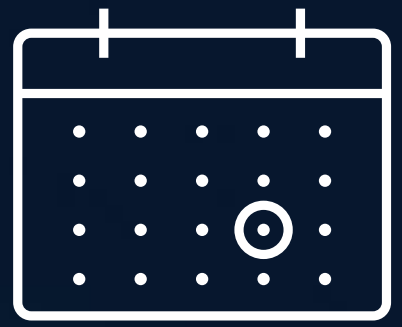


CISA. (2026). "BOD 26-04: Prioritizing Security Updates Based on Risk"

Cisco 脆弱性開示ポリシーの変更（2026年7月から）



脆弱性開示は
毎週水曜日*



脆弱性開示は
毎月第1第3水曜日*

7日前に事前予告

* 日本時間木曜日早朝1時頃

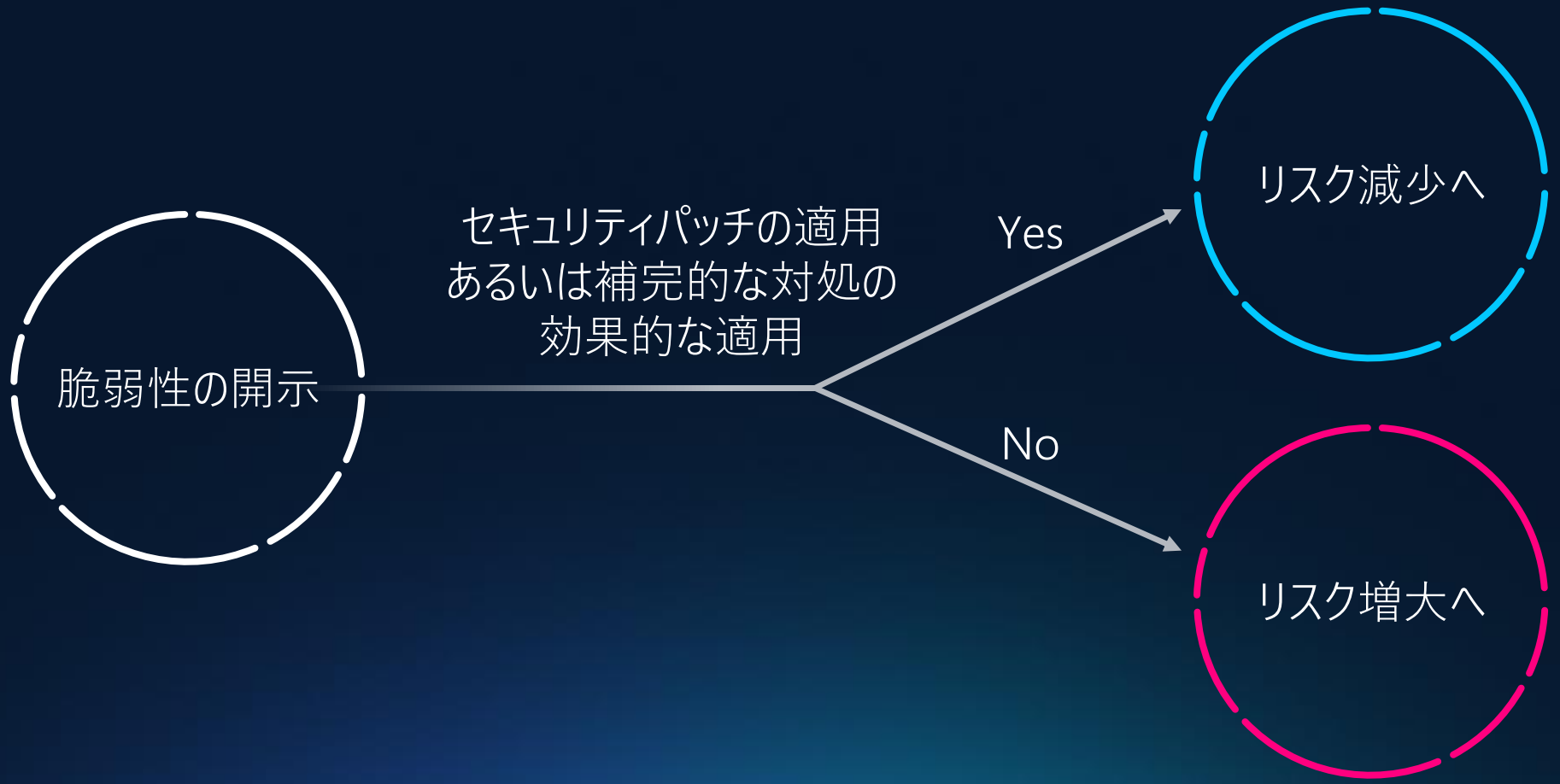
パッチ管理プロセスの効率化と計画的運用の実現

パッチスケジュールをまとめることによる、適用周期の軽減

事前予告による、計画的メンテナンスの機会提供

CWE毎にバンドルされたCVE。CVE毎の脆弱性対応から、
種類区分のコントロールによる、対応と簡素化

脆弱性開示の、本質的な理解



攻撃者より早く対処することが、求められるプロアクティブな防衛戦略

技術的負債は、攻撃者のターゲット

48%

ネットワーク資産のうち、老朽化または旧式化の資産が占める割合

40%

悪用された上位100件の脆弱性のうち、EOLシステムに影響するものの割合

32%

攻撃の影響を直接受ける資産のうち、導入から10年以上経過した資産の割合

WPI Strategy & Cisco. (2025). "Update Critical"
Cisco. (2026). "Cisco Talos 2025 Year in Review"

対策検討の方向性

脆弱性フレームワークの近代化

レガシーテクノロジーの更新

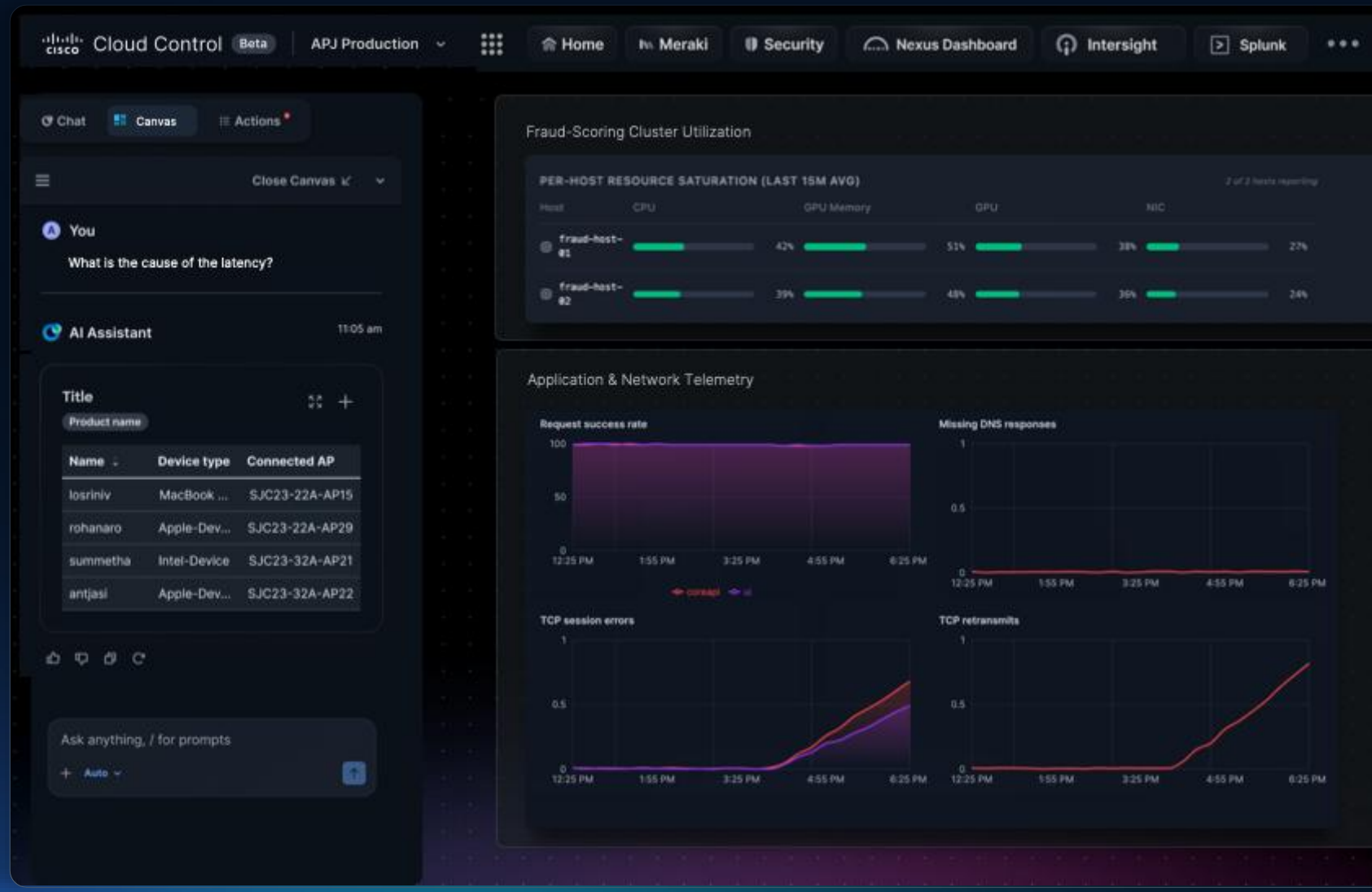
補完的コントロール

キャパシティの構築と国際的な整合

Cisco Cloud Control

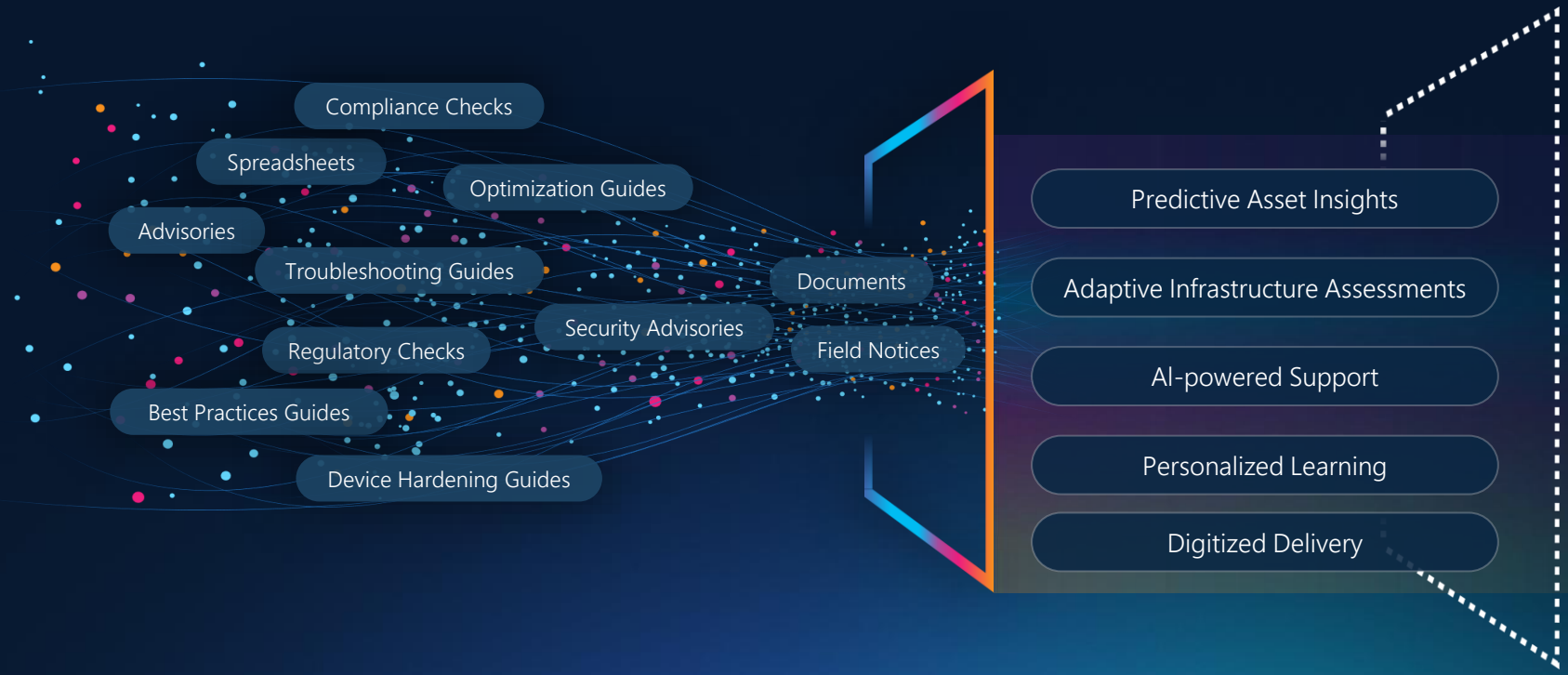
One operating model

- Network
- Security
- Identity
- Splunk



Cisco IQ

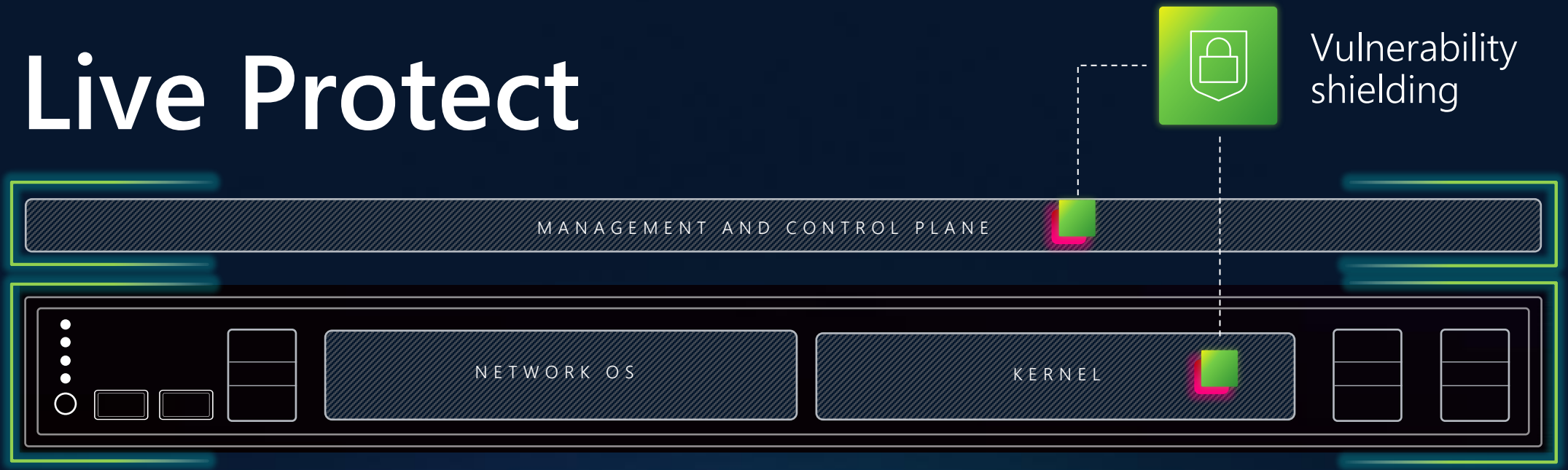
人間の専門知識と、エージェント型知能が融合



Benefits

- Complete landscape clarity
- Proactive resilience
- Rapid resolution
- Contextualized professional services

Live Protect



CISCO NETWORK DEVICES
STARTING WITH N9000

稼働中システムに適用

即時保護し、計画的にパッチ適用

ダウンタイムなし、再起動なし

継続的な再評価


CISCO