Cisco Secure Access for Government

AI Access protect your Organization

Milan Habrcetl, Account Executive Security

mhabrcet@cisco.com

3.2.2026

$9.3M

Average cost of a data breach per incident in the United States in 2024

Source: IBM, Cost of Data Breach Report, 2024

What’s driving interest in security service edge (SSE)?

- Constant threat of advanced cyberattacks on government agencies
- Need to modernize & simplify operations to improve incident response
- Increased insider threats
- Compliance requirements/Zero trust mandates across hybrid environments
- Improve human effectiveness by removing friction
- AI application

Support Continuous Enforcement and Mission Continuity

Per Office of Management and Budget (OMB) mandate and several other security frameworks

Zero trust is required in today’s workplace

Addressing all kinds of:

Users
(and devices)

Places
(and networks)

Apps
(and data)

… yet most zero trust projects are failing to deliver.

Modern security must be...

Adaptive

Safer for everyone and everything

Empowering

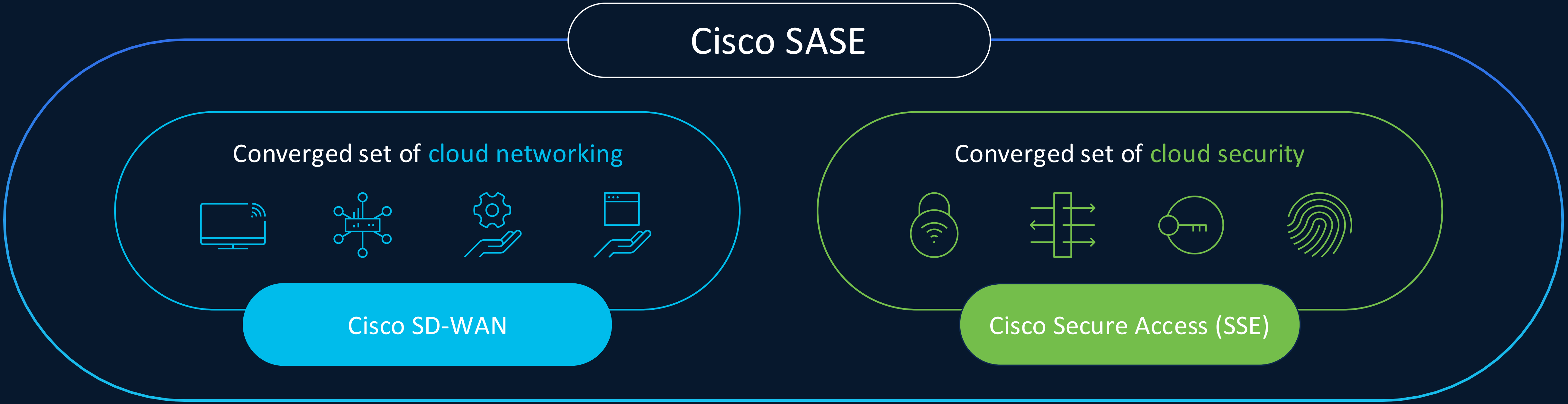
Better for users

Cost efficient

Easier for IT

Cisco SASE: Modernize across networking and security

Your FedRAMP SASE solution for a hyper-distributed world



Cisco SASE

Converged set of cloud networking

Cisco SD-WAN

Converged set of cloud security

Cisco Secure Access (SSE)

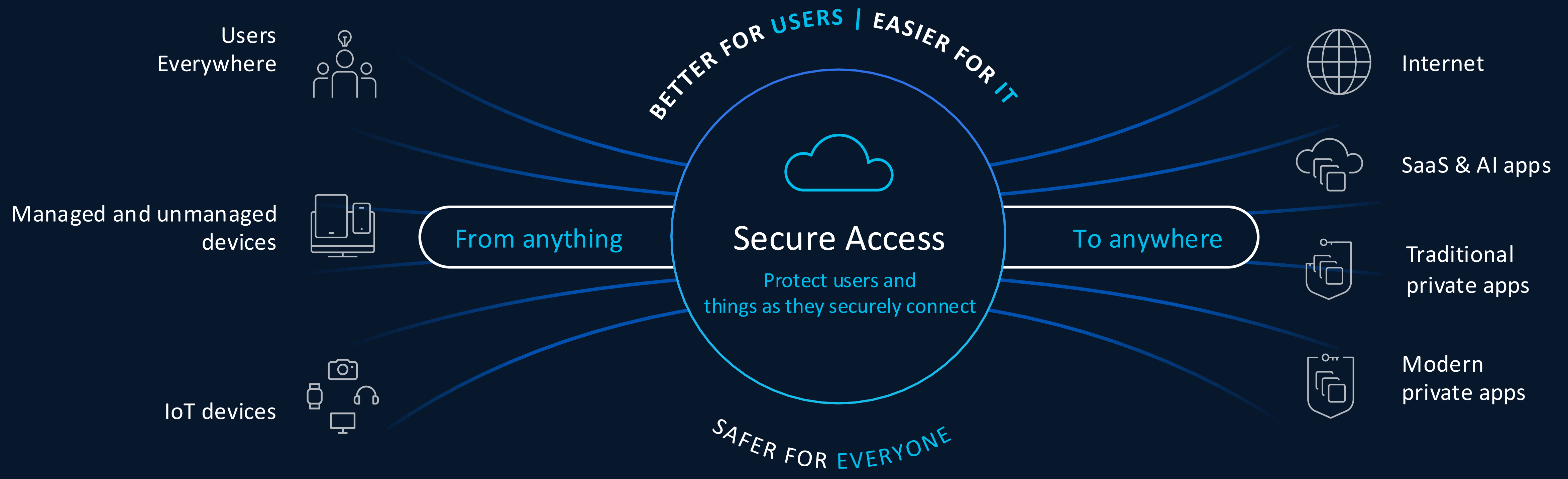
FedRAMP

GovRAMP

TX-RAMP

Cisco Secure Access for Government

FedRAMP Moderate-authorized cloud-native security grounded in zero trust



Remote	Campus	Regional	Mobile	Airplane	Overseas	Field	...

Meet cybersecurity compliance mandates

with Cisco Security Service Edge (SSE) for Government

CISCO SECURE ACCESS FOR GOVERNMENT

Authorizations

- FedRAMP
- GovRAMP
- TX-RAMP

- Zero Trust Network Access
- Cloud Access Security Broker (CASB) *
- Secure Web Gateway (SWG?.DLP) *
- Firewall as a Service (FWaaS)*
- VPNaaS
- DNS-layer security
- Data loss Prevention *
- Cisco Talos Threat Intelligence
- Remote Browser Isolation (RBI)
- Advanced Malware Protection
- Protective DNS Integration

Cisco Secure Access for Government

Proven cloud-native security converged into one service

SWG
>5 years

Advanced Malware Protection
>7 years

CASB
>5 years

DUO Posture
>4 years

ZTNA
>4 years

Cloud Firewall
>5 years

Secure Client
>3 years

DNS
>12 years

VPN Termination
>10 years

DLP
>5 years

RBI
>5 years

Cisco
Secure Access

- Single Console
- Single Client
- Unified Policies

Protecting 30,000+ customers | More than 220M endpoints

Cisco Talos Threat Intelligence

Leverage experts and AI for adaptive security – keeping you ahead of new threats

Unmatched visibility across the threat landscape powered by experts, data, and Gen AI

800B

security events/**day**

~2,000

new samples/**minute**

~9M

emails blocked/**hour**

~2,000

domains blocked/**second**

AI Policies: Protecting the usage of AI

Protect intellectual property as it flows in and out of AI systems

Threat Visibility

Discover and Assess Activities

Leakage Prevention

DLP Inspection of Prompts/Uploads

Threat Prevention

Block Apps and Control Downloads

Discovers and controls over 1200 Gen AI apps (including APIs)

Note: Commercial version of this capability is available.
FedRAMP version is phased, with Phase 1 authorization expected in June 2025

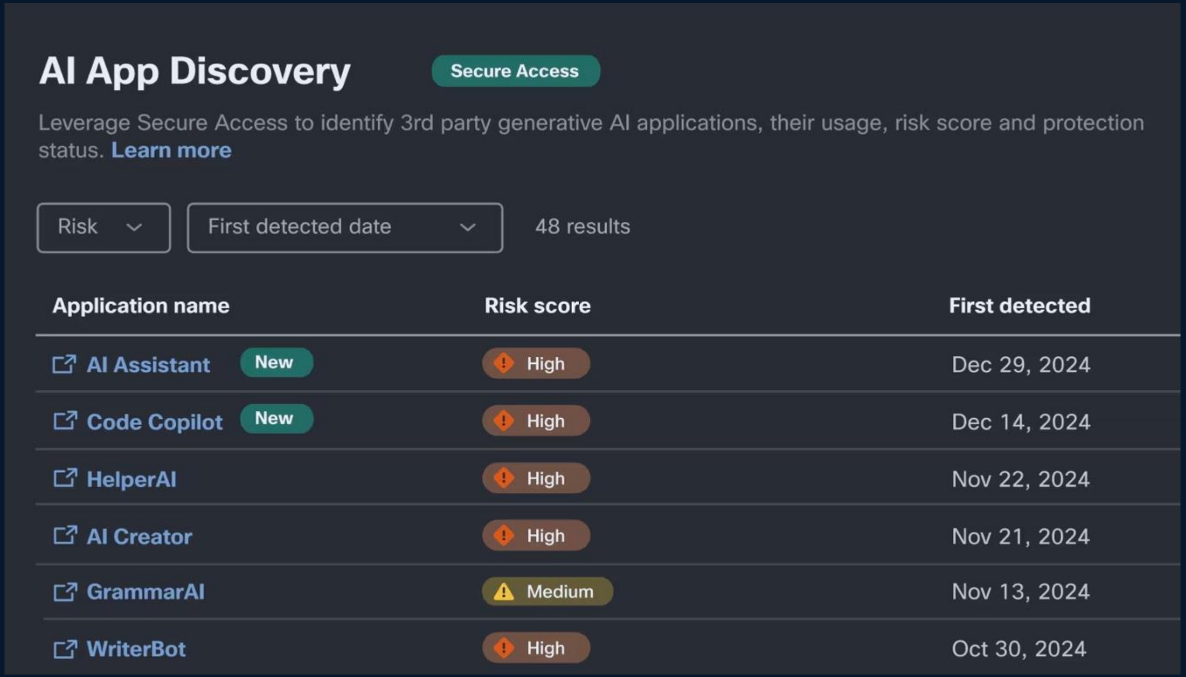
AI Access – Control Sanctioned and Unsanctioned GenAI apps

Superior visibility & control

- Discover Shadow GenAI apps – Allow, block and monitor
- Granular control for 1200+ GenAI apps
  - Sensitive documents
  - Source code
- Machine learning pretraining finds unstructured data and documents
  - Patent applications
  - M&A
  - Financial statements and more

Zero-Friction Security

- Built into Secure Access, no extra license
- Single unified policy framework
- Start fast with pre-built ML identifiers for classifying documents + AI guardrail protection



AI App Discovery

Leverage Secure Access to identify 3rd party generative AI applications, their usage, risk score and protection status. Learn more

48 results

Application name	Risk score	First detected
AI Assistant New	High	Dec 29, 2024
Code Copilot New	High	Dec 14, 2024
HelperAI	High	Nov 22, 2024
AI Creator	High	Nov 21, 2024
GrammarAI	Medium	Nov 13, 2024
WriterBot	High	Oct 30, 2024

1200+ Apps
Visibility & Control

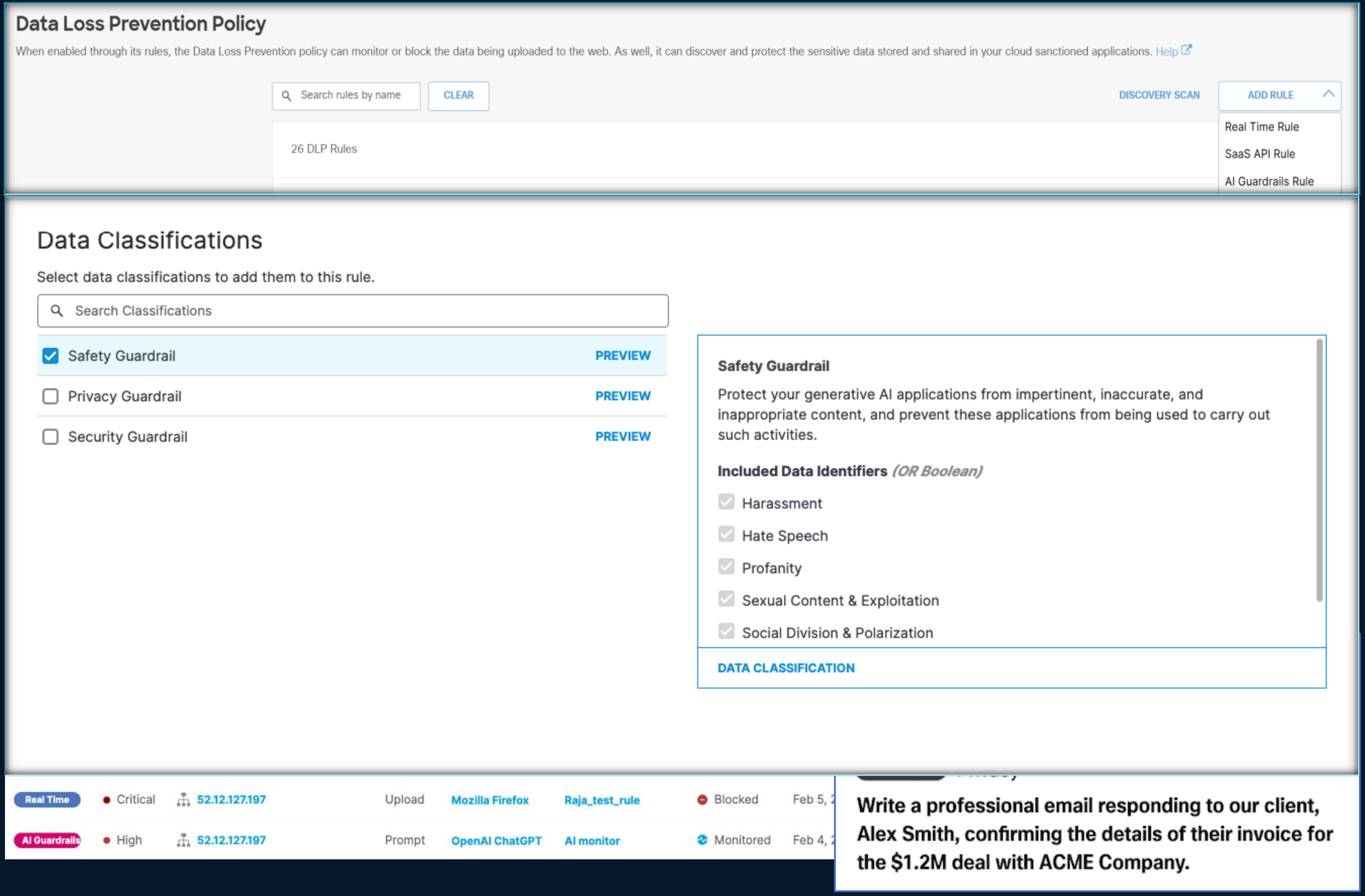
15+ Top Apps
Advanced Guardrails

1
Unified Security Framework

AI Access – AI Guardrails

Advanced Guardrails Objectives

- Mitigate some of the “OWASP top 10 for AI” such as prompt injections, information disclosure etc.
- Aligns with MITRE ATLAS compliance and governance
- AI Guardrails for Safety, Privacy and Security
- Works for Secure Access Advantage license
- Actions – Monitor or Block
- User Notification – Email
- Language Supported – English (Japanese Road mapped for coming Quarter)



Data Loss Prevention Policy

When enabled through its rules, the Data Loss Prevention policy can monitor or block the data being uploaded to the web. As well, it can discover and protect the sensitive data stored and shared in your cloud sanctioned applications. Help

26 DLP Rules

Data Classifications

Select data classifications to add them to this rule.

- ☑ Safety Guardrail — PREVIEW
- □ Privacy Guardrail — PREVIEW
- □ Security Guardrail — PREVIEW

Safety Guardrail

Protect your generative AI applications from impertinent, inaccurate, and inappropriate content, and prevent these applications from being used to carry out such activities.

Included Data Identifiers *(OR Boolean)*

- ☑ Harassment
- ☑ Hate Speech
- ☑ Profanity
- ☑ Sexual Content & Exploitation
- ☑ Social Division & Polarization

Real Time	● Critical	52.12.127.197	Upload	Mozilla Firefox	Raja_test_rule	Blocked	Feb 5, 2
AI Guardrails	● High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2

Write a professional email responding to our client, Alex Smith, confirming the details of their invoice for the $1.2M deal with ACME Company.

1200+ AI Apps	15+ Top Apps	1
Visibility & Control	Advanced Guardrails	Unified Security Framework

AI Guardrail Categories – Security for AI

- Intent Based Detection

Security

- Prompt Injection
- Response Detection

Both direction analysis is important

Privacy

- American Bankers Association (ABA) Routing Number (US)
- Bank Account Number (US)
- Credit Card Number
- Driver's License Number (US)
- Plus other common PII

Safety

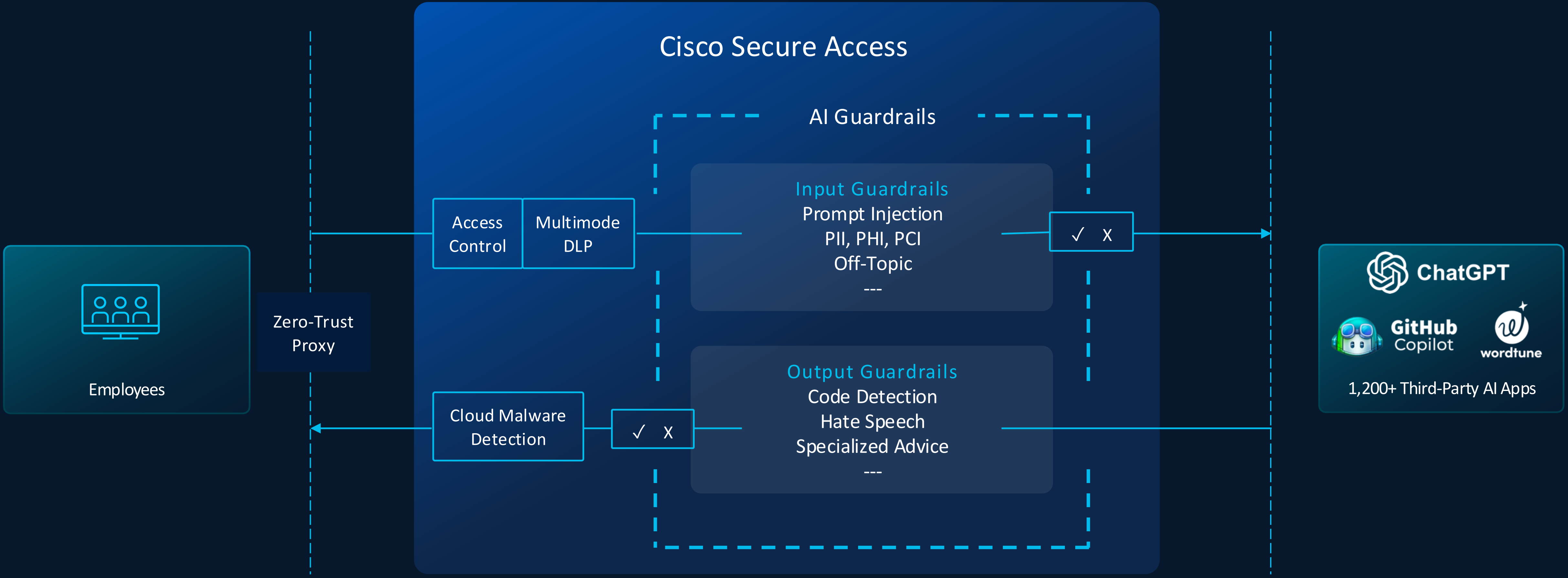
- Harassment
- Hate Speech
- Profanity
- Sexual Content & Exploitation
- Social Division & Polarization
- Violence & Public Safety Threats

Map guardrails to standards and frameworks like:

OWASP

MITRE ATLAS™

Protecting usage of third-party AI apps



Enterprise Network Traffic

Superior threat defense & manageability

99.7%

Efficacy rating for malware detection and blocking

Ranked #1 in the industry

87%

Fewer false positive detections for malicious content

vs. a leading competitor

one

Management interface for common and unified policies

vs. 4+ consoles for internet, app access, monitoring

Third party laboratory SSE competitive assessment

https://www.cisco.com/c/en/us/products/security/secure-access/miercom-sse-benchmark-report.html

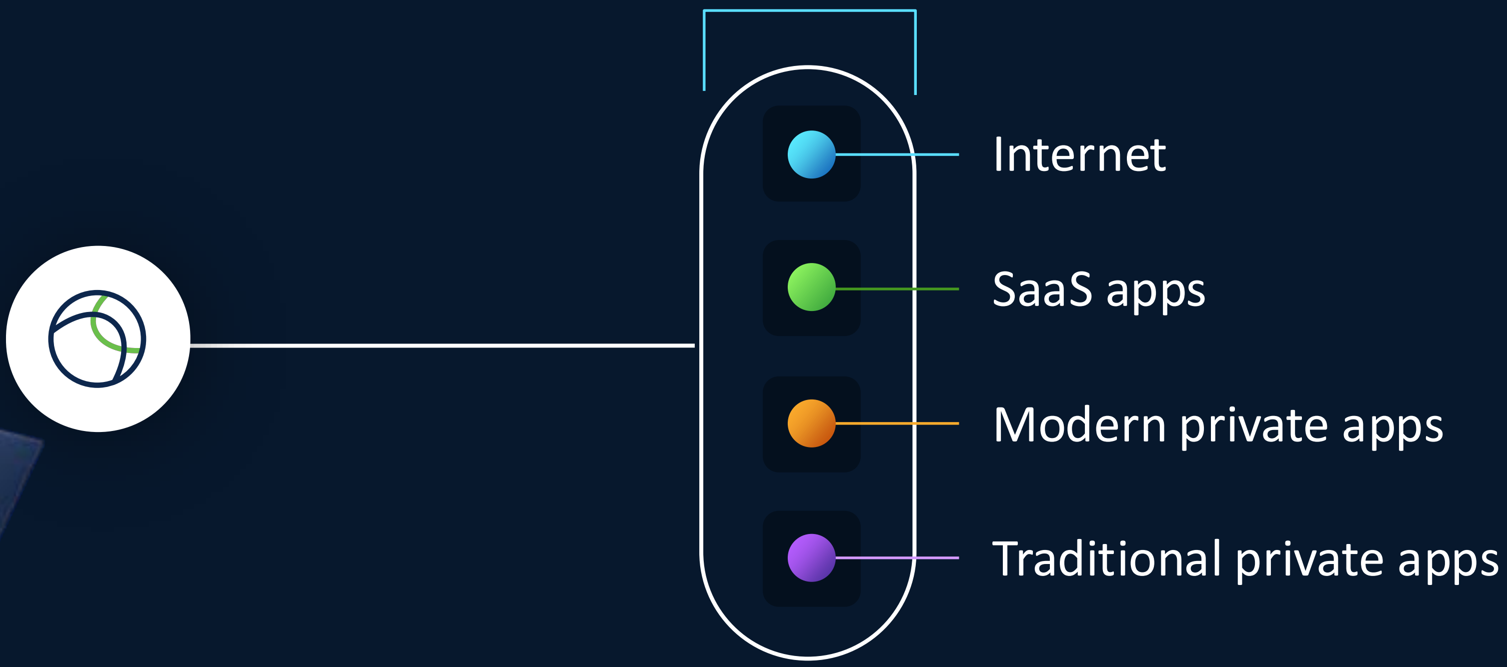
Better for users

Seamless secure access empowers a high-performance team

Single client, multiple functions

Seamless Access for Mission Continuity

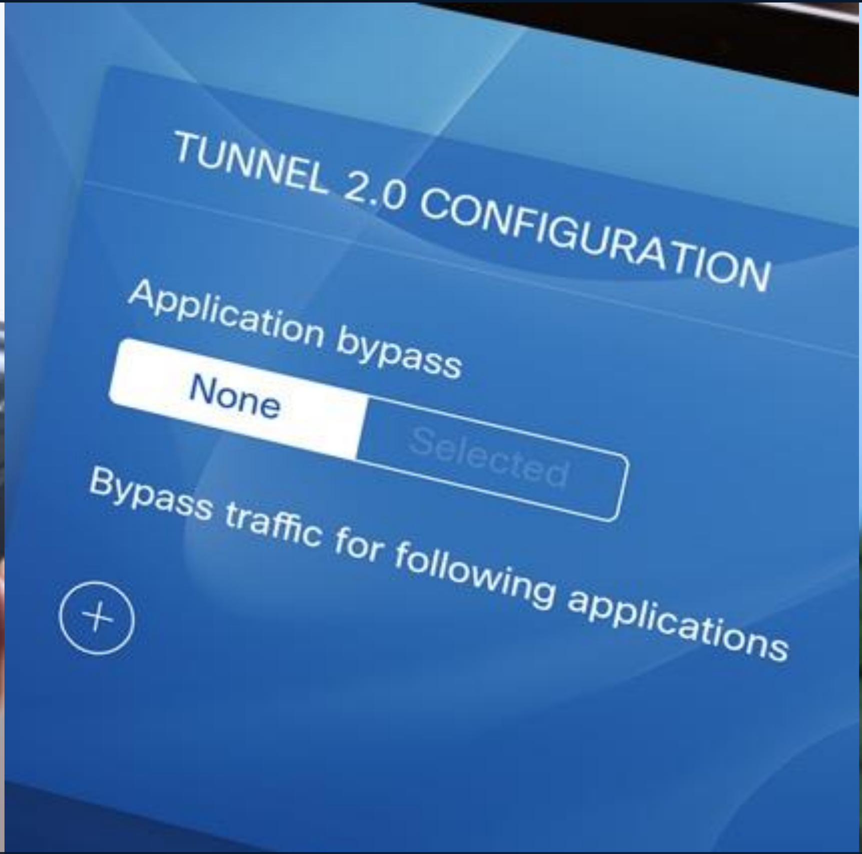
Seamless User Access



- ● Internet
- ● SaaS apps
- ● Modern private apps
- ● Traditional private apps

High speed access wherever the mission takes you

~300% faster than VPN on a plane



TUNNEL 2.0 CONFIGURATION

Application bypass

None | Selected

Bypass traffic for following applications

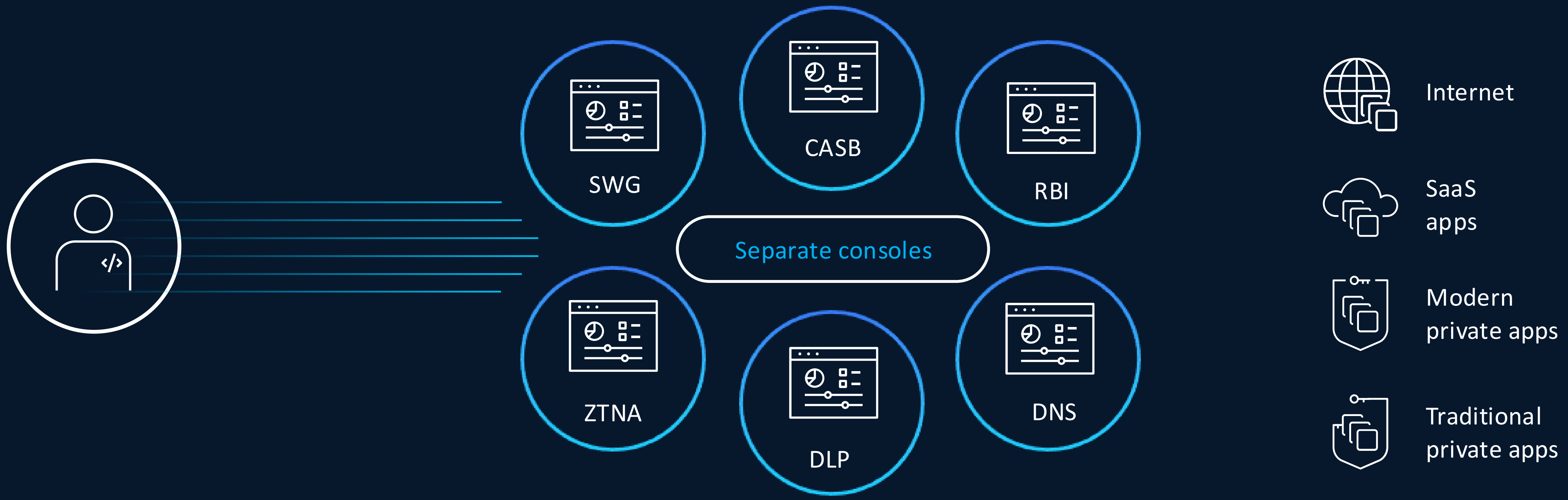
No application bypass needed

High performance for the field

Easier for IT

Efficient operations on a cost-effective single cloud platform

The multi-vendor approach is problematic



Multiple products increase cost and inefficiency

- Licenses/hardware
- Policy management
- Client management
- Reporting
- Elevated staffing levels
- Maintenance

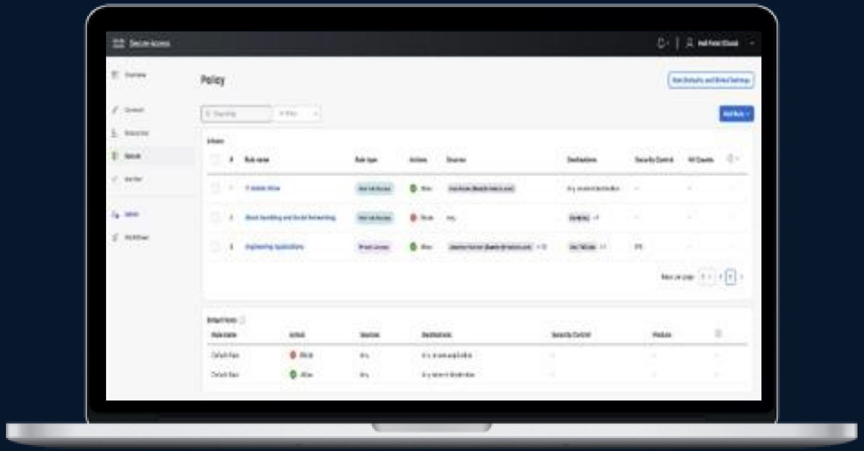
Simply see traffic, analyze risk, manage access

Single console

Unified Policy Management
Holistic Threat Visibility
Aggregated reporting

Single agent

Seamless user experience
Faster onboarding
Streamlined maintenance



Single license

Vendor/License consolidation
Deployment optimization Cost
efficiencies

Converged cloud security for lower cost and improved productivity

*Global general availability coming soon

Why Cisco Secure Access for Government?

Safer for everyone

Use an intelligence-driven, scalable defense to anticipate threats, adapt in real time, and respond with precision.

AI-powered adaptive security

Better for users

Empower high-performance teams with seamless, secure access - faster, uninterrupted connections.

High-performance zero trust

Easier for IT

Converge security in one console, one client, one cloud for simplified operations.

Cost-effective efficiencies

Děkuji