# Redrawing the battle lines with Cisco AI Assistant for Security

Data#3 | cisco Partner

**Cyber security has always been a game of cat and mouse. As attackers evolve their tactics, defenders race to close the gaps. However, this dynamic is changing. Artificial Intelligence (AI) is giving defenders today the tools to proactively anticipate and counter threats – rather than just react.**

AI integration with cyber security solutions has existed for a while. Its ability to sift through terabytes of data, identify patterns and irregularities, and process information at speeds well beyond human capability helps organisations boost security efforts by augmenting data, simulating attacks, and detecting anomalies.

Thanks to these advancements, **the next evolution in AI-fuelled cyber security has arrived with Cisco AI Assistant for Security.**

It's user-first conversational AI, harnessing Cisco's deep well of security data to offer instantaneous recommendations and actions - directly to your security team.

In this eBook, we take a deep dive into this game-changing solution. We explore the current limitations of AI-powered cyber security and the advanced capabilities of Cisco AI Assistant for Security, and discuss detailed scenarios of how your team can immediately put it to work in your security workflows.

# Contents

**To be an AI-first company, you must be a data-first company. With our extensive native telemetry, Cisco is uniquely positioned to deliver cybers ecurity solutions that allow businesses to confidently operate at machine scale, augmenting what humans can do alone. This advancement will help tip the scales in favour of defenders, empowering customers with AI built pervasively throughout the Cisco Security Cloud.**

**Jeetu Patel,** Executive Vice President and General Manager of Security and Collaboration at Cisco

# Cisco AI Assistant for Security.

Cisco AI Assistant for Security is an in-built generative AI-powered assistant here to make security simple. It's your always-on cyber security expert, parsing through complex data to provide clear and actionable intelligence at an extraordinary pace – helping you, its human counterpart, operate at machine-scale.

Like other conversational AI tools, Cisco AI Assistant for Security requires users to input their queries. The assistant then navigates the vast data terrain to retrieve and present the answers. By using natural language, cyber security management becomes more accessible, breaking down the barriers that once confined complex security tools to highly specialised professionals.

> **"With attacks getting more sophisticated and the attack surface getting larger, the only way to stop these attacks is by operating at machine scale, not human scale."**
>
> **Jeetu Patel, Executive Vice President and General Manager of Security and Collaboration at Cisco**

Cisco AI Assistant for Security is trained on one of the world's largest security-focused data sets, analysing over 550 billion security events daily. Based on the idea that coordinated cyber-attacks require coordinated defences across multiple domains, the first iteration of Cisco AI Assistant for Security uses its immense data-handling capabilities to assist with event triage, impact and scope, root cause analysis, and policy design.

This is just the beginning for Cisco AI Assistant for Security.

Cisco's ambitious roadmap will see capabilities expand from firewall management and event triage, to embedding artificial intelligence deeply into the fabric of its unified, AI-driven, cross-domain security platform. This expansion aims to enhance Cisco AI Assistant for Security with additional capabilities for automating key security tasks, like analysis and reporting – with a central focus of building a future where cyber security is more intelligent, automated, and intuitive.

## Fast facts

- **User-friendly conversational interface for easy interaction and query input**
- **Analyses over 550 billion security events daily**
- **Trained on one of the world's largest security-focused datasets**
- **Simplifies event triage, impact assessment, and policy design**
- **Part of Cisco's unified, AI-driven Security Cloud platform**
- **Geared towards IT admins, SOC analysts, and security professionals**

# Traditional obstacles to using AI in cyber security.

## How Cisco AI Assistant for Security overcomes them.

| Traditional cyber security management: | With Cisco AI Assistant for Security: |
|---|---|
| **Firewall policy management**<br>Manual and complex firewall policy management requiring technical knowledge for complex configurations. | Natural language processing and intuitive policy management allows non-specialists to easily discover, query, and modify firewall rules. |
| **Troubleshooting**<br>AI can assist in identifying issues, but often requires human oversight for diagnostics. | AI not only detects but also suggests actionable solutions, reducing manual intervention and accelerating problem solving. |
| **Policy monitoring and updating**<br>AI automates some aspects of policy management but may not proactively suggest optimisations. | Automatically identifies and suggests improvements for policy efficiency, such as removing redundant rules. |
| **Inspecting encrypted traffic**<br>Conventional AI tools struggle to balance traffic inspection with privacy concerns. | Employs an AI-powered Encrypted Visibility Engine with the 7.4.1 OS to analyse encrypted traffic for threats without needing decryption, preserving privacy and compliance. |
| **Handling data volumes**<br>Traditional AI systems analyse large datasets but may require extensive configuration and tuning. | Trained on extensive datasets, capable of analysing over 550 billion security events daily for comprehensive event analysis. Optimised for scale and accuracy without extensive setup. |
| **Incident response**<br>AI generally aids in identifying security incidents but may lag in real-time response. | Utilises AI's data processing capabilities to respond to incidents swiftly, significantly reducing reaction times. |
| **Security operations**<br>Traditional AI reduces manual tasks but can still be dependent on human configuration. | Decreases reliance on manual operations to minimise human error and enhance overall security posture. |
| **Skills gap**<br>Specialised skills required for AI cyber security are scarce and challenging to maintain. | Uses natural language processing to make cyber security management accessible to a broader range of professionals. |
| **Attacks on AI models**<br>Vulnerable to adversarial attacks due to AI models' sensitivity to data manipulation. | The Cisco Responsible AI Framework* with embedded security controls is designed to safeguard against adversarial attacks, focusing on the application of security by design principles. |
| **Trust and adoption**<br>Building trust and ensuring widespread adoption of AI can be difficult. | Cisco engages in external collaboration and industry leadership to advance responsible AI practices, enhancing trust and adoption.<br>Learn more about The Cisco Responsible AI Framework |

## Capability 1: Firewall policy management.

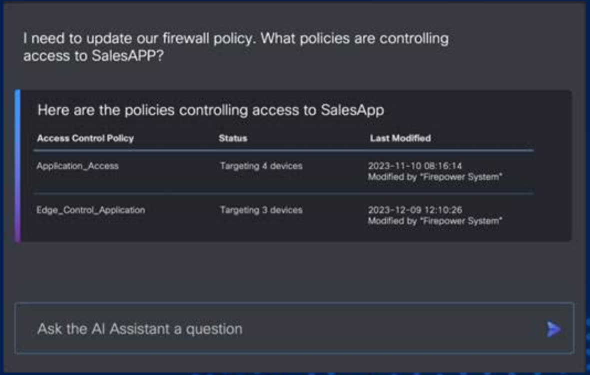
### The challenge:

A Cyber security Insiders report revealed 58% of organisations have more than 1,000 firewall rules[1] – but in highly complex environments they can reach the millions. Misconfigurations in these firewall rules are not just common. Gartner predicted them to be the cause of 99% of all firewall breaches through 2023[2].

### With Cisco AI Assistant for Security*

An AI-powered helper for firewall policy, developed inside Cisco's cloud-delivered Firewall Management Centre (cdFMC), lets users significantly reduce the complexity and time required for firewall management by:

- Entering queries to discover policies
- Requesting rule recommendations
- Eliminating duplicate rules
- Correcting misconfigured policies, and
- Automating complex workflows



I need to update our firewall policy. What policies are controlling access to SalesAPP?

Here are the policies controlling access to SalesApp

| Access Control Policy | Status | Last Modified |
|---|---|---|
| Application_Access | Targeting 4 devices | 2023-11-10 08:16:14<br>Modified by "Firepower System" |
| Edge_Control_Application | Targeting 3 devices | 2023-12-09 12:10:26<br>Modified by "Firepower System" |

### Scenario: Enhancing efficiency of firewall management.

Miranda is a Firewall Administrator facing a herculean task. Her company's network is protected by a complex matrix of firewall rules that number in the thousands, and she's has been tasked with reviewing and updating these rules to protect against the latest cyber threats.

This would usually involve combing through extensive documentation and manually checking each rule – a process that could take weeks and is notoriously susceptible to human error.

With Cisco AI Assistant for Security, Miranda's workflow is transformed:

1. Miranda starts by querying the AI Assistant about the rules that govern traffic in the company's core business applications. The AI Assistant provides her with an almost-instant summary.
2. Miranda notices an outdated rule that could potentially allow data leakage. When she asks for a recommendation to tighten the rule, the AI Assistant suggests a more secure rule that restricts traffic to only essential services.
3. After Miranda reviews and approves the new rule, the AI Assistant seamlessly implements it across the network, ensuring no traffic can bypass the updated security measures.
4. The AI Assistant also alerts Miranda to a rule causing unnecessary restarts of the firewall engine. It recommends an update to the Vulnerability Database to resolve the issue, which Miranda approves.
5. Finally, the AI Assistant analyses the entire rule set and identifies that approximately 30% of the rules are redundant or obsolete. Miranda uses the AI Assistant to optimise the rules, which further tightens security and improves network performance.

With the help of Cisco AI Assistant for Security, Miranda is able to enhance her company's firewall management process, saving time and reducing the risk of misconfigurations that could potentially lead to security breaches.

> **"We created a generative tool designed to simplify firewall management for both seasoned admins and novice users. Utilising advanced natural language processing (NLP) and machine learning (ML), it provides answers in seconds rather than forcing an administrator to spend their time sorting dependencies, network maps, and documentation."**

**Raj Chopra, SVP and Chief Product Officer of the security business group at Cisco**

## Capability 2: Troubleshooting and issue resolution.

**The challenge:**

Security professionals spend a solid one-third[3] of their time investigating and validating incidents that turn out to be non-existent threats. This distracts teams from zeroing in on genuine threats, equating to longer response times and increasing an organisation's susceptibility to cyberattacks.

**With Cisco AI Assistant for Security***

Reduce alert fatigue and help security specialists work faster and with fewer mistakes, quickly spotting, diagnosing, and resolving issues within the network's security infrastructure.

**Scenario: Detecting and responding to a ransomware attack.**

Rajiv, an IT security analyst, arrives at work to find the company's systems have been hit by a ransomware attack. In the past, addressing a crisis like this would involve manually identifying the compromised endpoints and servers - a process that could take hours, or even days.

Using the Cisco AI Assistant for Security, Rajiv takes action.

1. Rajiv queries the AI Assistant for a list of endpoints that have been communicating with known malicious IP addresses associated with the ransomware. The AI Assistant returns a list of potentially compromised systems.
2. He uses the AI Assistant to isolate the affected endpoints from the network, preventing further spread of the ransomware. With a simple command, the AI Assistant executes network segmentation rules.
3. To understand the scope of the attack, Rajiv asks the AI Assistant to analyse traffic patterns and logs for signs of data exfiltration. The AI Assistant uses its data analysis capabilities to provide insights into the attack vectors used.
4. Rajiv instructs the AI Assistant to apply the latest security updates and patches to other systems to prevent similar attacks. The AI Assistant automates the rollout of these updates across the network.
5. After the immediate threat is mitigated, Rajiv employs the AI Assistant to generate a comprehensive incident report. This report includes a timeline of events, affected systems, and response actions taken.

In this scenario, the Cisco AI Assistant for Security enables Rajiv to identify and isolate threats, apply necessary updates, and generate detailed reports for post-incident analysis via an interactive and responsive interface.

## Capability 3: Inspecting encrypted traffic.

**The challenge:**

Most network traffic is encrypted, making traditional security inspection methods challenging and resource draining. This leaves organisations trying to balance the need to protect privacy and the imperative to maintain security, often at a high operational cost.

**With Cisco AI Assistant for Security***

Leveraging Cisco's Encrypted Visibility Engine, a feature integrated within the Cisco Secure Firewall familyv7.4.1 onwards, Cisco AI Assistant for Security bypasses encryption issues by analysing encrypted traffic for signs of malware or intrusion - without the need to decrypt the traffic itself. When it identifies traffic matching known or suspected indicators of compromise, it can alert security teams or automatically block the traffic at the firewall level.

**Scenario: Enhancing Encrypted Traffic Analysis.**

Cyber security specialist, Emma is responsible for monitoring the network traffic of her company's data centre, where the bulk of traffic is encrypted. This encryption is critical for privacy and compliance but makes the task of threat detection challenging and time consuming.

With Cisco AI Assistant for Security, Emma gets to work.

1. Emma asks Cisco AI Assistant for Security to scan the network's encrypted traffic for signs of malicious activity. It quickly begins analysis without decrypting traffic, maintaining user privacy and data integrity.
2. Cisco AI Assistant for Security detects an anomaly in traffic patterns associated with the company's medical devices. It identifies communication with a known malicious server, indicative of malware activity.
3. Emma reviews the alert and, confirming the threat, instructs Cisco AI Assistant for Security to block the suspicious encrypted traffic at the firewall, cutting off the potential control channel for malware.
4. She then validates actions taken by examining traffic logs, generating a detailed report, outlining the threat detected, actions taken, and recommendations for future prevention measures.
5. Finally, Emma asks Cisco AI Assistant for Security to continuously monitor for similar patterns - ensuring real-time protection against threats hidden in encrypted traffic.

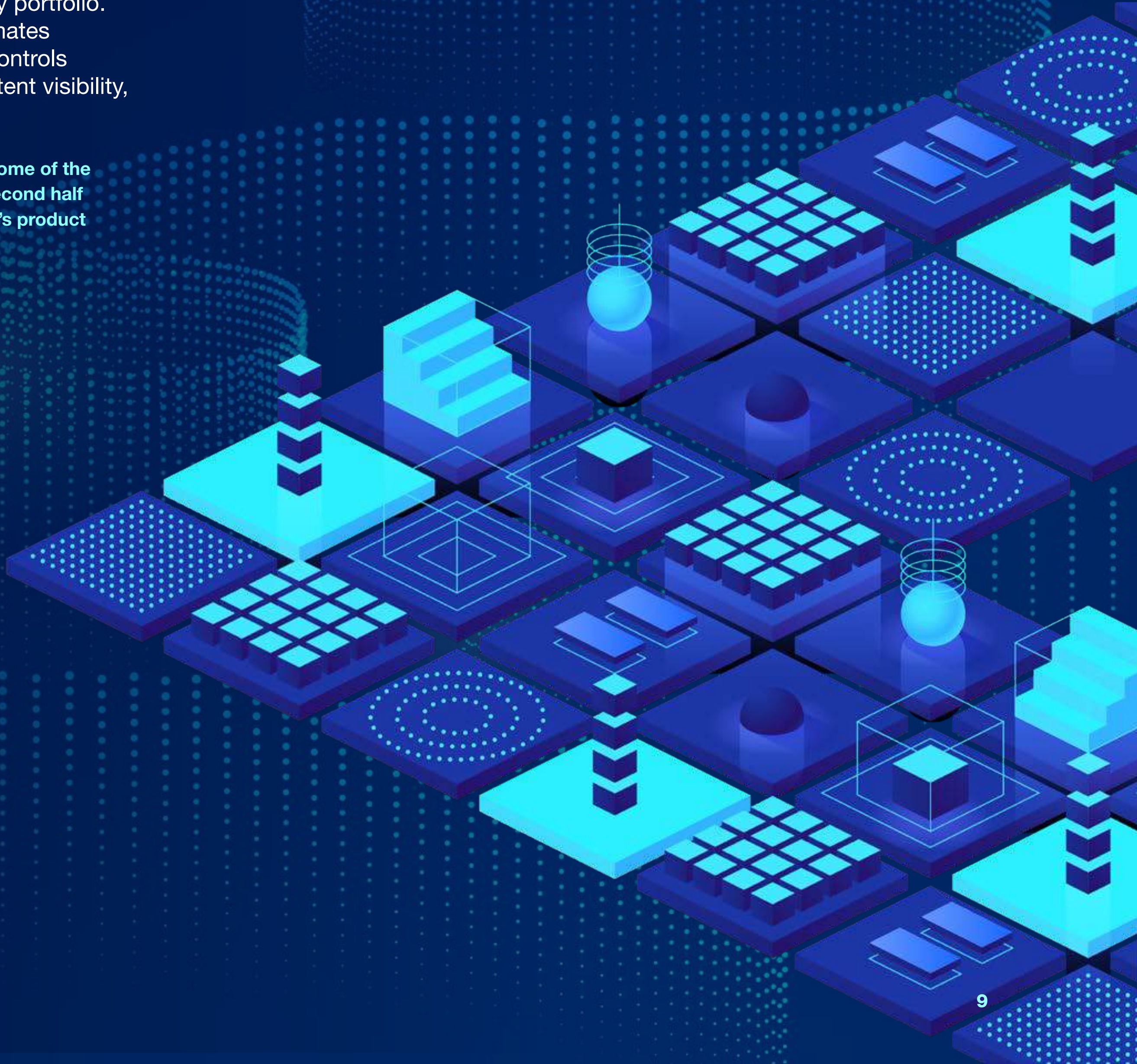
In this scenario, Cisco AI Assistant for Security gives Emma tools to proactively manage and mitigate risks associated with encrypted traffic. This ensures operational continuity, safeguarding against sophisticated cyber threats targeting encrypted channels.

# About Cisco Secure Firewall.

## Stop more threats and swiftly mitigate any that breach your defences.

Cisco next-generation firewall is a key pillar of the Cisco security portfolio. Delivering deep visibility to detect and stop threats fast, it automates network and security operations, offering world-class security controls everywhere - on-premises, virtual, and cloud - alongside consistent visibility, policy harmonisation, and unified management.

***Disclaimer: Please note that while we're excited to share these insights, some of the features discussed are part of Cisco's upcoming release planned for the second half of 2024. These details are subject to potential adjustments based on Cisco's product development and release strategy.**



# Data#3 and Cisco.

In Australia, our Cisco solutions stand unrivalled. Our dedication to excellence has been recognised many times, with Data#3 earning several prestigious titles - most notably, the APJC Customer Experience Partner of the Year (2023), Global Partner of the Year for Software (2023), and Cisco SMB Partner of the Year for Security (2023).

As a Cisco Master Security Specialised partner, our dedicated security team is here to help you overcome evolving cyber security challenges.

**To demo Cisco AI Assistant for Firewall, or learn more about the readiness of your organisation to deploy AI solutions, contact a Data#3 Cisco specialist today.**

**Learn more at data3.com/cisco/security**

data3.com

facebook.com/data3limited

twitter.com/data3limited

linkedin.com/company/data3

youtube.com/user/data3limited

Data#3 | cisco Partner

> The ability for AI to reshape our daily lives and professional landscapes is immense. As a longstanding Cisco partner, we're excited about the new Cisco AI Assistant for Security and how this will empower our customers with AI-driven efficiencies. The introduction of the AI Assistant to Cisco Firewall Management Center will help our customers quickly and easily configure policy changes. When combined with the new features in the 7.4.1 software release and the Encrypted Visibility Engine, this offers a truly compelling overall experience.

**Graham Robinson,**
**Chief Technology Officer, Data#3**