Open systems

CUSTOMER WEBINAR · 2026

QUESTIONS & ANSWERS

YOU ASKED. WE ANSWERED.

Every question from our customer webinar on AI security, Collective Defense, Lucy AI and the SASE roadmap, with answers from our product team.

16
QUESTIONS ANSWERED

6
TOPICS

01	Collective Defense	5 Q
02	Lucy AI & Mission Control	4 Q
03	Integrations & APIs	2 Q
04	Transparent Proxy & SWG	2 Q
05	ZTNA & Mobile Access	2 Q
06	Working with Open Systems	1 Q

ARGUS & APATE

01 COLLECTIVE DEFENSE

Q01

How do Argus, Mission Control, and Lucy AI work together? Specifically, what analysis or detection is performed by Argus versus Lucy, and how is that intelligence surfaced and acted upon in Mission Control?

Argus is the AI analyst behind Collective Defense. It works around the clock, autonomously and in the background, correlating security events from across our SASE services and from Apate, our decoys. Apate stays dormant until an attacker connects, then engages them and records what they do. Argus uses this evidence to decide whether an actor is malicious and, if so, blocks its IP address.

Today, Argus decides and blocks autonomously; Mission Control is not involved in these decisions. We are adding a choice for you: for each malicious actor Argus identifies, it either blocks the IP address on all sensors on its own or asks for your approval first for your sensors.

Lucy AI is the assistant you use to ask questions about your environment. It does not perform Argus's detection, and today it does not receive Argus's findings; you see them in the Collective Defense views of the customer portal. We are exploring an integration with Lucy so that you can ask Lucy why Argus acted on a given threat.

Q02

If we already work with an mSOC like Ontinue (using Azure Sentinel), can these AI security tools feed their alerts and data into it?

This is in active planning. Argus will be able to send its findings to your SOC or managed SOC provider, such as Ontinue. Argus also evaluates what attackers do on Apate decoys. For each malicious actor, you will receive the IP address, the verdict and Argus's reasoning, and potentially the full evidence behind it. All you will need to provide is an HTTPS endpoint (a webhook) that Argus is allowed to call. Each finding arrives as an indicator of compromise (IoC) that has been correlated across our customers, so your SOC can act on it in Sentinel.

We also plan to let you send your own security events to Argus for evaluation. Which sources fit depends on your setup, and we will work out the details with you. Argus's analysis runs in the EU.

Collective Defense does not require Mission Control services, so it fits alongside the SOC you already work with.

Q03

Is this included in NDR, or does it cost extra? If so, how much?

Collective Defense is a new service, separate from NDR, and complements it rather than replacing it. NDR analyzes network traffic at a single sensor. Collective Defense correlates security-relevant events from across our SASE services, at all sensors and for all customers. This means a threat detected at another customer's sensor can protect you before it reaches your network. Only attacker indicators, such as IP addresses, are shared across customers; your traffic and data are not.

You can activate Collective Defense in the customer portal and use it free of charge until 31.12.2026. After the trial, it is charged according to the price list, which your account manager can share with you.

Q04

Will the new features, like Argus, be onboarded to the Mission Control stack by default, or will they need to be acquired as an optional feature?

Argus is a separate, optional commercial feature. Lucy will be available for MC customers with all capabilities.

Q05

How do you make sure Apate (AI decoy) doesn't misclassify legitimate client requests as malicious and redirect them away from the real service, such as Active Directory? A false positive like that could cause connectivity problems for regular users.

Apate never intercepts or redirects traffic. Each decoy is a separate host on your network, and your clients reach the real services, such as Active Directory, exactly as before. Nothing in DNS or in your client configuration points to a decoy, so legitimate clients have no reason to connect to one. Apate becomes active only when someone deliberately connects to a decoy and starts interacting with it. That alone is a strong signal of suspicious, if not malicious, intent.

Some legitimate activity, such as regular network scans with tools like nmap, will touch decoys. We are building a self-service exclusion list in the customer portal for these cases: scanners you add to it will never be blocked. This applies across Collective Defense: you will also be able to list your most valuable assets up front, and Argus will never block them. Argus still analyzes everything on the list, so you keep full visibility. This gives you an additional safeguard.

ASSISTANT & ENGINEERS

02 LUCY AI & MISSION CONTROL

Q06

Will you always keep direct engineer access (MC), or will customers eventually have to go through Lucy AI first, even when they already know it's an issue she can't solve?

We will always offer direct engineer access; there is no need to go through Lucy first.

Q07

Is Lucy AI purely focused on SASE? What about services like Connectivity?

We plan to support Connectivity as well, not only SASE services.

Q08

When will Lucy be ready to actually use?

Lucy is already live and ready to use.

Q09

Will Lucy be able to dynamically load balance traffic between available ISP lines, ensuring the lines are used to their fullest, overruling bandwidth control and path control?

Not yet, but this is indeed a very interesting input. We are currently evaluating SD-WAN features for Lucy that go beyond what is possible today.

SIEM, ITSM & AI ASSISTANTS

03 INTEGRATIONS & APIS

Q10

How does Autonomous SASE integrate with our existing SIEM and ITSM/ticketing systems via its API-first design, and is there a Terraform provider for managing the network as code?

Publicly exposed APIs are documented on our public website at open-systems.com/developers. As more endpoints become available, we update the information there.

Terraform and A2A are currently in our backlog.

Q11

We use Microsoft Copilot as our primary enterprise AI assistant. Copilot can already access our Microsoft 365 data, and potentially other systems such as ServiC...

Yes, this will be possible in the future. An Open Systems MCP server, and potentially an A2A interface, are planned for 2027.

SECURE WEB GATEWAY

04 TRANSPARENT PROXY & SWG

Q12

Will the Transparent Proxy replace the SWG, or is it an additional service?

No. Transparent Proxy will not replace the SWG.

It is an additional way to use the existing SWG service. It extends SWG protection to entities that cannot use the current explicit proxy approach with a proxy PAC.

Q13

Could Transparent Proxy replace Cloud SWG?

No, Transparent Proxy does not replace Cloud SWG.

It is a design choice for how customers consume the SWG service. Initially, Transparent Proxy will only be available on on-premises SWG. Once available in the cloud, it will provide an additional way to use the existing Cloud SWG service, particularly for entities that cannot use an explicit proxy with a proxy PAC.

REMOTE ACCESS

05 ZTNA & MOBILE ACCESS

Q14

ZTNA: What are the plans for native RDP recording, mobile support, recording outage monitoring alerts, and faster ZTNA releases?

Native RDP recording

This is in our backlog, but it has not been prioritized over other features currently in development. If this capability is important to you, please position the requirement through your Account Management team to increase its visibility and support prioritization.

Mobile support

There are currently no plans to support mobile phones for ZTNA.

Recording outage monitoring & alerts

A recent incident highlighted a gap in our monitoring that we need to close. We plan to address this in the next product increment, by the end of 2026 at the latest.

Faster ZTNA releases

We expect the next ZTNA release in Q1 2027. Going forward, the plan is one major ZTNA release per year, as this provides customers with a predictable release cycle and limits the planning and operational effort required for rollouts.

Q15

Mobile access is also part of Open Systems' services. Will there be any changes to SSL VPN support, or AI integration for it?

We are prioritizing AI integration for ZTNA rather than SSL VPN. Strategically, ZTNA is our future platform for remote access, and this is where we plan to invest in APIs and integration with Lucy. SSL VPN will continue to be supported, but we do not currently plan a dedicated AI integration for it.

OPERATIONS

06 WORKING WITH OPEN SYSTEMS

Q16

It's impossible not to compare this to products we currently use (PAN). How is Open Systems better to work with?

We think we have an advantage when it comes to operational simplicity and the human touch with Mission Control.

WANT TO GO DEEPER?

Talk to your account manager about what these updates mean for your organization.