



Local Division Mannheim

UPC_CFI_414/2024

Decision

of the Court of First Instance of the Unified Patent Court

delivered on 5 December 2025

CLAIMANT

Centripetal Limited, Galway Technology Centre, Mervue Business Park -7XPF+6C -Galway –IE

Represented by Ralph Nack

DEFENDANTS

- 1) **Keysight Technologies, Inc.** Represented by Klaus Haft
1400 Fountaingrove Parkway - 95403 - Santa
Rosa - US

- 2) **Keysight Technologies Deutschland GmbH** Represented by Klaus Haft
Herrenberger Straße 130 - 71034 - Böblingen -
DE

PATENT AT ISSUE

European Patent No. EP 3 821 580

PANEL/DIVISION

Panel of the Local Division in Mannheim

DECIDING JUDGES:

This decision is delivered by the legally qualified judge Tochtermann, the legally qualified judge Sender, the legally qualified judge Knijff and the technically qualified judge Attali.

LANGUAGE OF PROCEEDINGS: English

SUBJECT-MATTER OF THE PROCEEDINGS: Infringement action

DATE OF THE ORAL HEARING: 9 October 2025

SUMMARY OF FACTS

1. Claimant sues Defendants for direct infringement of Claim 16 and indirect infringement of Claim 1 of European Patent EP 3 821 580 B1 (the patent-in-suit), relating to Methods and Systems for Efficient Network Protection, in Germany, Italy, France and the Netherlands, where the patent-in-suit is in force. The date of publication and mention of the grant of the patent-in-suit is 29 May 2024. Claimant is the registered and sole proprietor of the patent-in-suit. The opt-out pertaining to the patent-in-suit was withdrawn from the register on 12 July 2024.
2. Claim 1 of the patent-in-suit reads as follows in the language of the patent:

A method, comprising:

receiving, by a gateway (220) configured with a plurality of packet filtering rules, a plurality of packets associated with a network protected by the gateway;

filtering, by the gateway configured with the plurality of packet filtering rules, each one of the plurality of packets;

generating, by the gateway configured with the plurality of packet filtering rules, threat metadata associated with at least a first portion of the plurality of packets, wherein the threat metadata

associated with the at least first portion of the plurality of packets comprises one or more of a type of threat, a name of the threat, an identity of a threat actor, a risk score, a threat intelligence provider identity, provenance information, or other threat metadata provided from outside sources;

determining, by a broker (240) and based on the threat metadata associated with the at least first portion of the plurality of packets, at least one of a plurality of cyber analysis systems (230, 232, 234) to process the first portion of the plurality of packets;

receiving, by the at least one cyber analysis system (230, 232, 234) and from the broker, the first portion of the plurality of packets, the threat metadata associated with the first portion of the plurality of packets, and a configuration signal to configure the at least one cyber analysis system to perform a particular analysis method;

determining, by the at least one cyber analysis system configured according to the configuration signal, based on packet data, and based on the threat metadata associated with the packet data, at least one protection action for at least a second portion of the plurality of packets; and processing, based on the determined at least one protection action, the second portion of the plurality of packets, wherein the determined at least one protection action is implemented according to conditions defined by the plurality of packet filtering rules.

3. Claim 16 reads as follows:

A system comprising:
a gateway;
a broker; and
a cyber analysis system, wherein the system is configured to perform the method of any one of claims 1 - 15.

4. Claimant defines the allegedly infringing embodiment (“attacked embodiment”) in the Statement of Claim as comprising the following components and functions being connected and working together as a three-stage security system (see SoC paras. 70 et seqq.):

- **“Network Packet Broker”** (“NPB”) as “gateway”
- **“AppStack”**, a software implemented on the NPB, as “broker” component
- **“Application and Threat Intelligence Research Center”** (“ATI”) as “outside source”
- **“Data Loss Prevention”** (“DLP”), **“Intrusion Prevention System”** (“IPS”), **“SSL decrypt”** and/or **“Security Information and Event Management”** (“SIEM”) as “cyber analysis systems” (“CAS”).

5. The attacked embodiment – according to Claimant – is offered, sold and used by Defendants, Defendant 1 being a US company jointly operating with Defendant 2 as a German Company partaking in Defendant 1’s distribution, offering and sale, through their “Network Visibility” product portfolio in the relevant UPC member state countries (see Exhibits CL 13-16). For the details it is referred to the briefs.

6. In the reply to the Statement of Defence, Claimant presented three alternative infringement reads and defined the attacked embodiments as follows (cf. Reply paras. 66 et seqq., 117):

- First, the combination of the NPB (with AppStack) as gateway and broker and SecureStack, in particular its Threat Insights functionality, as CAS component.
- Second, the same system but run with the Threat Simulator software component as an additional CAS element, while not only the NPB, but also Defendants’ ThreatARMOR as well as Palo Alto Networks NGFW implement the claimed gateway functionality.
- Third, the same system with Threat Simulator endpoint integration.

It is out of dispute that Threat Insights has been discontinued since September 2022 (Rejoinder, para. 266, 296, 311) and ThreatARMOR since 31 January 2023 (Rejoinder para. 3, 74, 99, 243), respectively, i.e. commercialization stopped before the day of the grant of the patent-in-suit (29 May 2024). Upon question of the Court in the oral hearing, Defendants explicitly clarified that also no further updates pertaining to any of the features of the claims were provided or already sold systems after the patent-in-suit entered into force.

7. Further alternative infringements reads, which Claimant motioned to introduce with an application under R. 36 RoP, were not allowed by the Judge-rapporteur (Order of 1 August

2025) as confirmed by the Panel upon a request under R. 333 RoP (Order of 20 August 2025).

REQUESTS OF THE PARTIES

8. Claimant requests:

- I. to order the Defendants to refrain from making, offering, placing on the market, using, importing or storing for those purposes, in the territory of the Federal Republic of Germany, Italy, France and/or the Netherlands,

systems comprising a gateway, a broker and a cyber analysis system, wherein the system is configured to perform a method, comprising:

- receiving, by a gateway (220) configured with a plurality of packet filtering rules, a plurality of packets associated with a network protected by the gateway;
- filtering, by the gateway configured with the plurality of packet filtering rules, each one of the plurality of packets;
- generating, by the gateway configured with the plurality of packet filtering rules, threat metadata associated with at least a first portion of the plurality of packets, wherein the threat metadata associated with the at least first portion of the plurality of packets comprises one or more of a type of threat, a name of the threat, an identity of a threat actor, a risk score, a threat intelligence provider identity, provenance information, or other threat metadata provided from outside sources;
- determining, by a broker (240) and based on the threat metadata associated with the at least first portion of the plurality of packets, at least one of a plurality of cyber analysis systems (230, 232, 234) to process the first portion of the plurality of packets;
- receiving, by the at least one cyber analysis system (230, 232, 234) and from the broker, the first portion of the plurality of packets, the threat metadata associated with the first portion of the plurality of packets, and a configuration signal to configure the at least one cyber analysis system to perform a particular analysis method;
- determining, by the at least one cyber analysis system configured according to the configuration signal, based on packet data, and based on the threat metadata associated with the packet data, at least one protection action for at least a second portion of the plurality of packets; and
- processing, based on the determined at least one protection action, the second portion of the plurality of packets, wherein the determined at least one protection action is implemented according to conditions defined by the plurality of packet filtering rules;

(direct infringement of claim 16 of EP 3 821 580 B1)

- II. to order the Defendants to refrain from importing, storing, offering or placing on the market, in the territory of the Federal Republic of Germany, Italy, France and/or the Netherlands, to any person other than a party entitled to exploit the patented invention, means, namely gateways, brokers and cyber analysis systems, which are suitable for performing a method, comprising:
- receiving, by a gateway (220) configured with a plurality of packet filtering rules, a plurality of packets associated with a network protected by the gateway;
 - filtering, by the gateway configured with the plurality of packet filtering rules, each one of the plurality of packets;
 - generating, by the gateway configured with the plurality of packet filtering rules, threat metadata associated with at least a first portion of the plurality of packets, wherein the threat metadata associated with the at least first portion of the plurality of packets comprises one or more of a type of threat, a name of the threat, an identity of a threat actor, a risk score, a threat intelligence provider identity, provenance information, or other threat metadata provided from outside sources;
 - determining, by a broker (240) and based on the threat metadata associated with the at least first portion of the plurality of packets, at least one of a plurality of cyber analysis systems (230, 232, 234) to process the first portion of the plurality of packets;
 - receiving, by the at least one cyber analysis system (230, 232, 234) and from the broker, the first portion of the plurality of packets, the threat metadata associated with the first portion of the plurality of packets, and a configuration signal to configure the at least one cyber analysis system to perform a particular analysis method;
 - determining, by the at least one cyber analysis system configured according to the configuration signal, based on packet data, and based on the threat metadata associated with the packet data, at least one protection action for at least a second portion of the plurality of packets; and
 - processing, based on the determined at least one protection action, the second portion of the plurality of packets, wherein the determined at least one protection action is implemented according to conditions defined by the plurality of packet filtering rules.

(indirect infringement of claim 1 of EP 3 821 580 B1)

- III. to order the Defendants to communicate to Plaintiff, within thirty days upon service of the notification and, where applicable, translation pursuant to R. 118 (1) s. 1 RoP, the extent to which the Defendants have committed the acts described under I and II. above since 29 May 2024 and render accounts by stating in a uniform, orderly schedule, in writing and in electronic form, by producing supporting documents such as invoices, alternatively delivery notes or receipts, for the extent to which they have

committed the acts described under I. and II. above since 29 May 2024, in each case stating

1. the distribution channels of the infringing method and the distribution channels of the products obtained by the use of the infringing method, including the names and addresses of suppliers and other previous owners and the names and addresses of professional buyers;
2. the identity of any third party involved in the use of the infringing method and in the distribution of the products obtained by the use of the infringing method;
3. the quantity of products delivered, received or ordered, the prices paid for the products in question and the points of sale for which the products were intended;
4. the advertising carried out, broken down by advertising medium, its distribution, the distribution period and the distribution area; including the evidence for these advertising activities; and
5. the costs, with individual cost factors and profits realized listed separately,

whereas the relevant documentation, such as orders, order confirmations, invoices and copies of other purchase and sales documents is to be submitted, whereby confidential information outside of the scope of the requested information may be blackened out;

- IV. to order the Defendants to, within thirty days upon service of the notification and, where applicable, translation pursuant to R. 118 (1) s. 1 RoP,
 1. recall the infringing products referred to in section I. by informing third parties from whom the infringing products are to be recalled that this Court has found that the products infringe European Patent EP 3 821 580 B1, whereby the Defendants must give these third parties a binding undertaking to reimburse the costs incurred, to bear the packaging and transport costs incurred, to reimburse the customs and storage costs associated with the return of the products and to accept the products again;
 2. permanently remove the infringing products referred to in section I. from the distribution channels with reference to the fact that this court has found that the products infringe European Patent EP 3 821 580 B1, in particular by requesting third parties who are commercial customers but not end costumers to cancel all orders regarding the infringing products referred to in section I.
 3. destroy, at its expense, the infringing products in its possession referred to in section I.
 4. to provide the Court and the Plaintiff with written evidence of the measures taken within 30 days of service of the judgement.
- V. to establish that the Defendants are jointly and severally liable to compensate Plaintiff for any and all damage which the Plaintiff has suffered and will suffer in the future

as a result of the infringing acts referred to under I and II. above committed since 29 May 2024;

- VI. to order the Defendants to jointly and severally bear the Plaintiff's reasonable and proportionate legal costs and other expenses in connection with the present proceedings.
- VII. to permit the Plaintiff, at Defendants' expense, to announce and publish the decision in whole or in part in public media, in particular on the Internet.
- VIII. to order the Defendants to pay to Plaintiff an interim award of damages in the amount of EUR 100,000. This amount is to be amended if infringement continues.
- IX. to order that in case of any violation of the orders under I. and II., the respective Defendant shall pay a penalty payment in the amount of
 - up to EUR 100,000 for each day of violation of the order I.
 - up to EUR 100,000 for each day of violation of the order II.
 - up to EUR 50,000 for each day of violation of the order III.
 - up to EUR 50,000 for each day of violation of the order IV.
- X. to make these orders directly enforceable and permit, in the event that a security is ordered, the Plaintiff to provide such security also in the form of a bank or savings bank guarantee, and determine the amount of the security separately for the individual enforceable parts of the judgement.
- XI. In the event of failure to respond within the time limit, we request, pursuant to Rule 355 (1) (a), 355 (3) RoP, that the court issue the requested orders I. – X. by way of default judgement.

9. Defendants request with respect to the Infringement Action:

- to dismiss the action
- order Claimant to pay the costs

in the alternative, if the Court finds patent infringement, request the Court to

refrain from issuing a permanent injunction pursuant to Art 63 (1) UPCA and/or corrective measures pursuant to Art. 64 UPCA;

in the further alternative

in lieu of permanent injunctive relief, award Claimant reasonable monetary compensation in an amount to be determined by the Court in its sole discretion;

in the further alternative

to suspend the permanent injunction for a reasonable period of time, at least for 6 (six) months;

in the further alternative,

to make the enforcement of the decision dependent on the provision of security, which may also be in the form of a bank guarantee (Art. 82 (2) UPCA, R. 352.1, 354.1 RoP);

in the further alternative,

allow Defendants to avert enforcement of the judgment by providing security, which may also be in the form of a bank guarantee, without regard to any security provided by Claimant (R. 9.1 RoP).

10. Defendants filed a Counterclaim for Revocation (UPC_CFI_729/2024), which was heard together with the Infringement action according to Art. 33(3) UPCA (Order of 8 July 2025). However, during the oral hearing (see audio-protocol), Defendant put the Counterclaim for Revocation under the condition that the Panel finds for infringement and asked the Panel to only decide upon the counterclaim, if it finds that the attacked embodiments infringe upon the patent-in-suit. Claimant did not consent in the oral hearing, arguing that its consent was necessary. The Panel admitted the condition of Defendants (cf. audio protocol).

POINTS AT ISSUE

11. The parties are in dispute about various aspects of the Infringement Action, which are hereinafter detailed to as far as they are of relevance for the decision.
12. The parties are in dispute upon the proper construction of claims 1 and 16, respectively. In the center of the discussion is feature 1.4, i.e. the functionality of the “broker”, which is one of the functional units of the method and/or system as claimed.
13. In Claimant’s view the broker determines – based on threat metadata (features group 1.3) – a cyber analysis system to process the packets received by the gateway. The broker, to that end, is capable of deciding, which cyber analysis system shall be applied, and may be configured with rules for making such a decision. Still, the broker could also consider additional factors. Whether the broker is or is not physically separate from the gateway, is not decisive in Claimant’s opinion.
14. Defendants stress that the threat metadata, being the basis for the determination, have to be associated with the at least first portion of packets and serve as the basis for the determination of a CAS by the broker. The broker, however, was to be functionally differentiated from the gateway subject to features 1.1 to 1.3, without this meaning that it has to be a physically separate unit. However, the broker was the central managing component of the second stage of the method/system as claimed, whereas the gateway was responsible for the steps to be carried out at the first stage. Further, Defendants submit that the broker has to be capable to determine a specific CAS based on specific

threat metadata and has to send a configuration signal to a CAS (see feature 1.5). Therefore, it would be the broker, who sets up the CAS to perform a particular analysis method.

15. Defendants argue that, before the background of its construction of the patent-in-suit, namely of feature 1.4, all infringement reads were bound to fall through in the absence of a broker functionality embedded in the attacked embodiments.
16. Concerning the infringement read contained in the SoC, AppStack, according to Defendants, does not determine a CAS, let alone a specific CAS, as a broker based on threat metadata in absence of any logic for such determination, which has to be based on an analysis of metadata. AppStack was not capable of fulfilling this functionality because it worked in out-of-band mode alone, whereas an inline mode was necessary so as to fulfill the features of the patent claims 1 and 16. AppStack, indeed, applied filtering rules, but did not send packets to other parts of the system on the basis of threat metadata. Furthermore, AppStack would not send a configuration signal to a CAS, but only to a NetFlow collector (feature 1.5). In addition, SSLdecrypt was no CAS as it solely decrypted encrypted data and could not be combined with AppStack.
17. Also the further infringement reads presented in the Reply, are without merits in the eyes of Defendants. Claimant disregarded the patented claims, if – in its infringement reads – it mixed the functionalities of the gateway on the one hand side with the functionalities of the broker on the other hand side. For the realization of the claim features it was essential according to Defendants, that the units specified in the claim perform the functions as specified in the claim.
18. Defendants stated as undisputed facts and argued with regard to the new infringement reads presented in the Reply as follows:
 - AppStack/Secure Stack was only an optional software module on certain brokers allowing for decrypting and optionally re-encrypting network packets. However, SecureStack would not have any capability to analyze or inspect packets. A mere decryption of encrypted data was no inspection of packets in that sense.
 - Threat Insights neither was a part of SecureStack, as claimed by Claimant, nor did it block malicious traffic. It was implemented in AppStack source code and therefore only useable in out-of-band mode. It was only used as a way to generate interest in a separate hardware product called ThreatARMOR, the latter never generating any metadata as a gateway. Both products were discontinued before the patent-in-suit was in force. Threat Insights only visualized detected threats in different forms to the user and gave further information upon threats and therefore had a purely informational function. Furthermore, there was no functionality implemented in Threat Insights so as to deliver notifications in threats indicating a direct method of remediation. It only directed customers to the webpage of ThreatARMOR, on which general commercial information concerning

that product could be found. ThreatARMOR blocked malicious traffic based on its IP address.

- The Threat Simulator product with NPB/AppStack (and/or ThreatARMOR) as combined by Claimant's further infringement reads was a stand-alone product, which could not be used with NPB/AppStack or ThreatARMOR. The alleged combination would not work, because, under Threat Simulator, malicious traffic had to be allowed to run through the network to its designated agents ("breach and attack simulation, BAS") so as to check, if the system responds properly to the threat. If that communication was blocked based on the IP address, the testing scenario would not work, so that a combination of both products was dysfunctional.
- Neither was NPB a broker, as it could not determine a CAS based on threat metadata, because it never received threat metadata, nor was it allowable to amalgamate the functionalities of the distinct functional units of the gateway and the broker. Further, AppStack would not have any logic to determine a CAS based on threat metadata and could not be used inline.
- Also, neither AppStack nor NPB would determine Threat Simulator as a CAS. Threat Simulator only sent test packets from the so-called "Dark Cloud" to agents and those packets were addressed to the specific IP address of those agents. Therefore, the target location was already determined in advance, so that the packet was received in the agent, where a comparison was made based on a hash-value for that packet. Therefore, that agent would not have to be determined by AppStack based on threat metadata generated by a gateway – as the agent was already pre-determined on the basis of its IP address, this IP address not being threat metadata, nor generated by NPB or AppStack. These arguments were valid for both, Product Combination 2 and 3 of Claimant.

GROUNDS FOR THE DECISION

19. The Infringement Action had to be dismissed as Claimant at least did not sufficiently substantiate, in the light of the facts submitted by Defendants, that the attacked embodiments make use of feature 1.4 (also together with Claim 16) and include a broker with a functionality as provided for by the patent-in-suit. The further – substantial – non-infringement arguments of Defendants therefore do not have to be addressed.

Admissibility

20. The Local Division Mannheim has jurisdiction for the Infringement Action according to Art. 71(a),(b)(1), 4(1) Regulation (EU) 1215/2012, Art 33(1)(a),32(1)(a) UPCA.

The Patent-in-suit, esp. feature 1.4: the broker

21. The patent-in-suit relates to a method and system for efficient network protection. It describes that network threats and attacks may take a variety of forms, including unauthorized requests or data transfers, viruses, malware, large volumes of traffic designed to overwhelm resources, and the like. A variety of automated cyber analysis systems have been developed to protect networks against such network threats, which are, however, in practice often operated in a highly inefficient manner and are too slow. Moreover, automated cyber analysis systems usually were not deployed as inline systems, because that may decrease the overall network performance to unacceptable levels. Any potential threat could be reported to a human cyber analyst. Typically, however, confirmed threats/attacks represented less than 1% of the volume of enterprise communications with the internet, so that a conventional solution could be highly inefficient, slow and inaccurate. Thus, the effectiveness of network protection systems would have to be improved. To this end, the patent-in-suit protects a method and a system according to claims 1 and 16. The claims can be broken up in features for easier understanding as follows:

Claim 1

1.1	receiving, by a gateway (220) configured with a plurality of packet filtering rules, a plurality of packets associated with a network protected by the gateway;
1.2	filtering, by the gateway configured with the plurality of packet filtering rules, each one of the plurality of packets;
1.3	generating, by the gateway configured with the plurality of packet filtering rules, threat metadata associated with at least a first portion of the plurality of packets,
1.3.1	wherein the threat metadata associated with the at least first portion of the plurality of packets comprises one or more of - a type of threat, - a name of the threat, - an identity of a threat actor, - a risk score, - a threat intelligence provider identity, - provenance information, or - other threat metadata provided from outside sources;
1.4	determining, by a broker (240) and based on the threat metadata associated with the at least first portion of the plurality of packets, at least one of a plurality of cyber analysis systems (230, 232, 234) to process the first portion of the plurality of packets;
1.5	receiving, by the at least one cyber analysis system (230, 232, 234) and from the broker, the first portion of the plurality of packets, the threat metadata associated with the first portion of the plurality of packets, and a configuration signal to configure the at least one cyber analysis system to perform a particular analysis method;
1.6	determining, by the at least one cyber analysis system configured according to the configuration signal, based on packet data, and based on the threat metadata associated with the packet data, at least one protection action for at least a second portion of the plurality of packets; and

1.7	processing, based on the determined at least one protection action, the second portion of the plurality of packets, wherein the determined at least one protection action is implemented according to conditions defined by the plurality of packet filtering rules.
-----	--

Claim 16

16.1	a gateway;
16.2	a broker; and
16.3	a cyber analysis system,
16.4	wherein the system is configured to perform the method of anyone of claims 1-15

22. For the decision at hand some of the features need further explanation:

23. Claim 1 relates to a method according to which a gateway configured with a plurality of packet filtering rules receives a plurality of packets (feature 1.1), which are then filtered according to feature 1.2. The gateway generates threat metadata associated with at least a first portion of the plurality of packets (feature group 1.3/1.3.1). This functionality is attributed by the claim to the gateway.

24. According to feature 1.4 a broker, as a separate functional unit, – which however does not have to be embodied in a separate physical entity of the system – determines at least one of a plurality of cyber analysis systems to process the first portion of the plurality of packets. This determination of a CAS has to be based on the threat metadata associated with the at least first portion of the plurality of packets [0011: *“Based on the threat metadata, the first-stage TIG or another element of the NPS may select which (second-stage) cyber analysis systems may be used to process each non-zero threat-risk communication.”*].

25. The mere wording already makes the person skilled in the art understand that the broker has to be capable, by itself, of making the determination in an intelligent way in the sense that the broker must be able to read out the threat metadata, at least take it into account and dynamically select an appropriate CAS, which is equipped to deal with the specific potential threat.

26. This is reaffirmed by the description in [0014] (*“A plurality of second-stage cyber analysis systems may be differentiated by some combination of the type of analysis methods (e.g., signature-based, behavior-based, statistics based, etc.) and the types of threats and attacks that the cyber analysis systems analyze.”*) and [0018] (*“Further efficiencies may be gained by using first-stage threat metadata to select which cyber analysis system(s) (e.g. which analysis methods and types) should be applied to each (non-zero or medium threat risk) communication passed to the second stage. By significantly reduced loading and/or reduced scope of analysis methods and types, performance of the second-stage cyber*

analysis systems may be significantly increased and should, in many cases, be sufficient to enable active protections.”; also see [0043]: “The second stage may be composed of a collection of one or more automated cyber analysis systems 230, 232, ad 234, which are differentiated by the threat analysis method.”).

27. The skilled person understands before the technical-functional background that this intelligent decision by the broker, which dynamically selects the appropriate CAS based on the threat metadata, is essential to arrive at the aim of the invention: a more efficient network protection solution by avoiding that the packets are only sent further downstream to an arbitrary CAS by a broker, acting as mere, pre-configured switch without making an intelligent decision. What is necessary instead is a somewhat intelligent broker, which makes a deliberate choice between a plurality of CAS so as to dynamically select an appropriate CAS to deal with the potential threat.
28. As a further confirmation of this understanding, the skilled person reads [0045] of the description, which explains that, based on the associated threat metadata and other criteria, for example the application-level protocol (e.g., DNS, HTTP, HTTPS, SNMP, NTP, RTP, etc.), the broker 240 decides which of the one or more CAS will be applied to each communication.
29. Furthermore, the description of Figure 6 ([0053] lines 30-40) reinforces this construction (*“Based on the session protocol (such as, HTTP) and the threat metadata, the broker 240 may select, at Step 6-4, a cyber analysis system CA-SYS1 230. For example, the session communication data and the associated threat metadata may indicate that the potential threat type is credential harvesting. As such, the broker 240 may select a cyber analysis system which has been configured with signature rules for detecting web credential harvesting phishes, may perform further analysis on the session, and may send the session and metadata to cyber analysis system 230.”*). Equivalent technical information follows from the descriptions of Figure 8 at [0057], lines 40 – 44 and Figure 10 at [0063] et seq., where a CAS being a malware analysis system is selected based on threat metadata.

Insufficient substantiation of Claimant in the light of clear denial of facts by Defendants

30. As set out supra, Defendants have specifically contested that the attacked embodiments comprise a broker, which makes a determination of a CAS based on threat metadata, because the embodiments do not include such a functional unit being equipped with the necessary intelligence. In particular, AppStack – alone, or in combination with NPB – does not constitute a broker capable of implementing said CAS determination, when properly construed.

31. Next to the further non-infringement arguments

(discontinuation of ThreatARMOR/Threat Insights before the patent-in-suit entered into force

and/or dysfunctionality of Claimant's infringement read before the background of the real technical purpose of the attacked product (group) using AppStack: out-of-band functionality only – no inline functionality; no functionality for determining a CAS

and/or SecureStack-SSL: no CAS as relating to mere decryption alone and not combinable with AppStack as out-of-band system and not analyzing or inspecting packets

and/or no offering of a DLP, an IPS or a SIEM by Defendants

and/or Threat Simulator: sending Hash-value defined packet to predetermined agent not qualifying as a CAS)

Defendants – upon precise question of the Panel in the oral hearing - denied in all clarity that in the source code of the attacked embodiments, functionalities are incorporated, which would allow the embodiments to read threat metadata and then make a decision to which CAS a packet is channeled based on the specific threat metadata associated with the respective packet (audio protocol starting at 2:13:00 – 2:22:00 and specifically 2:38:20-2:39:50).

32. Before that background, it would have been upon Claimant to substantiate in more detail, why it is of the opinion, that this is not true or relevant and point to specific facts (R. 171 RoP) and, - if then again contested by Defendants - to offer adequate proof for such factual statement. In the absence of such statement, the Infringement Action has to be dismissed.

No decision on Counterclaim for revocation

33. As the condition, under which Defendants put their Counterclaim for Revocation during the oral hearing, is not fulfilled, because the Court did not find for infringement, the Counterclaim is not decided upon.
34. As discussed and decided during the oral hearing, such condition, which depends on internal procedural circumstances, is allowable under the Rules of Procedure, to which internal procedural conditions, which depend on the assessment of a particular question by the court, are not unknown (see e.g. R. 30.1.c, 118.2.a RoP).
35. It can be left open, whether this situation falls within the ambit of R. 263 RoP or R. 265 RoP. If regarded as a withdrawal according to R. 265.1 RoP, there is no legitimate interest of Claimant that the UPC confirms its patent as "UPC-approved and tested" before the background of the still pending proceedings before the EPO, as the EPO is equally equipped to decide upon the validity of the patent. Furthermore, the condition does not unreasonably hinder Claimant in the conduct of its Infringement Action in the sense of R. 263 RoP. Also the aspect of costs is not an interest in itself in this context, as the costs of the Counterclaim for revocation on Defendants part are not to be borne by Claimant. It therefore is solely Defendants decision, whether or not to put its Counterclaim under such condition, which may have consequences for bearing its related costs. Also the fact that

Claimant incurred costs to defend against the Counterclaim, until it was put under the condition, does not justify another result.

DECISION

- I. The infringement action is dismissed.
- II. Claimant has to bear the costs of the infringement proceedings.

Delivered in Mannheim on 5 December 2025

NAMES AND SIGNATURES

Tochtermann Presiding judge and judge-rapporteur	
Sender Legally qualified judge	
Knijff Legally qualified judge	
Attali Technically qualified judge	

Kranz For the CFI Registry	
---	--

Information about appeal

An appeal against the present Decision may be lodged at the Court of Appeal, by any party which has been unsuccessful, in whole or in part, in its submissions, within two months of the date of its notification (Art. 73(1) UPCA, R. 220.1(a), 224.1(a) RoP).

Information about enforcement (Art. 82 UPCA, Art. Art. 37(2) UPCS, R. 118.8, 158.2, 354, 355.4 RoP)

The decision has no enforceable content.