

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

CENTRIPETAL NETWORKS, INC.,

Plaintiff,

v.

CISCO SYSTEMS, INC.,

Defendant.

CIVIL ACTION NO.
2:18cv94

TRANSCRIPT OF VIDEOCONFERENCE BENCH TRIAL PROCEEDINGS

Norfolk, Virginia

May 18, 2020

Volume 8B
Pages 1157-1230

BEFORE: THE HONORABLE HENRY COKE MORGAN, JR.
United States District Judge

APPEARANCES:

KAUFMAN & CANOLES, P.C.

By: Stephen E. Noona

- and -

KRAMER LEVIN NAFTALIS & FRANKEL LLP

By: Paul J. Andre

Lisa Kobialka

Counsel for the Plaintiff

DUANE MORRIS LLP

By: Matthew C. Gaudet

Louis N. Jameson

Counsel for the Defendant

Carol L. Naughton, Official Court Reporter

I N D E X

PLAINTIFF'S
WITNESSESPAGE

NENAD MEDVIDOVIC

Direct Examination (Resumed) By Mr. Andre 1159

Cross-Examination By Mr. Gaudet 1189

JONATHAN ROGERS

Direct Examination By Ms. Kobialka 1194

E X H I B I T S

PLAINTIFF'S
NO.PAGE

PTX-199 1163

PTX-1237 1175

PTX-202 1179

PTX-528 1204

PTX-99 1214

PTX-547 1218

PTX-102 1225

—N. Medvidovic - Direct—

1 (The proceedings resumed at 2:12 p.m.)

2 THE COURT: All right, Mr. Andre.

3 MR. ANDRE: Thank you, Your Honor.

4 NENAD MEDVIDOVIC, called by the Plaintiff, having
5 been previously duly sworn, was examined and testified
6 further as follows:

7 DIRECT EXAMINATION (Resumed)

8 BY MR. ANDRE:

9 Q. Dr. Medvidovic, we just finished talking about the
10 importance of the Centripetal patents to cyber security. I
11 want to talk about how the importance of these patents are to
12 Cisco's new networking technology they released in June of
13 2017 and thereafter.

14 First, on the release, where Cisco unveiled the
15 network of the future -- and this is in Exhibit PTX-452 --
16 could you describe what Cisco was launching in June of 2017.

17 A. Sure. So Cisco said at that time that this is, in their
18 view, one of the most significant breakthroughs in
19 networking -- specifically, enterprise networking -- and what
20 I think is important to point out here is the highlighted bit
21 about halfway through that paragraph, where one of the things
22 that they highlight is the fact that this breakthrough allows
23 them to stop security threats in their tracks. So that's one
24 of the things that they specifically call out to.

25 Q. What does it mean, "stop security threats in their

—N. Medvidovic - Direct—

1 tracks"?

2 A. Essentially, basically, snuff them out. I think
3 Mr. Jameson this morning used the word "graveyard" a couple
4 times. So, you know, kind of send them to the graveyard, in
5 a sense; do not allow them to propagate, do not allow them to
6 do the damage that they would otherwise do, and things of
7 that nature.

8 Q. Now, I want to focus on three or four of the technologies
9 that were released in June of 2017 and thereafter, and the
10 first one is the Catalyst 9000 switching portfolio.

11 Now, this was in the same PTX-452. Could you
12 describe how Cisco described this new networking component?

13 A. Sure. So the first thing to note here is that they're
14 actually saying at that time this is a new family of switches
15 and that this has been built from the ground up. So this
16 doesn't sort of harken back to an older technology that
17 they've been able to evolve into this new generation of
18 switches, this is all new.

19 And what they're saying here on that toward the end
20 of that statement is that they're innovating, by using these
21 application-specific integrated circuits and that operating
22 system, IOS, that's been talked about quite a bit last week,
23 and what this allows them to do is, essentially, accomplish
24 certain things like performance, for example, but also the
25 thing that's highlighted in the middle there is unmatched

—N. Medvidovic - Direct—

1 security.

2 So they're actually saying that whatever security
3 capability they have in their switches -- which, again, are
4 built completely from the ground up -- that security, in
5 their view, does not have a peer in the marketplace.

6 Q. Also I want to talk about Encrypted Traffic Analytics.
7 Could you describe what -- how Cisco describes Encrypted
8 Traffic Analytics in PTX-452?

9 A. Yes. So this, again, is a statement made in this
10 document by, in this case, a Cisco vice president who
11 basically says that, hey, everybody thought this problem was
12 supposed to be unsolvable. They tried to figure out what
13 kinds of things are happening in your network traffic that
14 may be encrypted without being able -- or -- right, without
15 being able to or being forced to decrypt it or unencrypt it,
16 and to peek inside of it.

17 And what he's saying explicitly is that they
18 actually have this cyber intelligence. They can detect,
19 attack signatures, even in encrypted traffic, while at the
20 same time maintaining your privacy, meaning that Cisco itself
21 is never going to look inside of your encrypted data blocks,
22 for example, they will determine this based on the
23 unencrypted parts of the traffic, and that was discussed
24 quite a bit in Dr. Cole's testimony.

25 Q. I also want to talk about the DNA, the Digital Network

—N. Medvidovic - Direct—

1 Architecture, and part of that architecture is the DNA
2 center. Could you describe how they discuss the DNA center.

3 A. Sure. So the DNA, or the Digital Network Architecture,
4 center is this module, this system -- or subsystem in this
5 case -- that provides various different things, including the
6 provisioning and the policy and then, based on those, the
7 levels of assurance you may want from your network.

8 So, again, these are the kinds of things that
9 permeate the various press releases, white papers, and so on
10 that I have seen from Cisco, where the kinds of things that
11 they focus on end up being some of the words that we have
12 heard about in the past week and a half, at this point, and
13 some of those terms that play a very important role in the
14 kinds of technologies that we're discussing here.

15 Q. Let me show you what's been marked as PTX-199.

16 Dr. Medvidovic, what is PTX-199?

17 A. So this is a Cisco document. This is, I believe, on one
18 of their web pages. It is something that they represent to
19 the outside world as a sort of summary of the kinds of
20 capabilities that they provide in this new generation of
21 switches, this Catalyst 9000 generation of switches.

22 Q. If we can blow up the top portion of that, there's --
23 just the date.

24 It's dated January 3, 2020. Do you see that?

25 A. I do.

—N. Medvidovic - Direct—

1 MR. ANDRE: Your Honor, I'd like to move PTX-199
2 into evidence.

3 MR. GAUDET: No objection.

4 THE COURT: What was that date?

5 MR. ANDRE: The date was January 3, 2020.

6 MR. GAUDET: All right. That will be admitted.

7 (Plaintiff's Exhibit PTX-199 was received in
8 evidence.)

9 MR. ANDRE: Thank you.

10 BY MR. ANDRE:

11 Q. Now, Dr. Medvidovic, I want to go through -- I want to go
12 through this whole document, but I want to go through certain
13 sections and highlight certain sections, and could you tell
14 the Court how those sections are relevant to the Centripetal
15 patents and why the Centripetal patents are important to this
16 technology?

17 MR. GAUDET: Your Honor, we're going to object.
18 This expert's report never said anything about the Cisco
19 products in relation to the Centripetal patents. There is --
20 it has a description of the Centripetal patents generically,
21 it then has a generic description of the Cisco products, but
22 his report never opines on any connection or relevance of the
23 patents to the products.

24 THE COURT: Well, nobody has introduced this report
25 into evidence. I don't know what's in there.

—N. Medvidovic - Direct—

1 MR. GAUDET: Your Honor, for us it's just a basic
2 disclosure issue, which is to say the scope of his testimony
3 needs to be limited to what is in the report. I would simply
4 suggest that Mr. Andre --

5 THE COURT: I haven't seen the report. I can't rule
6 on that.

7 MR. GAUDET: Your Honor, we can get you a copy of
8 the report if Mr. Andre wants to give us a citation to where
9 this type of testimony was disclosed.

10 MR. ANDRE: Your Honor, in order to try to shortcut
11 this objection, we will just have Dr. Medvidovic talk about
12 the importance of the technology that's put forward. I think
13 it doesn't take a whole lot of effort to link this to the
14 actual patents themselves, but we'll just make it go a little
15 faster here, and we'll just talk with each of these
16 highlighted bullet points.

17 THE COURT: All right.

18 BY MR. ANDRE:

19 Q. So the second bullet point under the benefits for the
20 Catalyst switches, it says the benefits -- "it offers
21 end-to-end integrated security solutions, attacks and stops
22 threats, even with encrypted traffic."

23 Do you see that?

24 A. I do.

25 Q. Could you describe the importance of this technology to

—N. Medvidovic - Direct—

1 the Catalyst switch.

2 A. Sure. So without this ability, the Catalyst switch would
3 not be able to make those claims that it was able to make,
4 such as "unprecedented security" and some of the other terms
5 that we heard.

6 And, also, of course, the ability, as claimed by
7 their vice president, to be able to look at the traffic that
8 goes through without violating the user's privacy; in other
9 words, without having to actually unencrypt it and peek
10 inside of it. That is also a critical aspect of what they're
11 claiming is going to be the kind of winning proposition in
12 their new generation of switches.

13 Q. So is it important for the Catalyst switch to be able to
14 detect and stop threats?

15 A. Absolutely. We spoke about this before lunch, and the
16 Judge asked a couple of questions and also made some
17 observations.

18 If you don't do that, then you're exposing
19 everything that's past the switch, and it could be a whole
20 slew of different devices that are highly sensitive.

21 Q. And it says you detect and stop these threats even with
22 encrypted traffic. Is that important to the Catalyst switch
23 and the routers that have the same operating system?

24 A. It is -- yes. So I think the thing that maybe we should
25 touch upon here is the fact that the same operating system

—N. Medvidovic - Direct—

1 does run on the routers, and they do handle encrypted traffic
2 in the same manner.

3 Being able to do that, given that we've seen several
4 numbers shown over the last week, week and a half, on the
5 order of 70 percent, give or take, of all network traffic is
6 estimated by Cisco today to be encrypted. Being able to
7 actually do this with encrypted traffic is obviously
8 absolutely critical, because, otherwise, the majority of the
9 network traffic would be completely either missed or they
10 would actually be able to -- or, sorry -- they would be
11 forced to, on the fly, figure out how to unencrypt this,
12 which would be incredibly expensive, making their switches
13 and routers so slow as to be not particularly useful in the
14 real world. So they absolutely have to do this.

15 Q. And the second, the part of the highlight, the third
16 bullet point under "Benefits" in PTX-199, talks about
17 policies are created and applied throughout the network.

18 What is the benefit of being able to create policies
19 and be able to apply them throughout the network?

20 A. Again, the point here is that what you're trying to do is
21 you're trying to secure not one computer, not one machine,
22 you're trying to secure a subnetwork, so maybe a local area
23 network, something that exists in a building like the
24 courthouse or a company network, like an enterprise network.
25 And what you want to do is you want to be able to set these

—N. Medvidovic - Direct—

1 policies, which are essentially these sets of rules, that
2 specify what should happen if certain things are discovered
3 in the network traffic. And you want to be able to apply
4 those policies to everything in that particular network,
5 making it very efficient; otherwise, you'd really have to
6 spend a lot of time and a lot of resources, and, in fact, it
7 would be very error-prone if you were to do this one by one
8 on every single machine. So what you want to do is do it in
9 one place and then apply it centrally network-wide.

10 Q. Under the section entitled "End-to-End Security" on
11 PTX-199, the first sentence talks about using threat
12 intelligence.

13 Could you describe how important using threat
14 intelligence is to the Catalyst switches and the routers that
15 share the same operating system?

16 A. Absolutely. Threat intelligence is critical. I think
17 this has also been discussed in previous testimony.

18 Without engaging these intelligent solutions, a lot
19 of the more sophisticated kinds of things that might happen
20 in a network, where -- one of the terms that's been used
21 multiple times, including this morning, is obfuscation, for
22 example, occurs. Obfuscated traffic, for example, might not
23 be spotted in time without using this kind of threat
24 intelligence.

25 So what threat intelligence does is it essentially

—N. Medvidovic - Direct—

1 allows a network to make adjustments to things that on the
2 surface may look innocuous but, in fact, could be very
3 dangerous.

4 Q. Going down to the "Automation and Assurances" section of
5 PTX-199, the last sentence talks about, "using real time and
6 historical data analytics to learn, adapt, and even detect
7 problems before they happen."

8 Could you describe the importance of that technology
9 to the Catalyst switches and the routers which have the same
10 operating system.

11 A. Right. Both switches and routers will use the same
12 capabilities in this regard, and what this is actually
13 talking about is an ability of the switches and routers to
14 observe what's happening in the network and to apply
15 techniques that we've heard about before, things like
16 artificial intelligence and machine learning, to adjust, to
17 figure out what's happening in the network, to detect those
18 problems before they happen, and to take appropriate action,
19 whatever that action may be in a given context.

20 Q. And the last section of PTX-199 under the "Mobility
21 Challenge," "The policies are applied consistently for
22 security," and et cetera.

23 Do you see that?

24 A. I do.

25 Q. Could you describe how it's important to the Catalyst

—N. Medvidovic - Direct—

1 switches and the routers that the share operating system to
2 have the policies apply consistently for security?

3 A. Sure. This dovetails with the issue that we discussed in
4 the third bullet from the top, because, again, it deals with
5 the policies, but, in this case, what it's recognizing is the
6 fact that individuals may move and their devices may move
7 within a network.

8 And what this ensures is that those policies that
9 ensure the security of the entire subnet, for example, those
10 will not be dependent on where you are geographically. So it
11 does introduce this security in the face of the flexibility
12 that all of us are expecting nowadays of the devices that we
13 use and how we conduct our work.

14 Q. Let me go to PTX-995 next.

15 MR. ANDRE: And, Your Honor, I believe PTX-995 is
16 already in evidence.

17 THE COURT: 995. That was 199, the last one, wasn't
18 it?

19 MR. ANDRE: The last one was 199.

20 THE COURT: And this is 995.

21 MR. ANDRE: 995, and it's in evidence already.

22 THE COURT: Right, okay.

23 BY MR. ANDRE:

24 Q. Dr. Medvidovic, what is PTX-995?

25 A. So this is the Cisco Security Analytics white paper, and,

—N. Medvidovic - Direct—

1 as they say, it's a deep dive into this machine learning and
2 behavioral modeling step that we've spoken about before, the
3 point here being that what they're trying to describe is
4 their advanced threat detection capability.

5 Q. If we turn to Page 8 of this document, the top two
6 paragraphs talk about Encrypted Traffic Analytics.

7 THE COURT: This is AA?

8 MR. ANDRE: This is AA, yes, Your Honor.

9 THE COURT: Okay.

10 BY MR. ANDRE:

11 Q. Now, Dr. Medvidovic, there is a sentence here -- we're
12 talking about Encrypted Traffic Analytics. It says, "The
13 initial data packet is a treasure trove of metadata, because,
14 remember, all encrypted traffic sessions start out
15 unencrypted initially."

16 Do you see that?

17 A. Yes.

18 Q. And what's that referring to?

19 A. So this is tying back to that statement by the Cisco VP,
20 who was talking about the fact that their switches and
21 routers can -- well, he was talking about switches
22 specifically, but the application-specific integrated circuit
23 architecture, ASIC, mentioned here and the IOS operating
24 system, as we have heard before, they're identical between
25 the switches and the routers. So I'm not trying to represent

—N. Medvidovic - Direct—

1 here anything that is not factually true.

2 So, going back to my point, both the switches and
3 the routers are capable of using this bit of information,
4 that in every data packet is going to remain unencrypted, to
5 try to learn about what is actually happening within the
6 encrypted network traffic. So the -- in their view, in
7 Cisco's view, the beauty of this is the ability to make all
8 kinds of intelligent decisions and act accordingly, while --
9 and do so really fast, while at the same time preserving the
10 privacy and data confidentiality of whoever decided to
11 actually encrypt their data.

12 So if I'm communicating with my bank, for example,
13 Cisco does not need to know, for example, what my bank
14 account number is or how much money I may have in that bank
15 account. All they know is this header information that says
16 where the packet is coming from and where it's going to and
17 some other metadata of that kind. And based on that
18 information alone, they will be able to make these
19 determinations that they need to make.

20 Q. So the information where it says, "Cisco's unique
21 application-specific integrated circuit (ASIC) architecture
22 provides the ability to extract these data elements without
23 slowing down the data network," is that referring to the
24 actual switches and routers, the integrate -- the
25 application-specific integrated circuit?

—N. Medvidovic - Direct—

1 A. That is correct. This is the actual physical piece on
2 the -- or in, rather, one of those boxes that we have seen
3 pictures of, and that's what their ASIC, or
4 application-specific integrated circuit, is geared for.

5 So this is not the kind of integrated circuit that,
6 for example, is running in my computer that I'm using right
7 now. This is an application-specific type of solution that
8 is geared particularly to this specific problem that Cisco is
9 trying to solve.

10 Q. And that's located on the router and switches?

11 A. It's -- well, it's not located on them. As I said
12 initially, I said not on them but really physically it's
13 located inside of them.

14 Q. Okay. It's in the box?

15 A. It's inside the pizza box, yes.

16 Q. All right. And that element takes this initial data
17 packet and does this processing of that information, correct?

18 A. That is correct. It does all of this by using what
19 they're calling here the "treasure trove of metadata." So
20 this initial data packet, and that's the information that
21 they're using, and then they're doing all kinds of
22 manipulations, and intelligent decision making, and so on,
23 based on that.

24 Q. And then eventually some eventual -- the next paragraph
25 talks about the telemetry is then passed to the Stealthwatch.

—N. Medvidovic - Direct—

1 Do you see that?

2 A. I do.

3 Q. And can you describe what is important of this?

4 And you can read the whole sentence there, if you
5 like, and describe what's being discussed here.

6 A. Sure. So the idea is really twofold -- well, threefold,
7 really.

8 The first one is you don't want to look inside of
9 the encrypted traffic, because you don't want to compromise a
10 user's data privacy and confidentiality. So that's a
11 requirement that most users will expect. Cisco should not be
12 able to see my private data.

13 Based on that initial requirement, what Cisco does,
14 using this approach, is ensures two other things. The first
15 one is that they can do this at high speed so they can
16 process lots and lots of network traffic doing this analysis
17 of this metadata, or the treasure trove of metadata, as they
18 call it.

19 And then the other thing that's really important is
20 that Stealthwatch can actually do this with high fidelity,
21 meaning that it's very accurate about how it actually detects
22 the malware.

23 Two things that you would like to avoid in malware
24 detection: The first one is what is known as false
25 positives, which is where you keep flagging things as

—N. Medvidovic - Direct—

1 potential malware that is actually completely regular
2 traffic, it doesn't have any malware. And that's bad because
3 it's annoying, and it slows down the system, and so on, and
4 that becomes sort of the boy who cried wolf kind of thing.

5 The other one that's actually even more dangerous in
6 some ways is false negatives, which is something that
7 actually is malware, but Stealthwatch lets it through, for
8 example. And what this statement says is that Stealthwatch
9 is actually able to deal with both of those cases and detect
10 malware with this high fidelity.

11 Q. When it comes to the Encrypted Traffic Analytics, are the
12 packets being processed both at the routers and switches and
13 at Stealthwatch?

14 A. Yes. This is what this particular document itself
15 states, and I think we've heard other evidence introduced
16 earlier today and last week that talks about that.

17 Q. Like --

18 THE COURT: Is Stealthwatch -- could Stealthwatch be
19 classified as a firewall?

20 THE WITNESS: Your Honor, Stealthwatch itself is
21 not -- in the terminology used by Cisco, it's not considered
22 a firewall. The interesting thing here is that -- and I
23 think that's what your question is getting at; is that by
24 introducing this new generation of switches and routers and
25 injecting these security capabilities inside of them, what

—N. Medvidovic - Direct—

1 Cisco has done is it has moved some capabilities that
2 traditionally used to belong in firewalls -- it's moved some
3 of those into switches and routers.

4 So -- which is why I think, for example, your
5 question is an appropriate one, but terminologically, Cisco
6 also has a firewall which does use other technologies. So
7 this has some traditional firewall-like capabilities but is
8 truly not a firewall, per se. Cisco has another -- and we've
9 heard this before -- another set of products that actually
10 act as firewalls, and that's what they call them.

11 THE COURT: All right.

12 BY MR. ANDRE:

13 Q. Let's turn to the DNA center. I'd like to show you
14 what's been marked as PTX-1237, 1-2-3-7.

15 Dr. Medvidovic, could you describe what this
16 document is?

17 A. Yes. This is a Cisco data sheet, and this document is
18 from October -- well, the date when the document was printed
19 is October. I apologize. The actual document's update date
20 is September 16, 2019.

21 MR. ANDRE: And, Your Honor, I'd like to move
22 PTX-1237 into evidence.

23 THE COURT: All right. That will be admitted.

24 (Plaintiff's Exhibit PTX-1237 was received in
25 evidence.)

—N. Medvidovic - Direct—

1 BY MR. ANDRE:

2 Q. Dr. Medvidovic, I want to turn your attention to the very
3 first sentence there, where it says, "The Cisco DNA center is
4 a foundational controller and analytics platform at the heart
5 of Cisco's intent-based network for large and midsize
6 organizations."

7 What does it mean to be a "foundational controller
8 and analytics platform"?

9 A. In a sense, it's, if you will, the brain trust of what is
10 happening there. It forms the most important piece that
11 other things are built around, in a sense.

12 Q. Okay. If we go down to the second bullet point there
13 when it talks about policy, it says, "Define user and device
14 from a profile of highly secure access and network
15 segmentation based on needs."

16 Does the DNA center have a role in putting policies
17 onto the routers and switches?

18 A. Yes. So we talked about this before. This was in
19 Cisco's press release, where they talked about those
20 centrally determined policies that are then distributed
21 across the network. This is exactly what this particular
22 piece is talking about.

23 So the Digital Network Architecture center, or the
24 DNA center, is the piece that defines these profiles and
25 these policies and then pushes them to the appropriate places

—N. Medvidovic - Direct—

1 in the network, which are the routers and the switches.

2 Q. If we go down to the bullet point "Provision," do you see
3 that?

4 A. I do.

5 Q. And could you describe what's being discussed there?

6 A. Sure. So this is, again, the idea that once you
7 determine what these policies should be and once you define
8 them, you should be able to provision them, meaning that you
9 should be able to make them available to the places where
10 they're actually going to be applied.

11 So in the case of Cisco's architecture or the
12 architecture of an organization that purchases Cisco's
13 products, those policies themselves are going to be applied
14 at the level of routers and switches. So the DNA center, or
15 the Digital Network Architecture center, provisions its
16 policies that it defines to the routers and switches.

17 Q. At the end of that same paragraph it talks about,
18 "Additionally, the Stealthwatch security analytics service
19 provision network elements send NetFlow and Encrypted Traffic
20 Analytics to Stealthwatch."

21 Do you see that?

22 A. Yes.

23 Q. There's been some discussion here about the Digital
24 Network Architecture center. Does that include the
25 Stealthwatch security analytics component?

—N. Medvidovic - Direct—

1 A. This would indicate that it does. This is an indication
2 that Stealthwatch security analytics is connected to this
3 provisioning capability of the Digital Network Architecture
4 center.

5 Q. If you go down to the next bullet point, it actually
6 talks about, "The integration with Cisco's Stealthwatch
7 security provides detection and mitigation." Do you see
8 that, the last sentence under the "Assurance"?

9 A. I do.

10 Q. Could you describe what that's referring to.

11 A. So, basically, what this talks about is that Cisco's
12 Digital Network Architecture, and specifically this Digital
13 Network Architecture center, is capable of dealing with these
14 policies and provisioning the policies, et cetera, but then
15 it's also integrated with Stealthwatch itself.

16 And what it does is, in addition to its own, let's
17 say, core capabilities that we talked about in the first
18 couple of bullets, what it can also do is help deal with the
19 threats that are hidden, potentially, inside of encrypted
20 traffic. So there's kind of this natural integration of the
21 two pieces that allows you to deal with things both with
22 unencrypted and also encrypted traffic.

23 Q. Turn to PTX-202.

24 Could you describe what this document is,
25 Dr. Medvidovic?

—N. Medvidovic - Direct—

1 A. This is a Cisco Cognitive Threat Analytics white paper
2 that exists on their website, and this particular document
3 looks like it has been printed in January of this year. I'm
4 not sure I see the date as we sit here.

5 Q. This is on their website as of January 3, 2020, though?

6 A. That is absolutely correct.

7 MR. ANDRE: Your Honor, I'd like to move
8 Exhibit PTX-202 into evidence.

9 THE COURT: That will be admitted.

10 (Plaintiff's Exhibit PTX-202 was received in
11 evidence.)

12 BY MR. ANDRE:

13 Q. If you look at the very first sentence under the heading
14 that says, "Security That Evolves," could you describe what
15 this document is referring to?

16 A. Sure. So what this is talking about is that if you
17 assume that the world around you is fixed when you're trying
18 to provide a solution that deals with different threats,
19 malware, if you assume that that world is going to stay
20 fixed, then eventually your solution is going to get eclipsed
21 by the bad guys, basically.

22 And what this is talking about is that even today
23 what are considered even the most advanced methods will
24 become outdated at some point in the not-too-distant future.
25 So, as the title of this document suggests, what you need is

—N. Medvidovic - Direct—

1 security that itself evolves and tries to stay a step ahead
2 of the bad guys.

3 Q. Go to the next paragraph.

4 How does Cisco answer that challenge they just
5 discussed in that first paragraph?

6 A. So what this talks about is directly what it says; that
7 it answers that challenge using Cognitive Threat Analytics,
8 or what in some of the diagrams that we've seen has been CTA.

9 And what Cognitive Threat Analytics allows us to do
10 is discover threats in a network, do so very fast, and look
11 at various kinds of data breaches, through behavioral
12 analysis and detection of certain kinds of anomalies that
13 might escape sort of a vanilla, run-of-the-mill security
14 solution but that their Cognitive Threat Analytics is able to
15 catch.

16 THE COURT: Is this machine-driven advances that's
17 made that we might call artificial intelligence?

18 THE WITNESS: That is correct, Your Honor. There is
19 a tremendous use of artificial intelligence here, because
20 what it allows a computer to do is recognize various patterns
21 that a human would have a very difficult time with, given the
22 humongous amounts, massive amounts, of information inside the
23 data packets that end up getting passed through a network
24 device.

25 So what this does is it does all kinds of things

—N. Medvidovic - Direct—

1 where it will do various kinds of telemetry, and build logs,
2 and correlate things, and so on, stuff that computers are
3 really, really good at that humans would simply not have a
4 chance of accomplishing in a practical amount of time.

5 THE COURT: What it does is it creates new rules
6 which go to the switches and routers. Is that right?

7 THE WITNESS: That's precisely right. It deals with
8 things that it hasn't seen before and sort of on the fly
9 determines that this is a new thing, it's a bad thing.

10 And, if you remember from before, they do this with
11 high fidelity. So they believe or they claim that they can
12 do this in a way that will actually really protect you,
13 regardless of the fact that these new things had not been
14 seen before, and, essentially, the rules that you have today
15 are going to quite possibly be different from the rules that
16 you had yesterday.

17 THE COURT: Well, the thing that's confusing is the
18 terminology. I mean, you have policies, and you have rules.
19 I guess a policy is a set of rules. Is that the way it's
20 used?

21 THE WITNESS: That is precisely right. So you have
22 a set of rules. You combine them and create a policy. So a
23 policy could be anything like nobody in the courthouse could
24 get on, let's say, social networking sites, and then
25 additional rules that could be applied in other policies

Carol L. Naughton, Official Court Reporter

—N. Medvidovic - Direct—

1 could be, on top of that, particular computers cannot get off
2 of the, let's say, internal network, for example. So there
3 are various kinds of rules that you can build into different
4 policies that could be applicable all the way down to
5 individual users. So you could really fine-tune this, or you
6 could apply them at the level of an entire subnetwork. But
7 that's exactly correct.

8 THE COURT: All right.

9 BY MR. ANDRE:

10 Q. If we go down to the very next paragraph of this
11 document, it actually refers to not relying on the manual
12 rule sets.

13 Could you describe what is being discussed there.

14 A. Yes. So here it uses these sort of buzz words like
15 "advanced statistical modeling" and "machine learning," but
16 essentially what it does is exactly what the Judge just asked
17 about a second go. It, basically, looks at the network
18 traffic, and as it's looking at it, it learns and determines
19 what's happening inside of it and continually evolves its own
20 sets of rules, which, in turn, will help also evolve the
21 corresponding policies.

22 So, as I mentioned a second ago, the kinds of things
23 that are done today to protect me may be somewhat different
24 from the kinds of things that were sufficient to protect me
25 to the same extent yesterday. So this is constantly moving

—N. Medvidovic - Direct—

1 forward, and what it does is it tries to stay a step ahead of
2 malicious agents on the network, on the Internet.

3 THE COURT: Well, this ability of the system to
4 learn via the machine replaces reliance on historical data,
5 which used to be used in threat analysis.

6 In other words, historical data is at the end of the
7 trail, after the packet is received by the recipient. This
8 system learns new rules and applies them as the packets move
9 through the system, instead of waiting until the end.

10 THE WITNESS: That is correct, Your Honor. In a
11 sense, it pushes this notion of historical data to other
12 places like, in this case, the Cognitive Threat Analytics
13 system that Cisco provides. And what it does --

14 THE COURT: Well, it still uses the historical data,
15 but it adds this to the historical data, I assume.

16 THE WITNESS: Absolutely. It makes these
17 intelligent inferences based on the historical data, so it's
18 sort of like the difference between me reading an article
19 about what might have happened in Napoleonic France and a
20 professor of history, taking that same article and
21 extrapolating a lot of information and connecting it to a
22 bunch of different things that I might not even be aware of,
23 as a layperson.

24 That's exactly what machine learning in this context
25 does; it takes this data and then makes these very smart

Carol L. Naughton, Official Court Reporter

—N. Medvidovic - Direct—

1 inferences so that the whole is much larger than the sum of
2 the individual parts.

3 THE COURT: Well, in other words, it could learn
4 that Napoleon was eventually going to invade Russia.

5 THE WITNESS: And fail at it, too. That was the way
6 he approached --

7 THE COURT: And fail at it, huh?

8 THE WITNESS: Yep, that's exactly right.

9 THE COURT: Okay.

10 BY MR. ANDRE:

11 Q. Go down to the next paragraph. There's a paragraph with
12 three bullet points, and I want to talk about the importance
13 of the first bullet point to the system here.

14 A. Yes. So this, basically, dovetails with what we just
15 discussed.

16 This is machine learning and machines discovering
17 threats through this process of learning and applying these
18 rules and policies, and so on, inside of the Cognitive Threat
19 Analytics system. And the whole point is that we want to
20 take the human out of the loop, because this is not one of
21 the things that humans are very good at. There are lots of
22 things that we do very well, but this kind of thing and the
23 massive data scales that we're talking about here, we just
24 can't keep up, which is why we want systems like Cognitive
25 Threat Analytics to do this automatically for us.

Carol L. Naughton, Official Court Reporter

—N. Medvidovic - Direct—

1 Q. Go down to the bottom of this page. There's a heading
2 called "Stealthwatch With Cognitive Analytics."

3 Could you blow that up.

4 Could you describe to the Court why this is
5 important to the Cognitive Threat Analytics?

6 A. Absolutely. So everything we've talked about so far is
7 applicable in general with respect to Cognitive Threat
8 Analytics, this page that we're looking at right now, this
9 document. But, really, for the most part, a lot of the
10 things that have traditionally been done have dealt with sort
11 of exposed traffic or naked traffic, and what this is
12 addressing is the fact that Cisco also has a solution to do
13 those same kinds of things when the traffic itself is
14 encrypted.

15 So this Stealthwatch with cognitive analytics is
16 basically all these capabilities of advanced statistical
17 models and machine learning and all the things that we talked
18 about in the last few minutes, but with the added twist that
19 we're applying this to traffic where we can't actually see
20 what's inside of the data packets, other than that what they
21 call "treasure trove of metadata" that is hidden in the
22 packet headers.

23 Q. When it talks about "correlating local traffic models
24 with global threat behaviors to give you a rich threat
25 context around network traffic," what's that referring to?

—N. Medvidovic - Direct—

1 A. This is basically generating that intelligence. It says
2 that the amount of stuff that you can see at any one point in
3 time is going to be a tiny slice of whatever is happening on
4 the network, and what this is doing is it's building those
5 correlations so that it's capable of determining things that
6 a naked eye could completely miss.

7 That deals effectively with, for example, obfuscated
8 traffic, so it's capable of building these correlation models
9 and determining things that were previously not possible
10 before this kind of technology was built.

11 Q. You mentioned earlier based on the Judge's question about
12 firewalls. I want to talk briefly about the Firepower
13 Management Center, which is one of the issues here.

14 If we can go to the slide with the Firepower
15 Management Center, could you describe what is the Firepower
16 Management Center, and what is the brain inside of it.

17 A. Sure. So this box here that I called before a pizza box,
18 because that's a colloquial term used in the industry in
19 terms of the shape -- it looks like a box in which you might
20 get a pizza, a take-out pizza -- this is one of the Cisco
21 firewall boxes that we talked about before, and inside of it,
22 this Firepower Management Center deals with managing said
23 firewall with malware protection, with intrusion prevention
24 and detection, and so on.

25 And what it does is it gets a lot of data from all

—N. Medvidovic - Direct—

1 kinds of third parties, and it also gets the data from the
2 Cisco security analytics, and the Firepower Management Center
3 kind of aggregates all that data, ingests it, correlates the
4 various kinds of observations, creates these incident reports
5 and what they call, on the bottom on the right, refines the
6 security posture. And that's really nothing more than
7 adjusting how the system itself, in this case the firewall,
8 is going to respond to subsequent traffic coming down the
9 pike, coming down the network, based on what it has seen
10 previously and on these models that it's been able to build,
11 the correlation that's it's been able to establish, and so
12 on.

13 THE COURT: Would you call this the last line of
14 defense, if it gets through the routers and switches?

15 THE WITNESS: In fact, Your Honor --

16 THE COURT: Then it will get to the firewall
17 management center at the end of the line, so to speak?

18 THE WITNESS: In a sense, it's definitely the outer
19 line of defense, but one way I think of, maybe a more
20 accurate way to think about it, it would be your first line
21 of defense. Because your routers and switches will be, in a
22 way, hidden behind the firewall, so the first thing that the
23 outside traffic will hit is the firewall, and then the
24 firewall will do its job, try to do as much of this as it's
25 been built it do, and then when it lets the traffic

—N. Medvidovic - Direct—

1 eventually through to the routers and switches, then those
2 security capabilities inside of them will have to provide
3 additional defenses.

4 And, as we talked about --

5 THE COURT: So it's more of a gateway.

6 THE WITNESS: Yes, in a sense this is the gateway;
7 although, I think it's important to keep in mind that the way
8 both -- or all three, I guess, the firewall, the routers, and
9 the switches, are used within a Cisco architecture, all of
10 them are gateways, they're just control gates at different
11 points in your, let's say, fortifications.

12 THE COURT: But this is the first, not the last,
13 usually.

14 THE WITNESS: Correct, this is, in a sense, the
15 first line of defense, because you place your firewall at the
16 very outer edge of the network you're trying to protect. You
17 can think of it that way.

18 BY MR. ANDRE:

19 Q. Does the firewall and the routers and switches -- are
20 those, as you say, different kinds of gateways? Are they all
21 in line with the system?

22 A. Yes. So at some point, as we saw in that very first
23 document from 2017, Cisco decided to put a lot of these
24 security capabilities into their switches, into their
25 routers, and, once that was done, those switches and routers

—N. Medvidovic - Cross—

1 also became gateways, because they provide a lot of security,
2 which I think I mentioned just a few minutes ago.
3 Traditionally, way back in the day, all of that was the job
4 of a firewall, and the dumb routers and the dumb switches
5 were there really to route traffic and make sure that it gets
6 to the appropriate locations as quickly as possible.

7 Now, with this new generation of things, there is
8 this sort of infusion of a lot of sophisticated capabilities,
9 security capabilities, not just in the firewall but also in
10 the routers and in the switches, and that means that all
11 three of them control different gates in your system,
12 depending on how your system is configured. But all three of
13 them are gateways.

14 Q. Thank you, Dr. Medvidovic.

15 MR. ANDRE: I've got no further questions, Your
16 Honor.

17 THE COURT: So is your short presentation complete
18 now?

19 MR. ANDRE: It evolved.

20 THE COURT: All right, Mr. Gaudet.

21 MR. GAUDET: Thank you, Your Honor.

22 CROSS-EXAMINATION

23 BY MR. GAUDET:

24 Q. And good afternoon, Dr. Medvidovic.

25 A. Good afternoon.

—N. Medvidovic - Cross—

1 Q. Dr. Medvidovic, you did not, yourself, perform an
2 infringement analysis to determine whether Cisco in any of
3 these products infringed any of the Centripetal patents; is
4 that correct?

5 A. That's correct.

6 Q. Okay. Now, I just want to talk briefly about
7 Stealthwatch and some of the related products to be sure
8 we're on the same page about their operation.

9 Now, if packets, right, traffic arrives at a router
10 or a switch and the customer has Stealthwatch, then
11 information about those packets, in the form of NetFlow
12 summaries, will be sent from the router or switch to
13 Stealthwatch; is that correct?

14 A. I think -- I mean, this has come up a lot earlier today
15 in the context of Dr. Cole's cross-examination, in
16 particular. That is not something that I opined on in my
17 report explicitly, but I believe that the way Dr. Cole
18 described it is accurate, based on what I've seen.

19 So some of that data will go to Stealthwatch. Some
20 of that data is going to be summaries, but I believe that
21 Dr. Cole also talked about some other information that goes
22 beyond just what you called summaries, also going to the
23 Stealthwatch.

24 Q. Okay. But the packets themselves --

25 THE COURT: All right. You're going to jump into

—N. Medvidovic - Cross—

1 trying to get on this point that information from the packets
2 goes to Stealthwatch instead of the packets themselves, so
3 you're going through the same thing that your predecessor
4 did.

5 MR. GAUDET: Your Honor, I'm done with that topic.
6 He had said one thing during his direct examination that I
7 was concerned might have contradicted something Dr. Cole
8 said. He just clarified that's not the case. I'm done with
9 that topic.

10 I actually only have one more topic. I might get
11 the record for shortest interaction with a witness.

12 THE COURT: Well, I'll think up an award for that,
13 if you give me a little time.

14 BY MR. GAUDET:

15 Q. Dr. Medvidovic, by the time that Stealthwatch performs
16 whatever analysis it's going to perform on the information it
17 received from a router or switch, the packet, the packet that
18 arrived at that router or switch, it's already at its
19 destination. Do you agree with that?

20 A. I have not done the analysis of the speed at which these
21 things occur, and, to be honest with you, I have not seen any
22 documents that suggest that I would be able to take your
23 statement, your question, at face value. I don't think
24 that -- it's possible that Cisco has done those kinds of
25 benchmarks. I have not seen any of them.

—N. Medvidovic - Cross—

1 Q. Fair enough.

2 MR. GAUDET: Your Honor, I would like to lay claim
3 on my award for this. My cross-examination is complete.

4 THE COURT: All right. I'll write "award" right
5 here.

6 THE WITNESS: Your Honor, do I get an award for
7 being the shortest witness so far?

8 THE COURT: How tall are you? You mean the briefest
9 or the shortest?

10 THE WITNESS: Oh, that's a good point.

11 MR. ANDRE: He towers over 6 foot, so I don't think
12 he's going to make the shortest.

13 THE COURT: All right.

14 MR. ANDRE: Your Honor, I don't have any redirect
15 for Dr. Medvidovic. Thank you.

16 THE COURT: All right.

17 MR. ANDRE: He's no longer -- we brought him back
18 twice in the case, and this is the last you'll see of him in
19 this case, I hope.

20 THE COURT: Does the defense agree with that?

21 MR. GAUDET: We do, Your Honor. I was on mute. I
22 apologize.

23 THE COURT: All right, Doctor. You can be excused
24 as a witness, with the understanding that you can observe the
25 remaining portions of the trial, if you wish, on audio -- or,

1 if everybody lets you, I suppose you can do it on video --
2 but you should not discuss your testimony with any other
3 witness in the case until the case is concluded.

4 THE WITNESS: I understand, Your Honor.

5 THE COURT: And you're not obligated to watch or
6 listen to anything further, if you don't choose to. So
7 you're excused.

8 THE WITNESS: Thank you, sir.

9 (Witness excused.)

10 MR. ANDRE: Your Honor, Ms. Kobialka will be doing
11 the next witness for Centripetal, so I will slide out and let
12 her slide in.

13 THE COURT: All right.

14 MS. KOBIALKA: It's nice to have a chance to move
15 Mr. Andre to the side here.

16 At this time, Your Honor, we would like to call
17 Mr. Jonathan Rogers, of Centripetal Networks.

18 THE COURT: All right.

19 (The witness was sworn.)

20 THE COURT: What bridge is that in the background?

21 THE WITNESS: That is a new bridge that they just
22 built, which goes from Portsmouth, New Hampshire into
23 Kittery, Maine. It's a three-level bridge for trains and
24 cars, Your Honor.

25 THE COURT: Well, I'll be crossing it this summer.

—J. Rogers - Direct—

1 I go to Maine every summer. That's a brand new bridge?

2 THE WITNESS: Yes, Your Honor. That one is on
3 Route 1-A, I believe.

4 THE COURT: All right. You may proceed.

5 MS. KOBIALKA: Thank you, Your Honor.

6 JONATHAN ROGERS, called by the Plaintiff, having
7 been first duly sworn, was examined and testified as follows:

8 DIRECT EXAMINATION

9 BY MS. KOBIALKA:

10 Q. Mr. Rogers, what is your position at Centripetal?

11 A. I am the Chief Operating Officer.

12 Q. And how long have you been at Centripetal?

13 A. I've been at Centripetal since about May 2010. I was the
14 fourth employee.

15 Q. Any relation to Mr. Steven Rogers, who has already
16 testified?

17 A. Yes. Steven is my father.

18 Q. Let's do a little bit about your background, if we could
19 pull up the first slide.

20 Could you give us an overview of your educational
21 background?

22 A. Sure. So I entered higher education at Boston
23 University, where I got a Bachelor of Science in electrical
24 engineering. And while I was there, I focused my studies in
25 communication systems, and then later, after that, I got a

—J. Rogers - Direct—

1 Master's degree in business administration from the
2 University of Maryland, where in that degree program I
3 concentrated in finance.

4 Q. And can you talk a little bit about your work experience,
5 which is the rest of the slide there?

6 A. Yes. After graduating in my undergrad, I entered the
7 U.S. Navy. I was commissioned as an officer in the Navy, and
8 I joined a community which is called Cryptology and
9 Information Warfare. It's the Navy's security group, and
10 what the Navy's security group does is both protect naval
11 military communications, as well as the corollary to that,
12 which is to exploit adversary communications.

13 And I got assigned from there, as a military
14 officer, to be stationed at the National Security Agency,
15 where I spent a number of years working in the National
16 Security Operations Center, which is, in effect, the signals
17 intelligence fusion center for the country, so a very
18 critical environment.

19 And then later, I moved on to an assignment where I
20 would forward-deploy on attack submarines for the collection
21 of intelligence.

22 Q. And then I see something there at the Central
23 Intelligence Agency. Could you describe that?

24 A. Yes. So after my tour in the Navy, I became a civilian,
25 and I joined the Central Intelligence Agency, where I became

—J. Rogers - Direct—

1 a technical intelligence officer. And my responsibility was
2 to run large development programs for communication systems
3 for some of the most sensitive communication systems we have
4 in the country.

5 Q. And did you take all of that background and then go to
6 Centripetal?

7 A. Yes, absolutely. So when Steven was founding the
8 company, he came to me with a vision for how we could take
9 intelligence, and if we could operationalize that in the
10 Internet and do that at scale, that we could effectively
11 solve the majority of the cyber security problems.

12 So as an intelligence officer, that resonated with
13 me, but I also knew that that was something that would have
14 to be done in the private sector, so I leapt at the chance
15 and joined Centripetal.

16 Q. I notice you referred to your father as "Steven." Could
17 you just explain that?

18 A. Sure. It's a long-time habit from working together. We
19 just use a first name basis to keep it professional.

20 Q. Now, did Centripetal recruit a board of directors?

21 A. We did. So because of what we were doing and our
22 corporate strategy, which was to take intelligence and to
23 operationalize that data and to use some of the same
24 defensive approaches using intelligence that the intelligence
25 community itself uses, we retained a number of executives in

—J. Rogers - Direct—

1 the intelligence community to come and join our board and our
2 advisory board.

3 So one of those gentlemen was Bob Flores, who was
4 the former Chief Technology Officer of the CIA. Another was
5 Bob Gourley, who was also a former Chief Technology Officer
6 but of the Defense Intelligence Agency. We were joined by
7 William Crowell, who was the Former Deputy Director of the
8 National Security Agency.

9 And another gentleman who joined as the head of our
10 advisory board is a gentleman named Dr. Paul Kaminski, and
11 he's a very notorious individual in the defense and
12 technology community. He's Chairman of the Defense Science
13 Board, and one of his personal accomplishments is that he ran
14 the program to deliver stealth technology to the
15 United States.

16 Q. We've heard a lot about the technology, but I was hoping
17 from a marketing perspective we could maybe talk a little bit
18 and just see what Centripetal's product looks like.

19 So could you just describe Centripetal's solution
20 that it offers in the marketplace today?

21 And I think we have a slide so we can take a look at
22 it.

23 THE COURT: Do we have a book for his direct
24 examination? I think we do.

25 MS. KOBIALKA: Yes, Your Honor.

J. Rogers - Direct

1 THE COURT: Let me get that.

2 Okay.

3 BY MS. KOBIALKA:

4 Q. So if you could just describe what we're seeing on here
5 with respect to the RuleGATE and the QuickTHREAT Advanced
6 Cyber Threat.

7 A. Sure.

8 THE COURT: Is this a demonstrative exhibit? Is
9 this in the book or not?

10 MS. KOBIALKA: It is a demonstrative, Your Honor,
11 and I believe it should have been provided to you, as well,
12 in hard copy.

13 THE COURT: In the book? It has demonstratives
14 here.

15 MR. JAMESON: Unless I'm missing something, I
16 thought this was Plaintiff's Exhibit 547 at Page 10.

17 MS. KOBIALKA: It is also PTX-547 at Page 10, but
18 there is --

19 THE COURT: I guess it must be in two places,
20 because it's with the demonstratives.

21 MS. KOBIALKA: Yes, this one we used as a
22 demonstrative.

23 THE COURT: Okay.

24 BY MR. ANDRE:

25 Q. Mr. Rogers, if you could, explain what we're looking at

J. Rogers - Direct

1 here.

2 A. Yes, certainly. So in the center is our RuleGATE product
3 platform, and that is the product that we've been developing
4 since our inception, for taking intelligence and applying
5 that in the network-to-network traffic.

6 And so on the left-hand side what's visualized is
7 dynamic threat intelligence that gets delivered into the
8 RuleGATE, and on the right-hand side is the user interface
9 that a threat operator would see when they review the results
10 from the RuleGATE.

11 Q. And is that user interface called QuickTHREAT?

12 A. Yes. That's just a marketing term that we use for that
13 user interface.

14 Q. I've also heard the market term CleanINTERNET. Could you
15 explain what that is?

16 A. Yes. CleanINTERNET is a marketing term for where we take
17 the RuleGATE platform and we provide that to our customers as
18 a subscription service. So it's, in effect, a RuleGATE added
19 service where Centripetal does the management.

20 Q. And I'm looking on the demonstrative here. It says,
21 "RuleGATE devices are deployed in a customer's network at key
22 points for real-time evaluation and management."

23 Could you just explain in layman's terms? What does
24 that mean?

25 A. That means that you can put the RuleGATE at an enterprise

—J. Rogers - Direct—

1 that has critical connections, like to the Internet, and the
2 RuleGATE can be used to clean up that Internet connection and
3 to get rid of threat traffic.

4 Q. So when Centripetal offers clean Internet security as a
5 service, just how does that work? Do you take a RuleGATE and
6 put it in the client's network? Could you just explain that?

7 A. Certainly. So every time that we get a customer who
8 subscribes to CleanINTERNET service, we'll take a RuleGATE,
9 we'll deploy that in their Internet connections, and then we
10 will run threat intelligence that we curate and send down to
11 the RuleGATE devices, which will then both detect and block
12 threats. And the reporting of that comes back to us in our
13 security operations center, and then we meet with our
14 clients, discuss the results, and constantly tailor the
15 security approach.

16 Q. I'd like to just briefly identify some of the different
17 types of customers you have.

18 A. Yes. We have customers across many different segments.

19 THE COURT: Before we get into that, let me clarify
20 this clean network. Would you give me that again? I'm not
21 sure I got it.

22 THE WITNESS: Yes, Your Honor. So CleanINTERNET is
23 a marketing term that we use to brand a service, where we
24 will take the RuleGATE product that we've developed, we'll
25 deploy that in our customer's network, and we'll run it for

—J. Rogers - Direct—

1 them, so to protect their enterprise and to clean up their
2 internet connection. We call that CleanINTERNET service.

3 THE COURT: So that doesn't mean, for example, that
4 your service would replace any other security device on a
5 client's network. It would function in addition to what they
6 already have?

7 THE WITNESS: Yes, Your Honor. In most cases, it
8 will be an additive layer of security. The client will
9 maintain other tools that are in place, and we'll be that
10 additive intelligence layer where they subscribe to our
11 service, and we clean up their Internet connection.

12 THE COURT: What do you mean by you "clean up" the
13 Internet?

14 THE WITNESS: Well, we use threat intelligence to
15 identify all of this malicious and unwanted traffic that's
16 both coming at them and that may be exfiltrating from their
17 network, as well. And so, ideally, we will be able to block
18 and to remove that threat traffic.

19 THE COURT: Okay. You may proceed.

20 MS. KOBIALKA: Thank you.

21 BY MS. KOBIALKA:

22 Q. And maybe I'll just ask one follow-up question.

23 Is it similar to where somebody gets like a cable
24 box and they get some services provided to them? Could you
25 kind of explain that? That might help.

—J. Rogers - Direct—

1 A. Yes, exactly. So instead of buying a RuleGATE, deploying
2 it, and operating it themselves, with CleanINTERNET we own
3 the RuleGATE device, but as part of the service, we deploy it
4 to the customer, and then we run it for them. So it's very
5 much like a cable box and an Internet service provider.

6 Q. All right. So, just briefly, you were going to describe
7 the customers that you have and the different industries
8 they're in.

9 A. Certainly. So CleanINTERNET is a solution. The
10 RuleGATE, as a product, is applicable to pretty much every
11 type of business that connects and uses the Internet, and so
12 we've got a broad range of customers that cover everything
13 from government agencies, like the Department of Homeland
14 Security, and components therein, Immigration and Customs
15 Enforcement, to executives. We protect a U.S. cabinet
16 secretary. We protect the chief executive of a foreign
17 country. We protect foreign government agencies.

18 Then we have critical infrastructure providers, like
19 power plants, hospitals, technology companies that actually
20 operate some of the infrastructure for the Internet, regional
21 banks, retailers, so a very broad and diverse set of
22 customers.

23 Q. To date, how much has Centripetal spent on research and
24 development, from the founding of the company through the
25 present?

—J. Rogers - Direct—

1 A. So to date we've invested approximately \$65 million in
2 developing our products and services.

3 Q. And those are the ones we just talked about a minute ago.
4 Is that right?

5 A. That's correct.

6 Q. Now, are patents important to Centripetal?

7 A. They're extremely important. What a patent does is it
8 serves as a barrier to entry, so that a company who has the
9 vision for something can have the room to go in and to
10 execute. So this is a very capital-intensive space. We've
11 invested a lot ourselves, and our patents are critical to us.

12 Q. Does Centripetal mark its products with patent numbers?

13 A. Yes, we do. In our research, we will come across
14 innovative solutions that we'll then proceed for filing for
15 patent protection on.

16 When those patents ultimately issue, we produce a
17 label that has all of the issued patents that are applicable
18 to the product, and we mark that product when it's
19 manufactured.

20 Q. I would like to show you what we've marked as PTX-528.

21 MS. KOBIALKA: And this should be in your binder,
22 Your Honor.

23 THE COURT: All right, I have it.

24 BY MS. KOBIALKA:

25 Q. Mr. Rogers, could you just describe what you're looking

—J. Rogers - Direct—

1 at here?

2 A. So this is the patent-marking label that we affix to the
3 RuleGATE product. This is a photograph of that.

4 MS. KOBIALKA: Your Honor, I'd like to move this
5 into evidence.

6 MR. JAMESON: No objection, Your Honor.

7 THE COURT: That will be admitted.

8 (Plaintiff's Exhibit PTX-528 was received in
9 evidence.)

10 THE COURT: Now, there was an *inter partes* review of
11 certain of your patents, and I think certain claims were
12 disallowed.

13 Were any of the patents shown in this picture among
14 those who had particular claims disallowed?

15 THE WITNESS: I believe so, Your Honor. I believe
16 that some of these patents were subject to IPR.

17 THE COURT: Yes, well, some of them were subject to
18 IPR, and some of them they disallowed, and others they
19 didn't. But some of these patents do include claims that
20 were disallowed on IPR, but, of course, none of those are the
21 subject of this proceeding.

22 THE WITNESS: I believe that's correct, Your Honor.

23 THE COURT: Okay. All right. You may proceed.

24 BY MS. KOBIALKA:

25 Q. Now, when do patent numbers get added to the product?

—J. Rogers - Direct—

1 A. So immediately after the issuance of the patent, we
2 update our label and affix that to all of the manufactured
3 products.

4 Q. And has Centripetal marked the five patents asserted in
5 this case on its RuleGATE products after those issued?

6 A. Yes, we have.

7 Q. Okay. Can you describe what the marketplace was like, in
8 terms of offering products for sale, when you first entered
9 the marketplace?

10 A. So when we first entered the marketplace, we were
11 advocating for a real-time operationalized threat
12 intelligence defense, and at that point, we had a green field
13 with respect to that idea. No one else was advocating for
14 that type of defense, and that was very new, as far as a
15 security strategy.

16 Q. Okay. Was there a shift in security strategies in the
17 marketplace?

18 A. Yes. We started to see a shift towards the desire for an
19 intelligence-based defense, towards adopting intelligence
20 strategies, and then we also started to see a shift towards
21 our approach, which was to apply intelligence in a zero trust
22 way.

23 THE COURT: In a what? A zero what?

24 THE WITNESS: In a zero trust way.

25 THE COURT: What does that mean?

—J. Rogers - Direct—

1 THE WITNESS: What that means is that the legacy
2 network security products operated with some assumptions of
3 trust. They assumed that the corporate network was something
4 that you could trust and the internet was something that you
5 couldn't. And that assumption is what got defeated, what
6 proved to be invalid, as security threats evolved.

7 Because what turned out is that you could have
8 malware active inside of your network, and it could get out
9 because the network security devices assumed that the
10 corporate network was trustworthy and didn't examine for
11 those types of threats.

12 And it was also possible to engineer ways to get out
13 from phishing and other types of approaches, like a bad actor
14 inside of your company.

15 THE COURT: So a zero trust means you didn't trust
16 anything.

17 THE WITNESS: That's exactly right, Your Honor. We
18 didn't trust anything, and we wanted to evaluate all traffic
19 against all intelligence all the time.

20 THE COURT: And you're saying that you were the
21 first company to do that?

22 THE WITNESS: Certainly, the different techniques
23 that we developed for taking intelligence and applying it in
24 that way, yes, Your Honor.

25 THE COURT: Well, what is it that you're claiming

—J. Rogers - Direct—

1 that you did first; apply this proactive as opposed to
2 reactive approach, or the zero trust, or both?

3 THE WITNESS: There's a number of things to it, Your
4 Honor, and both of the ones that you mentioned are certainly
5 part of it. But when you decide that you're going to rely on
6 external information, in the intelligence community, one of
7 the first problems that you have is to be able to get all of
8 that data into a system and to make it active. And there's a
9 lot of that data, so you wouldn't want that to be some type
10 of a static thing that's done by an operator or that's done
11 manually. So you have all of that intelligence that you have
12 to dynamically deliver into a system.

13 Then the next problem that you have is you can't
14 afford to have an outage, because if you were to have an
15 outage when you updated, you may never be in service, because
16 the outage time, with the amount of updating that you have to
17 do, would be a huge impediment to operations. So you have to
18 be able to rapidly swap out those policies without losing
19 anything. So that's a key problem.

20 Then you have the problem of most solutions, as I
21 mentioned, were -- had some trusts, had some assumptions of
22 trusts built in. So they weren't necessarily scrutinizing
23 all of the ways in which exfiltration could be accomplished.

24 And then, of course, we saw the development of
25 encrypted traffic, which obfuscated all of the other

—J. Rogers - Direct—

1 approaches, and we developed solutions there, as well, Your
2 Honor.

3 THE COURT: All right.

4 BY MS. KOBIALKA:

5 Q. Mr. Rogers, this concept of zero trust, is that an
6 industry term that's used?

7 A. Yes, there's been a movement towards zero trust because
8 the security problem has gotten so bad that it is -- it's
9 ended up being -- there's ended up being a recognition that
10 everything should be inspected.

11 Q. And has there been some examples that you can think of of
12 an insider letting information out?

13 A. Yes. There's famous examples of insiders getting
14 information out. Edward Snowden is a very good example of
15 that. So you can have untrusted individuals, as well as
16 untrusted software, malware, et cetera.

17 Q. Okay. So now turning back to the market that Centripetal
18 was seeing, over time did you see other parties start to
19 enter that market?

20 A. We did. We saw large network security equipment
21 manufacturers start to move into the space.

22 Q. And who did you see?

23 A. Well, the first one that we saw and came across was a
24 company called Ixia, and they were bought by another company,
25 Keysight.

J. Rogers - Direct

1 THE COURT: Another company what?

2 THE WITNESS: They were bought by another company
3 whose name is Keysight, Your Honor.

4 THE COURT: Keysight?

5 THE WITNESS: Yes, Your Honor.

6 THE COURT: Okay.

7 BY MS. KOBIALKA:

8 Q. And did you have litigation with Keysight before Judge
9 Morgan?

10 A. Yes, we did. That was the subject of our other and first
11 lawsuit.

12 Q. Now, did you see any other follow-on companies coming
13 into your market?

14 A. Yes. We saw Cisco move into the space, and -- oh, go
15 ahead.

16 Q. Were there any other follow-ons that you saw?

17 A. Yes. Since then, we have also seen Juniper and --
18 Juniper Networks and Palo Alto Networks move into the space.

19 Q. Now, when there wasn't the competition, was that
20 reflected in Centripetal's sales?

21 A. Yes. We initially entered the market and started selling
22 to very large enterprise. They had what we call value at
23 risk. They had the biggest problem and the highest cost
24 associated with it, so they have a strong willingness to
25 adopt new technologies. And we were successful at selling in

Carol L. Naughton, Official Court Reporter

—J. Rogers - Direct—

1 that space. We ended up doubling our revenue year over year
2 for our first three years when we were making sales there,
3 but in 2017, we saw that large enterprise market flatline on
4 us.

5 Q. So what did Centripetal have to do in order to address
6 this competition with the sales that you were seeing?

7 A. So when we saw large network security companies come into
8 the space, we knew that we weren't going to be effective at
9 competing head-to-head against them with no technology
10 advantage; that competing against our own technology, when
11 the marketing resources, the sales resources, and the
12 distribution channels are all immensely lopsided, wasn't
13 going to be effective.

14 So what we did was we invested even further in the
15 RuleGATE platform to be able to remote-control it and to
16 develop all of the technologies to where we could make
17 CleanINTERNET service viable. And when we had that, we moved
18 further down markets, out of the large enterprise space and
19 into the middle market, where we could win smaller customers,
20 albeit one by one.

21 Q. So initially were the customer base, largely in the
22 enterprise base, the big companies?

23 A. Yes. The large enterprise space is ideally where you
24 want to enter with new technology, because your individual
25 deal prices can average 250,000 or more, and you have very

—J. Rogers - Direct—

1 strong margins, so you can begin to recoup a lot of the high
2 capital investments that you've made.

3 But in the middle market, your deal sizes range more
4 on the order of \$25- to maybe \$50,000 a transaction, and your
5 margins are lower.

6 Q. Has Centripetal continued to make revenues, even in 2017
7 and thereafter?

8 A. Yes. We've continued to provide our RuleGATE product as
9 a service under the CleanINTERNET moniker, and we've
10 continued to win a number of customers every year.

11 Q. I'd like to talk about the communications that
12 Centripetal has had with Cisco over the years, and I have a
13 timeline here.

14 If we could pull up slide, I believe, 4.

15 So looking at timeline, it starts with this June
16 2015 date, and my question to you is: Prior to that date,
17 were there any communications between Centripetal and Cisco?

18 A. Yes. We had developed a technology partnership prior to
19 this, in 2014, with a company called ThreatGRID. That
20 company was a provider of threat intelligence data, and they
21 ultimately got acquired by Cisco.

22 Q. Okay. Can you explain why would you enter into a
23 partnership with ThreatGRID? What was the purpose of that
24 partnership?

25 A. So the purpose of that partnership was because we saw a

—J. Rogers - Direct—

1 unique problem that they had, which was the operationalizing
2 of threat intelligence data.

3 At this point in the market, customers didn't have a
4 way of operationalizing the threat intelligence data, and
5 that was something that we brought to the table for
6 ThreatGRID.

7 THE COURT: What is the name of the company? Threat
8 what?

9 THE WITNESS: ThreatGRID. G-r-i-d, Your Honor.

10 THE COURT: And they were acquired by Cisco?

11 THE WITNESS: That's correct, Your Honor.

12 THE COURT: When?

13 THE WITNESS: I believe that was partway through
14 2014.

15 THE COURT: Okay.

16 BY MS. KOBIALKA:

17 Q. Now, turning to the timeline, were there a number of
18 meetings with Cisco in 2015?

19 A. Yes. We had interest from an individual at Cisco named
20 Pavan Reddy. He was looking to have us build complementary
21 solutions for customers where we could operationalize threat
22 intelligence.

23 MR. JAMESON: Your Honor, I'm going to object to the
24 testimony from this witness with respect to an interaction
25 between Steve Rogers and Pavan Reddy on the basis of hearsay.

—J. Rogers - Direct—

1 He was not a party to this conversation that he is testifying
2 to.

3 MS. KOBIALKA: Actually, I can move past this. I
4 don't need to get into those.

5 I was just asking whether or not there were a number
6 of meetings between Centripetal and Cisco in 2015.

7 BY MS. KOBIALKA:

8 Q. Mr. Rogers, can you just answer that question?

9 THE COURT: Yes, well, he can answer that question.

10 THE WITNESS: Yes, there were several meetings in
11 2015 between Centripetal and Cisco.

12 BY MS. KOBIALKA:

13 Q. And were there also demonstrations of Centripetal's
14 product to Cisco?

15 A. Yes, there were demonstrations.

16 Q. Okay. Now, at some point in early 2016, was an NDA
17 signed between Cisco and Centripetal?

18 A. Yes. We were introduced to the Cisco corporate
19 development team, had a couple of discussions, and then we
20 entered into a nondisclosure agreement.

21 MS. KOBIALKA: At this time, Your Honor, I would
22 like to mark and move into evidence PTX-99, entitled
23 "Confidentiality Agreement."

24 THE COURT: PTX-99 will be admitted.

25 (Plaintiff's Exhibit PTX-99 was received in

J. Rogers - Direct

1 evidence.)

2 BY MS. KOBIALKA:

3 Q. Mr. Rogers, is this the confidentiality agreement that
4 Centripetal signed with Cisco?

5 A. Yes, it is.

6 Q. And what is the date of the agreement?

7 A. The date of the agreement is January 26 of 2016.

8 Q. And if we turn to the very last page of this exhibit,
9 with the Bates number 1938, who signed the agreement?

10 A. I signed the agreement on behalf of Centripetal, and a
11 gentleman named Karthik Subramanian signed the agreement on
12 behalf of Cisco.

13 Q. And what was being discussed between Cisco and
14 Centripetal around this time?

15 A. There were a number of things. In addition to the
16 synergy for our technical solutions and how we could
17 operationalize threat intelligence and how that could be
18 relevant to joint customers, we were discussing with the
19 corporate development team the potential for Cisco to become
20 a strategic investor of Centripetal.

21 Q. Okay. So I want to make sure I understand.

22 What do you mean by "synergy" of technical solutions
23 between Cisco and Centripetal, in just plain English?

24 A. In plain English, that we could operationalize threat
25 intelligence, and that was something that they saw a value in

—J. Rogers - Direct—

1 for us to joint-sell to customers.

2 Q. And then you said the words "strategic investor." What
3 do you mean by that?

4 A. So a regular investor is just purely motivated by a
5 financial return. A strategic investor has other
6 business-level alignment, other mutual interests. In this
7 particular case, that was our technology.

8 Q. And did you sign the NDA in connection with the
9 possibility of jointly selling products and for the strategic
10 investment to discuss those possibilities?

11 A. Yes, all of those possibilities were with respect to the
12 nondisclosure agreement.

13 Q. So I'd like to go back to the timeline, if we can.

14 So after the NDA was signed in January 2016, what
15 happened next?

16 A. We had a couple conversations with the corporate
17 development team in preparation for a technical meeting that
18 they were putting together, and then they collected a group
19 of top-level Cisco technologists to come in to have a
20 briefing with us.

21 Q. And was that briefing the Webex on February 4, 2016?

22 A. Yes, it took place over Webex on February 4, 2016.

23 Q. And leading up to that Webex, were you provided with
24 information about what needed to be presented on that
25 February 4, 2016 meeting?

—J. Rogers - Direct—

1 A. Yes. The corporate development team was collecting the,
2 you know, top technology leaders for the security group to
3 come and participate in this meeting with us. They gave us
4 guidance on the agenda, on what to present and how to present
5 it, both to set out the market, how we saw the problem, and
6 what we uniquely did to address that technology problem.

7 Q. Who attended the meeting on behalf of Centripetal?

8 A. On behalf of Centripetal, I attended; our CEO, Steven
9 Rogers, attended; our Chief Technology Officer, Sean Moore,
10 attended; our Chief Architect, a gentleman named David Ahn,
11 attended; our then head of sales and partnerships, a
12 gentleman named Haig Colter, attended; and then, to provide
13 the demo, two individuals came in, a Doug DiSabello and a
14 Peter Geremia, to conduct that demonstration.

15 Q. Was that demonstration done just toward the end of the
16 Webex meeting?

17 A. That's correct; they came in at the end to do that.

18 Q. And who attended on behalf of Cisco?

19 A. On behalf of Cisco was a gentleman named Bret Hartman, a
20 gentleman named T. K. Keanini.

21 THE COURT: And what? Let me get this, now.

22 THE WITNESS: Yes, Your Honor.

23 THE COURT: Cisco, Hartman. Who was the next one?

24 THE WITNESS: I didn't hear the one you mentioned.

25 THE COURT: Hartman.

—J. Rogers - Direct—

1 THE WITNESS: Yes. So after Bret Hartman, there was
2 a gentleman named T. K. Keanini.

3 THE COURT: How do you spell that?

4 THE WITNESS: The initial T. K. and then last name
5 Keanini, which is spelled K-e-a-n-i-n-i.

6 THE COURT: Okay.

7 THE WITNESS: Then there was a gentleman named Tom
8 McDonough.

9 THE COURT: All right.

10 THE WITNESS: And there was a gentleman named
11 Michael Pakuchek (ph). And I'm afraid I can't spell that one
12 for you, Your Honor.

13 THE COURT: Okay.

14 THE WITNESS: And then also attending were all of
15 the representatives from the corporate development team.

16 So there was a gentleman named Karthik Subramanian,
17 a gentleman named Prasad Parthasarathi, and one other
18 gentleman named Peter Shih.

19 THE COURT: S-h-i? C-h-i?

20 THE WITNESS: S-h-i-h, I believe, Your Honor.

21 THE COURT: Okay.

22 BY MS. KOBIALKA:

23 Q. And outside of the corporate development team,
24 Mr. Keanini, Mr. Pakuchek, and some of the other individuals,
25 what was their roles at Cisco?

—J. Rogers - Direct—

1 A. My understanding is that they were all principal
2 engineers, chief technology officers, so highly technical
3 leaders, with the exception of Mr. McDonough, who I
4 understand is a more general business executive.

5 Q. Okay. At this time I'd like to show you PTX-547.

6 MS. KOBIALKA: And this is already admitted into
7 evidence. There may be a few more pages we'll add into
8 evidence.

9 THE COURT: PTX-547?

10 MS. KOBIALKA: Yes.

11 THE COURT: You've got various pages from this
12 exhibit?

13 MS. KOBIALKA: That's correct, Your Honor.

14 THE COURT: I know I've seen Page 7 before. All
15 right, PTX-547 will be admitted.

16 MS. KOBIALKA: Thank you.

17 (Plaintiff's Exhibit PTX-547 was received in
18 evidence.)

19 BY MS. KOBIALKA:

20 Q. Mr. Rogers, what are we looking at?

21 A. So when we came onto the Webex, I saw that the Webex
22 session itself was being recorded by Cisco, and this is the
23 presentation that I put together and briefed to Cisco.

24 Q. Did you draft this presentation?

25 A. Yes, I did.

—J. Rogers - Direct—

1 Q. And did you present it to Cisco, or were there other
2 people that presented to Cisco?

3 A. Yes, I did, I presented this to Cisco. Steven did some
4 introductory remarks, and then I gave this briefing.

5 Q. And is this a standard presentation that Centripetal
6 gives to anyone?

7 A. No, this is far from it. I built this up in particular
8 with the guidance from the corporate development team for how
9 they wanted us to structure the agenda and the information
10 that we would disclose.

11 Q. Okay. If we could turn to Page 7 of this document,
12 ending in Bates number 19389.

13 MS. KOBIALKA: And we have seen this before.

14 BY MS. KOBIALKA:

15 Q. I'd like to ask you, why did you mark "Confidential and
16 Proprietary Cisco-CNI NDA" at the bottom?

17 A. So because of the fact that we had put in place the NDA,
18 and because of the agenda that was requested, I felt that we
19 had adequate protection to be able to go into a deeper level
20 of disclosure about what we were doing and how we were doing
21 it with respect to the market.

22 Q. Okay. And if I look at the first bullet -- and,
23 actually, the whole slide -- it says, "Centripetal's patented
24 filter algorithms eliminate the speed and scalability
25 problem..." and it continues on.

—J. Rogers - Direct—

1 Can you explain? What was the purpose of this slide
2 and presentation to Cisco?

3 A. So the purpose of this particular slide is we had gone
4 through an overview of the threat intelligence market and the
5 variety of information that's available, the need and the
6 motivation to use that, and this slide was to illustrate how
7 we uniquely have developed solutions to those problems and
8 what those solutions are, those technology solutions.

9 Q. And when you presented this slide, did you describe
10 Centripetal's patented filter algorithms?

11 A. Yes, absolutely. So where I set out the computational
12 problem, I'm describing the function of many of the different
13 algorithmic techniques that we have to use in the product in
14 order to be able to operationalize intelligence.

15 So one of the first things that you see is I'm
16 stating the input/output capacity, and that's what you have
17 to have on an Internet link to be able to implement a zero
18 trust inspection. So that is no assumption of trust, apply
19 all of the intelligence, and evaluate everything, and then
20 describe our use of complex indicators and how those have
21 multiple fields that allow us to do things like detect
22 exfiltration.

23 Then I articulated that, in addition to those other
24 inspection techniques, a critical problem you have is to be
25 able to correlate back to an individual host to be able to

—J. Rogers - Direct—

1 identify it. So simultaneous with all of this other
2 inspection, you have to run a correlation algorithm to
3 process for the host ID.

4 And then one of the last things that I described was
5 that, in addition to all of this, if you could capture the
6 full content of a flow, the way that we had developed for
7 being able to capture PCAP, that if you could also be flow
8 aware --

9 THE COURT: What is PCAP?

10 THE WITNESS: PCAP is a capture of packets. It's a
11 recorder.

12 And so if you could capture that flow, that you
13 could also inspect encrypted traffic, because during that
14 flow are messages that you can use to determine if there's a
15 threat. And that's something that we were particularly proud
16 of at the time, because encryption was a huge problem for us
17 and for everyone else. And the fact that we had solved that
18 and recently filed for our patent on it, I felt comfortable
19 disclosing that in this presentation.

20 THE COURT: Had you obtained or just applied for a
21 patent on them?

22 THE WITNESS: We had filed for it, Your Honor.

23 THE COURT: What patent was that?

24 THE WITNESS: That was our encrypted traffic
25 inspection patent, which is our '856 patent, Your Honor.

—J. Rogers - Direct—

1 THE COURT: Okay.

2 BY MS. KOBIALKA:

3 Q. I'd like to turn to the next page.

4 MS. KOBIALKA: This ends in Bates number 19390, and
5 it's slide Page 8 of this presentation, and if we could
6 enlarge the figure here.

7 BY MS. KOBIALKA:

8 Q. I see on the bottom it says, "Patented system, live
9 update, and correlation technologies automate workflow.
10 Automate or die."

11 Do you see that?

12 A. I do.

13 Q. Why did you put that in the slide?

14 A. Because there were a couple other things that I needed to
15 amplify.

16 So on the previous slide, I had illustrated how
17 difficult the computational problem was for applying
18 intelligence, but then here I was illustrating the fact that
19 that intelligence changes all the time and that you also have
20 to be able to update that changing intelligence live, and
21 that you have to have the correlation technology to help you
22 with the determining which of those hits that you get from
23 intelligence are the most meaningful, and that if you didn't
24 also have these techniques, that you would have an
25 insurmountable technical problem.

—J. Rogers - Direct—

1 THE COURT: Well, all of those names on the upper
2 left side of that chart, whatever you call it, are they
3 sources of threat intelligence?

4 THE WITNESS: Yes, Your Honor. In our system we
5 have over 90 different threat intelligence companies that
6 deliver threat intelligence data. They all use different
7 formats. They all update on different intervals. And so
8 what this image is showing is the operational challenge of
9 taking all of that disparate threat information and
10 delivering that dynamically into actionable policies and
11 actionable intelligence.

12 THE COURT: These are just examples of your sources.

13 THE WITNESS: That's correct, Your Honor.

14 THE COURT: You had more sources out there; you just
15 used these as examples of your sources.

16 THE WITNESS: That's correct. These are just a
17 couple of leading names in this particular space, Your Honor.

18 BY MS. KOBIALKA:

19 Q. And I see there's a figure at the bottom, and it says
20 "RuleGATE," but there's a little box with a slash through it.
21 What does that represent?

22 A. That's an icon for the RuleGATE product.

23 Q. Okay. And so did you explain all of the things that you
24 just talked about to Cisco at the Webex meeting, with regard
25 to how the RuleGATE did this correlation technology and the

—J. Rogers - Direct—

1 live updates?

2 A. Yes, I did. I went through the bullets on the right and
3 commented on each of these features that we provide.

4 Q. And I'd like to go to the next page. This one is
5 entitled "Real Time Analytics," and it ends in Bates number
6 19391, and I see at the bottom again it says, "Patented
7 Technologies," and there's an asterisk.

8 Just briefly, what was the purpose of the slide?
9 What did you tell Cisco about it?

10 A. So we were about to give a demonstration which was, in
11 part, of the user interface that a threat operator would see.
12 And one of the principal problems that those individuals have
13 is, when you have an alert, knowing the severity of it.
14 Because you may not know whether it's somebody in the
15 cafeteria on their mobile phone or whether the internal
16 affected resource is your database that houses all of your
17 sensitive customer information. But one of the things that
18 you need to know to be able to determine that is the identity
19 of the internal host.

20 So I was amplifying some of the different
21 technologies that we have and the algorithmic techniques that
22 then inform what you see on this particular user interface.

23 Q. Now, after the Webex meeting, was there any follow-up
24 between Centripetal and Cisco?

25 A. Yes, there was follow-up on both the corporate

—J. Rogers - Direct—

1 development and investment front and then also further
2 technical follow-up with different Cisco employees.

3 MS. KOBIALKA: I'd like to mark PTX-102, and I don't
4 believe this one is in evidence yet, Your Honor.

5 THE COURT: PTX-102? It doesn't look familiar to
6 me.

7 PTX-102 will be admitted.

8 (Plaintiff's Exhibit PTX-102 was received in
9 evidence.)

10 BY MS. KOBIALKA:

11 Q. And if we can enlarge the top e-mail here.

12 Mr. Rogers, can you describe what this e-mail is
13 that you sent, it looks like, on February 5, 2016.

14 A. Yes. This is a follow-up meeting that I sent the day
15 after our briefing with the entire team to the Cisco
16 representatives that I was in contact with.

17 Q. And, for spelling purposes, are the e-mail recipients the
18 corporate development team, with some pretty lengthy last
19 names?

20 A. Yes. Peter Shih, Karthik, and Prasad.

21 Q. Now, looking at this e-mail, the second sentence says,
22 "The group seemed to hone in on our filter technology and
23 algorithms."

24 Why did you write that sentence in this e-mail to
25 the corporate development team after the Webex meeting?

Carol L. Naughton, Official Court Reporter

—J. Rogers - Direct—

1 THE COURT: I think I've seen that before.

2 MS. KOBIALKA: I'm sorry, Your Honor?

3 THE COURT: I said I think I've seen that particular
4 e-mail before. It looks familiar.

5 MS. KOBIALKA: I believe it came up with Dr. Cole
6 yesterday.

7 THE COURT: Okay. All right. Go ahead.

8 THE WITNESS: Could you please repeat the question?

9 BY MS. KOBIALKA:

10 Q. So the sentence, "The group seemed to hone in on our
11 filter technology and algorithms," why did you write that in
12 this e-mail to the corporate development team the day after
13 the Webex meeting?

14 A. Because after I had structured the presentation to talk
15 about the technology problems and then culminated into how we
16 uniquely solved that, that was where we got a number of
17 questions about the filter technology and about the
18 algorithms.

19 Q. And those are the ones that we looked at in the Webex
20 presentation that we just saw a minute ago?

21 A. That's correct.

22 Q. Okay. The next sentence says, "The algorithms are a
23 significant networking technology with broad application that
24 we've productized for security."

25 Why did you write that sentence?

—J. Rogers - Direct—

1 A. I wrote that sentence because there was a realization
2 from the group that what we were was a networking technology,
3 and it was recommended that a potential point of follow-up
4 would be with the routing and switching group.

5 Q. I don't understand. What do you mean "the routing and
6 switching group"? For what purpose?

7 A. Because our technology was relevant to our routing and
8 switching.

9 Q. Then the next sentence says, "There were also a few
10 questions on our patents, and if it would be helpful, I would
11 be happy to provide some materials or set up a discussion on
12 the filter technology and patents."

13 Explain. Why did you write that sentence?

14 A. We had gone through that discussion, and I had
15 highlighted the technologies that were patented. We had a
16 number of questions there, and I was offering to have
17 additional discussion on that, as well, if it would be
18 helpful.

19 THE COURT: Well, did I understand you to say that
20 this presentation was recorded?

21 THE WITNESS: Yes, Your Honor. When we entered the
22 presentation, we saw a sign in the Webex meeting that said,
23 "This session is being recorded by the host."

24 THE COURT: Well, was it recorded by audio or video
25 or both?

—J. Rogers - Direct—

1 THE WITNESS: I believe that would be both in Webex,
2 Your Honor.

3 THE COURT: Is that recording an exhibit in the
4 case?

5 MS. KOBIALKA: No, Your Honor, and we've never seen
6 the recording. It wasn't recorded by Centripetal.

7 THE COURT: So you've never seen that recording?

8 The witness should answer the question, rather than
9 the attorney.

10 You've never seen that recording, Mr. Rogers?

11 THE WITNESS: No, Your Honor. Apart from that
12 message that we saw when we came into the meeting that said
13 it was being recorded, we've never seen anything since.

14 THE COURT: Did you ask for it?

15 THE WITNESS: We did not, Your Honor.

16 THE COURT: Okay.

17 MS. KOBIALKA: Your Honor, it was requested in
18 litigation, but we don't have that. We never received it
19 from Cisco.

20 THE COURT: It was requested in the litigation?

21 MS. KOBIALKA: Yes.

22 MR. JAMESON: And, Your Honor, Cisco responded that
23 the recording does not exist, because it was not recorded.

24 MS. KOBIALKA: Should I continue on, or is this a --

25 THE COURT: Yes. So let's -- this is a good time, I

—J. Rogers - Direct—

1 think, to adjourn.

2 How much longer do you think you're going to be with
3 this witness, Counsel?

4 MS. KOBIALKA: 15 minutes, at most.

5 THE COURT: Well, we'll do that tomorrow. Who else
6 is going to be testifying tomorrow?

7 MS. KOBIALKA: Tomorrow we have Mr. Gibbs, who is a
8 sales representative of Centripetal.

9 Then we have Dr. Striegel, who relates to the past
10 damages.

11 Then Mr. Gunderson, who provides his opinion on past
12 damages.

13 And then Mr. Malackowski.

14 THE COURT: What is he going to testify on?

15 MS. KOBIALKA: His testimony is relating to the
16 future harm, so the damage to Centripetal and its patents.

17 THE COURT: Will he be your last witness?

18 MS. KOBIALKA: Yes, he would be.

19 THE COURT: Do you expect to get through all of them
20 tomorrow?

21 MS. KOBIALKA: If the crosses aren't too long, we
22 do.

23 MR. JAMESON: I love how you blame that on me,
24 Ms. Kobialka.

25 MS. KOBIALKA: I didn't.

1 THE COURT: Well, I don't think it's the crosses
2 which have been long, Counsel, it's been the directs. The
3 cross-examination hasn't been that long.

4 I said something about going to Maine. That
5 presupposes that this case will be over before the summer
6 ends.

7 All right. We'll be adjourned for today. I'll see
8 you tomorrow morning at 10:00.

9 (The proceedings recessed at 3:59 p.m.)

10
11 CERTIFICATION

12
13 I certify that the foregoing is a correct transcript
14 from the record of proceedings in the above-entitled matter.

15
16
17 _____/s/_____

18 Carol L. Naughton

19 May 18, 2020
20
21
22
23
24
25