FINAL TRANSCRIPT

Thomson StreetEvents℠

HPQ - Technology Series: HP Security Solutions

Event Date/Time: Apr. 12. 2011 / 4:30PM GMT

THOMSON REUTERS

CORPORATE PARTICIPANTS

Tom Reilly
Hewlett-Packard - VP, General Manager - HP Security Solutions

CONFERENCE CALL PARTICIPANTS

Abhey Lamba
ISI Group - Analyst

PRESENTATION

Operator

Good day, ladies and gentlemen, and welcome to the Hewlett-Packard Technology Series Webcast hosted by Internal Strategy and Investment Group. My name is Jeff, and I will be your conference moderator for today's call. At this time, all participants are in a listen only mode. Mr. Abhey Lamba of International Strategy and Investment Group will be facilitating a question and answer session after the presentation.

(Operator Instructions)

At the end of the webcast, there will be a brief three question survey. If you'd like to participate in the survey, you will need to take your popup blocker off. As a reminder, this conference is being recorded for replay purposes. I would now like to turn the presentation over to your host for today's call, Mr. Abhey Lamba of International Strategy and Investment Group. Mr. Lamba, please proceed.

Abhey Lamba - *ISI Group - Analyst*

Yes, thanks, Jeff. We are happy to host HP's second technology series event for 2011. In today's webcast we'll discuss HP's security business with Tom Reilly, Vice President and General Manager of HP Security Solutions. Tom served as the CEO of ArcSight until the acquisition of the Company by HP last year, and prior to becoming CEO, Tom served in several leadership positions at ArcSight, including President, Director, and Chief Operating Officer.

He was also the CEO of Trigo Technologies, a product information management software company, until he sold the company to IBM in 2004, and then he served as VP of Business Information Services of IBM for several years. Tom also holds a B.S. in mechanical engineering from UC-Berkeley.

We'll now have a brief presentation by Tom. After the presentation, we'll open it up for questions and answers. With that, let me turn it over to you, Tom.

Tom Reilly - *Hewlett-Packard - VP, General Manager - HP Security Solutions*

Thank you, Abhey. Before I dive into the presentation, let me take a minute on the forward looking statements. Some of the information provided during this call may include forward-looking statements that are subject to risk and uncertainties, and actual future results may vary materially. We won't be discussing new information on HP's financial performance during the current quarter or future periods.

Let me move forward to the presentation. What I hope to cover with you today is give you a sense of why the security market is a very exciting market right now, and It's going through some major changes, and why HP has entered into this market, and we think it's the right place for HP to be in. So, with that, let's get started. I'm trying to advance my slide, so just give me one

moment here. All right. So we have some folks working advancing the slide for us, but in the interim, let me start my discussion, and I apologize for the technical difficulties here.

So, the security market is going through a fundamental change right now, and we can tie that fundamental change to -- oh, our slide are up. Okay. So, let me talk about the market size first. The IT -- the traditional IT security market, sized here at $87 billion, overlaps with another market called the governance, risk and compliance infrastructure market at $72 billion. Combined, that is roughly $159 billion of market opportunity.

First, HP is not going after the complete market. We're very focused on a high growth area that we call security intelligence and risk management, which is an overlap of those two markets, and the technologies and service capabilities within that overlap size to about a $23 billion market, and this is the area we're focused on. We call it security intelligence and risk management, because we don't intend to do the traditional endpoint security controls, nor are we focused on a lot of the policy stuff in the GRC space.

Instead, we think there is a high growth area that is very differentiated for HP to leverage its current assets and its current capabilities to go after this security intelligence and risk management market, which is $23 billion, and we estimate growing at about a 12% CAGR.

Now, the security market has been around for a long time. Yet, all of us read every day, if not every -- well, every day we hear news about new breaches, new security threats online, and so, the problem hasn't been solved. And the traditional approach has been in place for 20 years, and we've been going down the same path, which is technologies that are focused on securing the infrastructure and creating hard perimeters around the infrastructure, security -- or, technologies that control access to applications in the service layer, and limit who gets access to those systems, and then, finally, technologies that kind of put controls around people and what they're able to do on the IT infrastructure.

And while these are great technologies in place, they're challenged, because the market is going through some major changes. What we've seen over the last 20 years is every time there's been a fundamental transition in how IT is delivered, from mainframe to client server to the web, and now, to cloud computing, every one of these transitions has introduced new threats. And so, what we're seeing, over the years, is threats aren't going away. They're actually increasing.

And as these threats are increasing, we have less and less visibility into what is happening on our networks. We're getting more information about what is happening on our systems, yet we have less ability to deal with that information and understand how we can use that information to protect our businesses.

Increasingly, we're hearing how major brands are getting impacted, and intellectual property is getting stolen, and identities are begin lost, and these thefts or cyber crimes are actually having greater impact, and we're less effective at responding. And we're seeing rising regulations and cost. And so, it's not uncommon to hear CIOs say that they are -- their agenda is being driven by compliance and auditors versus by business users, and we're seeing increasing regulations.

And why this is happening is that as we continue to innovate in IT, the latest innovation being cloud capabilities, we introduce new vectors for cyber attacks. Look at what just happened in the past week with the cyber attack on Epsilon, which we've lost hundreds of millions of email addresses that impacted many, many businesses. Well, it turns out Epsilon is a cloud based service, and when you have cloud based services with multitenant environments, there's -- the risk is so much greater, because a breach can affect hundreds of companies, as it did last week.

So, we believe the traditional security model is not adequate for the enterprise of the future. The traditional model was security products delivered by security suite vendors, basically, bolted on to IT infrastructure after the fact. These tools were designed at the network layer, then they moved to the OS layer of devices, then through the data layer to the applications to the users, and organizations are continually throwing point products at the problem, trying to lock down every part of the IT stack at each of these layers.

The problem is these tools are designed to protect technology. They work independent of one another. Your design goal is to achieve 100% security. You never know if you've reached there, and so, they're just not meeting the needs of the modern enterprise. If you look on the right, the modern enterprise is continuing to innovate, as we move to cloud computing, as we give employees more access to information, if we're -- as we virtualize these environments. And so, you have yet another hurdle for the security providers to try to innovate and catch up, and we think this is the wrong approach.

So this is where HP comes in. We believe it's time that security is built into the IT management systems. It's built into the IT infrastructure, and it's planned in from the get go. And we believe that the new leaders in security are going to come from the IT management vendors versus the security suite providers.

So let's talk about the four things that we're very focused on doing in this chart. First off, we need to take all those point security solutions that companies have deployed and unify them and bring the information from them into a common store. So now, they're working in unison, and we can look up and down the stack and understand where threats or vulnerabilities may lie. We need to combine what we're learning on this -- from the security tools with all the information we have from the IT systems.

So, in today's modern world, when you see a CPU's performance going down, and if you have an online business application, you see the server performance going down, it could be a very good thing, because you're having increased business, or it could be a very bad thing, because it's under attack. And so, we're integrating information from the IT side of the world with the security side of the world to get a more complete view of what is happening in the enterprise.

We roll this information up, and we can get what we call security and risk intelligence, clear understanding of who and what is on your network, what is it doing, vis a vis, its -- the intended purposes of that application, and now we can surface this. We surface this into the upper layer here, which we call our business risk dashboard, where we can reports and visibility into where your greatest vulnerabilities are, where your greatest risks are in the enterprise. So, HP's approach is very different from the traditional approach that security vendors have been taking.

Not to say that we intend to compete with traditional security players. What we're doing is we're augmenting the great products that companies like McAfee or Trend or Symantec have been delivering to market around endpoint security or creating firewalls. We're augmenting that, and we're basically providing the tools for our customers to have greater visibility into what is happening in their network.

We call that seeing. And we're showing them where the greatest vulnerabilities are, what activity is happening on that, where do they have the greatest exposure to compliance failures, and give them the tools to see that.

We are focusing on what we call -- the security intelligence really comes down to correlating and taking hundreds of millions, if not zillions of events in any one enterprise in a given day, and allowing them to process that information and understand where the greatest risks are and when they're occurring, and then we give them the tools to respond. And you're either going to respond to a specific threat, where you need a quarantine or isolate or remove some activity from the network, and you're responding proactively, where you're making investments to achieve compliance or minimize your risk.

So now let's talk about how we will deliver our solutions. We believe that in a hybrid world, security needs to be delivered in a hybrid fashion, and you need to look across your hybrid environment. So, traditionally, we secured layers of the stack, but where HP is focused is actually securing business processes may -- that may stand on premise technologies all the way out to cloud, virtual, and mobile environments.

And so, we have solutions that can be deployed on premise. We have solutions that can be deployed in the cloud and embedded in the cloud, and we actually -- they need to work together, so that, if you have a business process that goes across both your on premise and your cloud environment, you can look at that complete process and assign a risk or vulnerability, in order to understand what is happening to it.

And then, finally, we are delivering our capability with services as well. So we can offer it in a managed service capability, we can offer it in a SaaS environment, and we also offer on premise consulting services. So, HP is delivering the full spectrum of capabilities in delivering our solution.

To talk just a little bit more about the cloud, interestingly enough, if you look at what happened with Epsilon last week, we need to take a very different approach to how you secure the cloud. And it can't be just a contractor approach, where you work with a service provider and say, are you going to secure my environment, and they give you SLAs in a contract. We believe that the cloud requires transparency, so customers should have visibility into what is happening in their portion of a multitenant environment in the cloud.

With that transparency should come a compliance visibility, and so, if you're moving credit cards, employee information, health records, or financial data in the cloud, you need to achieve [SOCS], FFIEC, HIPAA, or PCI compliance. So we believe that needs to be built in.

We recently announced, with our TippingPoint team and VMware, the notion of secure virtual frameworks, so we're very excited about the early work we're doing in virtualized environments in the cloud. And then, finally, we need to offer, in the cloud services, the most advanced research of the latest attacks, because these cloud environments are securing the assets of many corporations.

I'll give you a sense of a couple scenarios, just to kind of talk about what is different about security intelligence from traditional security controls and why this is pretty exciting. Let's take a scenario where your business is an online business, and you sell tickets to events. And suddenly -- maybe you're selling tickets to a documentary, which is very controversial, and you come under a -- an attack, which is really what we call political activism. Someone is trying to bring your site down.

Well, how do you distinguish between legitimate users, who are coming to your site to buy tickets, and malicious users, who have this political agenda, and they're trying to bring your site down or void it. Well, this is where security intelligence comes in -- the ability to discern between those different types of users.

And it requires using our Fortify technology to understand the users' activity within the application itself, using TippingPoint's research to have what are known bad IP addresses, what types of code is out there that is malicious code, and then using ArcSight as the intelligence engine to look at the actual transactions and flag what can be malicious users, notifying our TippingPoint assets, and blocking that activity.

Another scenario that I find very exciting is in healthcare. So, in healthcare, there is tremendous opportunity in moving towards the electronic health record, or else, called electronic patient record. We know that EPR can take out significant costs out of the healthcare system and improve care. And a lot of our health information is going to be in the cloud, and it's going to move between your local health provider to a hospital.

That information moves from a hospital to a lab. That moves from the lab to the payers. Payers will share some of that information with corporations who pay a lot of the premiums, and so, we really have to take a close look at protecting health records. The challenge is you can't just lock out access to health records, because you could really impact someone's care. So how do you do it? You need a security intelligence solution.

So, in this example, let's say a hospital has a VIP in-house, and that VIP is Harry Callahan -- Dirty Harry, for you movie fans. One of my favorite guys. Well, he's in the hospital, and a pediatrician tries to access Dirty Harry's record in the cloud. Well, a security intelligence solution would say, well, something is out of context here. Why would a pediatrician be accessing an older person's record? However, we have to let him have access, because that pediatrician may be working on a relative of Dirty Harry's and needs to see some historical information. So our solution would allow access, but it would notify compliance.

Shortly thereafter, a payroll clerk attempts to access Dirty Harry's record while he's in the hospital. Now there are reasons, but this is of enough risk where we say no, let's block access, let's notify compliance and not give them access. This is the type of security solution that our customers want, which is, finding that gray area, and you can only do it with intelligence in understanding this.

So, let me talk about another area we're working on, and this is very exciting for customers, and this is notion of risk management compliance. I said earlier that traditionally, companies are -- their design goal is 100% security, and they try to lockdown every single vulnerability. Well, no company can ever achieve that. It's just -- the IT environment is too dynamic. So we're advocating, and we've been working on this for many months, now, with customers, a different approach, and we call it a risk management approach.

Instead of trying to achieve 100% security, realize that you can't do that, and rather, you want -- we'll give you the tools that allow you to understand where your greatest risks are, how you can improve your risk posture by making investments in those areas, and where -- what are the most critical business processes you should be securing and the most sensitivity you should be securing and what are less areas where you may want to take more risk, and this is what we're calling our business risk management platform.

Before I jump into some of the specifics, let me give you an analogy. In the IT world, every CIO knows that they have to commit SLAs to their end users, and they run these SLAs on dashboards, and so, they manage their business from a set of dashboards. And so, if it's [meantime] between failure, they know hard drives fail, and they have backups.

If it's application up time, they know applications eventually go down, and they have the processes and systems to recover them, but they report on the up time of their applications. They know that networks have to have quality of service, and so, they plan for peak times on their networks. And databases have to perform at transactions per second, and when they hit certain thresholds, they may have bursting capability in the cloud to address that, and this is how they run IT infrastructures.

There is no equivalent in the security world. In the security world, I always say, you code, and you hope. And we need to change that. And so, we believe security needs the equivalent of a SLA, but we call it a risk level agreement. And so, I apologize if these screen shots are small, but let me give you a sense of how this would work.

We believe that you need to look at your business processes and understand, for your most critical business processes, what kind of risk posture are you taking with them? And we can do that by mapping vulnerabilities to assets that support a business process and applying risk scores, and in this upper right, have a heat index that shows you which business processes may be at the most risk, then to allow you to drill down and understand why are those business processes at risk, and what investments can be made to improve them? And finally, to take a completely different view and say, and how am I achieving my goals for compliance, and where can I make improvements to achieve compliance better? And so, we call these risk level agreements, or risk dashboards.

Another way to look at it is, boy, wouldn't it be helpful if I could break my organization down from a user perspective and understand which users are introducing the most risk into my environment. And now, we start prioritizing our intelligence understanding around these users that are doing the most risky things, and that can be users that are downloading the largest files or users that are visiting competitive websites, users that are on performance plans -- employees that are on performance plans.

There's a number of ways to isolate who are the most risky individuals in our organization, and you can up level that to a department. What department or division is demonstrating activities that are introducing significant risk to the environment? And so, we're building out the dashboards and reports that allow you to hone in on the departments that introduce the most risk.

Well, what could be an example? Let's say one division does a very poor job of de-provisioning employees that have left the business. Well, how can that be a concern? Well, if you have a cloud based service that has your financial data in it, and you haven't de-provisioned an employee, and they go off to a competitor, and they can still access that cloud based system, you're introducing a risk. So these are areas that we're working on.

So, in summary, we believe that the market is looking for new approaches to addressing the security challenge. We hear it every day in the news that breaches are occurring, so it's apparent that the traditional tools are no longer adequate in and of themselves. So, the approach we're taking is to unify the security layer, to integrate security information with IT information, to bring that up into an intelligence platform that gives you real-time understanding, and then, to present that in a set of dashboards to customers.

And this really allows you to do three things. It allows you to see what is happening on your network and on your infrastructure and within your applications, to understand how that is impacting you, from a risk perspective, and then, to react accordingly. And you're either reacting in a response to an immediate threat, or you're acting very proactively to improve your posture going forward. These capabilities can only be done by an IT operations vendor who has that insight from the IT management systems on the right side of this chart.

This vision can be delivered by HP, and we do it by working with the traditional security vendors in improving this area -- this whole opportunity area. And we're doing this on tremendous assets. I'm very proud of what we achieved at ArcSight. I am very, very impressed with the teams here at TippingPoint and Fortify. Each of us is a leader in our core area, Fortify, at the application layer, TippingPoint, at the network layer, ArcSight, in the security intelligence area, and combined, we have, I think, a very competitive solution, some of the smartest folks in security working on this, and a great foundation to deliver on this vision and strategy.

So, I'll summarize this with why HP has really focused on getting into the security space. Our vision is for everybody on. HP is focused on delivering a seamless, secure, and context aware experience for a connected world. That means we believe in cloud and the hybrid environments. We believe in the consumerization of IT, where more people are going to expect broader access to information to get their jobs done.

We believe in more devices getting connected in the world, and we realize that the one thing that could slow that opportunity down is concerns around data privacy and security, and that's why we're in the business. We're going to tackle it head-on, and we're going to focus on the areas that enable that feature for everybody on. And that concludes our presentation. I think we're going to move to Q&A now.

Abhey Lamba - *ISI Group - Analyst*

Yes, thanks, Tom. That was a quite helpful presentation. Before we actually -- I've got a couple of follow-ups. Before we go into that, Jeff, could you please give the instructions again on how to queue up a question?

QUESTIONS AND ANSWERS

Operator

Absolutely. (Operator Instructions)

Abhey Lamba - *ISI Group - Analyst*

I think we are also taking questions through the webcast. There's a link, question and answer, right above the presentation in the webcast. So if you want, you can click on that link and submit a question.

Before we poll for questions, Tom, I just want to follow up on a few things you mentioned on the -- during the presentation.

Tom Reilly - *Hewlett-Packard - VP, General Manager - HP Security Solutions*

Sure, Abhey.

Abhey Lamba - *ISI Group - Analyst*

You highlighted the security intelligence and risk management of the focus area of the $23 billion opportunity and a CAGR of 12%. Can you give some granularity on that? What constitutes that $23 billion of opportunity? What are the areas where you have products, and what are the areas you're building out?

Tom Reilly - *Hewlett-Packard - VP, General Manager - HP Security Solutions*

Yes. Abhey, I think it's a very important question for us to dive down a bit into. First off, the security market is a very large market, and a good portion of it is well served today. And so, I think one of the most important decisions we made is what should we not go after versus what are we focused on, and this allows us to partner effectively with, I think, some of the key players, whether it's Symantec and McAfee, and complement their solutions where there are significant opportunities.

So that category is what we call security intelligence and risk management. What's in there? There's a subcategory called security and vulnerability management, where you're getting better vulnerability information about all the assets that are on an IT infrastructure, from the network right up through applications users, the data layer.

There's a lot of tools in network security, in network forensics. There's portions of the identity and access management -- not the traditional identity and access management market, but portions of that where you're having better insight into what users' roles are, what they're entitled to do, and the ability to monitor, vis a vis, those roles and entitlements.

There are areas in data security and secure content, where it's all about intelligence and where that data is, where is it going. Those are areas we believe we should be playing in. And then, there's the area of risk and reporting on risk and better management tools to reduce your risk and effectively invest.

So those are kind of the areas that HP is very focused on. If you look at each of these areas, they tend to be the high growth areas within security. They tend to be the higher price point, I think, higher value innovative type solutions, and they're areas where we know that we can leverage our leadership in IT management solutions to offer us differentiating capabilities as we move into these spaces.

Abhey Lamba - *ISI Group - Analyst*

Got it. Now that's helpful. So, I can see how Fortify and ArcSight fit into this strategy. Can you talk about the strategic advantage that TippingPoint provides with this strategy, and are there any cross selling opportunities that are clear to you?

Tom Reilly - *Hewlett-Packard - VP, General Manager - HP Security Solutions*

Tremendous. This strategy was built -- so, first off, the strategy we've presented here is a cross HP strategy, built with the folks at TippingPoint, Fortify, within our services organization, even with our PSG, IPG teams. So, security is a cross initiative at HP.

Specific to TippingPoint, tremendous technology and essential to our strategy. TippingPoint not only gives us great visibility into what is happening at the network layer and what is transpiring across it, but they give us filtering capabilities to block access when we have known vulnerabilities. The TippingPoint research team is best in class, and already, we're seeing great synergies of leveraging that research into the ArcSight platform and the Fortify platforms.

I showed you those two scenarios, which specifically require each of the assets we have, Fortify, ArcSight, and TippingPoint, to resolve, and we're building these integrations out. So, this is where -- we talk about this as a platform approach, where it's not just a standalone security process that we're investing in. We're investing in a platform that helps customers to solve these very complex problems, and TippingPoint is a key part of that.

Abhey Lamba - *ISI Group - Analyst*

Got it. Now, before I go further, Jeff, are there any questions lined up? Anything on the web, Katrina?

Unidentified Company Representative

We do have a question on the web. The mobile market is high growth, but there's no security vendor that has really figured out how to monetize things like Smartphones, the iPhone, or even HP's TouchPad. So, what is your view? And also, how do you position in network security, and what kind of apps do you need to go after and build out that space?

Tom Reilly - *Hewlett-Packard - VP, General Manager - HP Security Solutions*

Okay. So, the question on mobile market. One of our fundamental beliefs at HP is centered around the mobile market, and we'll go even further than just mobile devices. We believe that corporations are going to see an increasing number of devices being brought onto their networks by their employees, and whether that is tablets, that is phones, it's PDAs, it's special laptops.

Increasingly, we're seeing employees of corporations have a preferred device that they want to get their job done with, and the reason is because they have to work around the clock, seven days a week, 24 hours a day. So they pick these devices that are basically attached to them all the time.

Now that introduces a lot of security challenges, and again, why HP is getting into this market. Obviously, we make and sell a lot of those endpoint devices, and we want to make and sell more of them, and so, we need to take on the security challenges of how do you do that. It's probably a pretty complex area to discuss on this call, but essentially, you need to have better understanding of who is behind these devices. Based on who they are, what are they entitled to see, and then, to give them that access, but also have the ability to monitor and respond, because these devices do introduce a lot of new security threats.

So this is one of the areas that we are actually working on with our POM organization and the PSG group, understanding how we can have better insight into these devices, as they come on networks, and to basically profile them and to help secure them. Now, there are a bunch of other companies that are building endpoint technology to go on those devices and help lock them down, and that is where we'll continue to partner with those types of folks.

Abhey Lamba - *ISI Group - Analyst*

Tom, it's kind of related to this one. You also mentioned in one of your slides that -- how the security model is broken, and on the left side, you had different stacks and how they were kind of -- they're being secured today. Can you elaborate further on the -- on this, and talk about how these solutions are changing, which solutions that exist today could become redundant, and what are the newly emerging technologies? A couple examples would be helpful.

Tom Reilly - *Hewlett-Packard - VP, General Manager - HP Security Solutions*

Yes, as I was presenting that slide, I thought I should have changed the title. I shouldn't -- the traditional security is not broken. It's just -- it's not adequate to secure the modern enterprise. I think all the investments that customers have made, whether it's in firewalls, it's in endpoint scanning, it's in encryption -- all those technologies are necessary. They're just no longer adequate to solve the challenge. If they were adequate, we wouldn't be reading about all these breaches that are continually occurring.

So, what we intend to do is to take the information that those devices and those technologies are generating, and they generate huge amounts of information -- to take that information, bring it into a central location, and use it for better intelligence around what is happening. And there will continually be new endpoint technologies. To the last question, around this whole mobile market, there's new products going onto these mobile endpoint devices, which we have to gather data from.

Now, this is not like futures we're talking about here. This is the business that ArcSight has been in for ten years. It's been unifying those security products into a common platform and a common dashboard to relate all those events and get broader information. What we're doing now, unique within HP, is taking that security world on the left and tying it to the IT operations world on the right. And why that is important is because of the move towards hybrid environments, where you're using cloud technology and virtualization, you need the context from the IT management merged with the security world, and so, that's the gap we're filling here. This is all technology that is emerging, is in place, and a bunch of new stuff that we're still developing.

And then, finally, I think part of that question was around the network layer. We actually think we have great assets at the network layer with TippingPoint. TippingPoint gives us great visibility into the network, has great intelligence of what is happening in the network, the ability to block malicious traffic. You couple that with a tremendous research team that we have there and the Zero Day Initiative that TippingPoint has, our research organization, coupled with Zero Day Initiative, discovered the vast amount of vulnerabilities, more so, than any other vendors out there. And so, this is a scenario of great strength that we have.

Abhey Lamba - *ISI Group - Analyst*

Speaking of network layer, Tom, I -- now, TippingPoint clearly helped (inaudible) intervention, but there are other aspects of network security. Do you think you're going to treat them just like endpoint security, for example, UTMs or firewalls and VPM stuff, or is that an area where you can get more intelligence on network security and can help you with your security intelligence market?

Tom Reilly - *Hewlett-Packard - VP, General Manager - HP Security Solutions*

Well, I think there's opportunities for us there. The firewall market is going through a -- kind of a major refresh, and we think that there's some opportunities for new ways to look at solving that problem. There is activity at the application layer, at the data layer, so a lot of this is merging together. I don't think we'll get into the traditional markets, but there are some new areas that we are focused on offering capabilities.

Abhey Lamba - *ISI Group - Analyst*

Got it. Jeff or Katrina, do you have any other questions before I keep going?

Unidentified Company Representative

We do have another question from the web. Can you tell us a little bit about your go to market solutions? What is your relationship with channel partners, and how will you leverage channel partners in delivering the solution?

Tom Reilly - *Hewlett-Packard - VP, General Manager - HP Security Solutions*

Okay. And, Katrina, maybe I'll broaden that question from the web just a bit. Channel partners are very important, but even more importantly is service partners. As you take this new risk approach to securing an enterprise, as companies want to take advantage of cloud computing and giving users broader access to more information with a broader set of device types, services play the very key role in solving this for customers.

They need to take a risk based approach. They need to have better tools, better management, better policies internally. They need to have resources that understand, kind of, the risk introduced by this modern world, and this is where we're very excited about partnering with, first off, HP services arm, but also, those of our partners, whether it's the large integrators or security specialist firms across the globe.

So, ArcSight, TippingPoint, Fortify -- we all come to HP with our traditional partners we've had. We're leveraging HP's PartnerONE program, which gives us broader access to HP's partner community, many of which have great skills around the IT management tools, and now, an area that we really hope to leverage. So, our plan is to continue investing in the channel, and that is VARS and resellers, to continue investing in the system's integrators, who are building practices in this space, and to work with HP's own services arm in building out capabilities here.

Abhey Lamba - *ISI Group - Analyst*

Good. Now, actually, on one of the slides, Tom, you had mentioned about being number one in security visibility and management and integration with leading IT management solutions. Now, are you referring to your systems management tools -- integration of systems management tools, like [Opsware, of] their products? And do you have a single console to which we can manage security and systems management?

Tom Reilly - *Hewlett-Packard - VP, General Manager - HP Security Solutions*

Okay. Big yes, Abhey. So, first off, I do believe that addressing this area, what we call security intelligent risk management, is going to be an area that you have to be an IT management or IT operations vendor to deliver this capability. This is why we're very excited to be part of HP, and I would say that's across ArcSight, Fortify, TippingPoint, as we look at where the security market is going.

HP is a leader in operations management, application life cycle management, great assets in information management, and all of this are capabilities that we need to leverage, both from a technology standpoint, but also from a go to market capability. And so, our reach, just through our software assets and understanding of IT operations, is tremendous.

And so, I think, yes, one of the advantages HP has is our presence in IT operations, and that gives us a great entree into talking to CIOs about their opportunity in the future to take advantage of cloud and cloud activity, but how that introduces new security challenges and how we're building security into these new systems.

Abhey Lamba - *ISI Group - Analyst*

Now, are your products kind of well integrated to work with each other, or are these separate products that companies have to use?

Tom Reilly - *Hewlett-Packard - VP, General Manager - HP Security Solutions*

Well, let me take that in two parts, Abhey. Our security products -- so, our security portfolio can be purchased as standalone products. Each one is kind of best in breed solution that addresses specific parts of the challenge, but we are making investments of integrating these offerings into a platform, where, if you start building them up and adding the capabilities together, you get exponential value.

So, our teams have already done a number of integrations. In fact, that first scenario -- actually, both those scenarios that I showed slide on? We actually demonstrated those back in February at the RSA conference, so those scenarios are well integrated. So we're integrating the security products.

Likewise, we are integrating our security products with our IT operations capabilities. So what would be one example? HP has one of the market leading configuration management databases, where all of your assets on an IT network are maintained in database in how they should be configured. We're -- we've built the integration between that and our intelligence platform, so that we can understand all those configurations and assets and map them to business processes. So we're building that out.

We've delivered universal log management, which is the ability to collect logs from IT operations and security events into a common platform. So there's a lot of integration occurring there as well, and these are the types of capabilities our customers are leading us towards.

Abhey Lamba - *ISI Group - Analyst*

Great. Thank you. Katrina, do you have any other questions on the web?

Unidentified Company Representative

Yes, Abhey, we do have another question from the web. How is HP addressing cloud security, and how is the cloud security that you're offering tied to the rest of HP's cloud strategy as you -- as it was announced a month ago?

Tom Reilly - *Hewlett-Packard - VP, General Manager - HP Security Solutions*

All right. So, these are very, very related, and I would say if there's one reason why HP has decided against the security business, it's because HP knows it needs to be a leader in cloud capabilities. And so, this is where security is a cross Company initiative for us, and we're investing from on premise all the way out to the cloud.

There's a lot of things that need to be done in securing the cloud, and rather than going through the whole laundry list of what that means, maybe I'll just share what I think are the differentiating things that we think will help cloud adoption accelerate. So, first off, I think, rather than security being an inhibitor of cloud adoption, or a concern, we can turn into an advantage, and let me give you an example.

Let's say you're a healthcare provider, and you have -- you're adopting electronic medical records system. Well, once you adopt that electronic medical records system, and you put it onsite, on your premise, you have to be HIPAA compliant. And so, now you have to have the resources, the skills to manage that compliance mandate. You have to satisfy auditors. But what if a vendor

came along and said, let us manage that for you in the cloud. We will help you achieve your compliance, and, by the way, we can spend much more on securing this infrastructure than you ever could, Mr. Healthcare Provider -- that you don't really have the resources.

But to do that, you have to give them complete transparency, so the first thing we want to do is have transparency in the cloud. You need to operate the cloud towards compliant standards, whether it's PCI for credit card data, HIPAA for healthcare records, SOCS for financial information or customer data.

So you need to operate it in a compliant way. You need to have the most advanced awareness of vulnerabilities in the cloud and offer what we call system assurance to understand those vulnerabilities. And also, we believe that we can apply tremendous research -- leveraging our research teams of the latest threats and use that to help secure the cloud. So these are some of the areas that we think can be differentiating for HP, in addition to all the traditional things you need to do in securing cloud, whether it's both private or public.

Abhey Lamba - *ISI Group - Analyst*

Just following up on that, Tom, I think, in one of your slides, you also showed different stacks and kind of talked about how different layers will kind of have security information that your intelligence systems are going to extract and work off of. Are all the endpoint security systems evolved to a point where they can handle the evolving kind of security landscape, because of adoption of cloud, or are there endpoint solutions that are still in the works, which would help you have better solutions on the management side?

Tom Reilly - *Hewlett-Packard - VP, General Manager - HP Security Solutions*

Well, Abhey, we believe that there are a lot of endpoint solutions today, and there will be a lot of new endpoint solutions in the future, and we'll -- as endpoints change themselves, and we're seeing one major change right now in the whole virtualization and, of course, all these device types, and it seems like, gosh, what else could we innovate? Well, trust us, in five years, ten years, there will be new things, and there will be new endpoint devices.

The point that we -- the area that we, HP, needs to anticipate is every one of these endpoint security devices, whether it's on a server, it's on a mobile device, it's on a laptop, it's tapping into a database, it's looking at an application, they generate tremendous amounts of information. And this -- we call this machine generated data, right? What's transpiring? And that information is exploding, and so, what we're focused on is the ability to get intelligence out of that information and apply it to a security view or a risk perspective.

And so, I think we'll continue to see new endpoint technologies. These new endpoint technologies will be standalone, looking at that specific device or component on an IT infrastructure, and that is technology that we need to continually tap into.

Abhey Lamba - *ISI Group - Analyst*

Got it. Katrina, do we have any more?

Unidentified Company Representative

Yes. Yes, Abhey, there's another question, kind of specific to the markets that we're targeting. Are the solutions -- are you focusing more on large enterprise customers, or will there be any focus or opportunity with SMB? And then, also, how will you work with other vendors' platforms in providing your solutions?

Tom Reilly - *Hewlett-Packard - VP, General Manager - HP Security Solutions*

Okay. So, cyber criminals do not distinguish between size of corporations. They don't distinguish between -- there's no boundaries in cyber crime, and that's one of the challenges. However, our belief is that the solutions we're focused on delivering today, we're primarily targeting the large enterprises. We think that these are the companies making the greatest investments in security technologies. They understand the security intelligence and risk management value proposition.

The key verticals for that, we believe, are -- the public sector is a very large investor in cyber security and mostly focused on cyber war activity and protecting classified data and communications, financial services, healthcare, telecommunications, and critical infrastructure providers. That's where we're focusing all of our effort.

However, as we continually see, the market will expand from enterprise to large midmarket companies and, eventually, move into smaller organizations, as the skill sets and the awareness of the capabilities grows. But I would say our focus is on the traditional large enterprises.

Abhey Lamba - *ISI Group - Analyst*

Any more, Katrina?

Unidentified Company Representative

That was the last question from the web.

Abhey Lamba - *ISI Group - Analyst*

Okay. I have one last question before we can close it down, Tom.

Tom Reilly - *Hewlett-Packard - VP, General Manager - HP Security Solutions*

Okay.

Abhey Lamba - *ISI Group - Analyst*

Now, (inaudible) recently identified software as the largest delivery method for security solutions. Do you share that viewpoint, or is there going to be more (inaudible) for security hardware solutions, or do you think this is going to go the more for software route?

Tom Reilly - *Hewlett-Packard - VP, General Manager - HP Security Solutions*

Abhey, well, I'm a software guy, so I think I'll (inaudible) with you on that. But I think HP has come to the realization, also, that software is a -- is the primary technology vehicle to solve a lot of problems and especially in the security space. This whole approach around security intelligence management is a major software play, up and down the stack, leveraging a lot of our software for assets.

That said, we do believe that endpoint devices should continually have security embedded into them and built into them. Even if you look at our strategy for cloud, we don't expect security to be added on to the cloud. It needs to be built in as our cloud services are being put out there. So what you're going to see is HP is going to be investing heavily in software solutions, but

also, embedding into a lot of our platforms and our products a native security, then, just kind of elevates the overall security of the ecosystem, as those devices get interconnected, and it gives us better intelligence.

Customers like to buy security solutions prepackaged on hardware, and we call that appliances. But whether it's TippingPoint, ArcSight, or even Fortify, most of our customers are buying our solutions prepackaged on appliances, which happen to be HP appliances we're delivering on, and that seems to be their preferred buying mode.

Abhey Lamba - *ISI Group - Analyst*

Good. Thanks. Do you have any final comments, Tom?

Tom Reilly - *Hewlett-Packard - VP, General Manager - HP Security Solutions*

Yes, Abhey. Well, first off, thank you for the tremendous questions. Thanks to the folks on the phone for all your questions and giving me the opportunity to address you.

It's interesting. I think the security market is a tremendous place right now, and although it's been in the works for 20 years, it is actually getting really exciting now, because of the great transformation that is happening in the broader IT landscape. And it's introducing new threats. The awareness of cyber crime in cyber security is higher than ever. Customers are looking for vendors like HP to enter into this market.

I'm now part of a great team. HP is either -- depending on how you add up the numbers, either the fourth or fifth largest security player, but I believe we're the fastest growing, and number one, number two, and number three, we don't view as competitors. We view as good partnering opportunities, that being Symantec, McAfee, and Trend. So this is just a very exciting place, and I think it's a tremendous opportunity, not only because security is a big market, but because this is tied to our broader initiatives of cloud and what we intend to do there in connectivity.

So, I thank everyone for giving me the time to address you, and thanks for your great questions, and I hope to have the opportunity in the future. Thank you.

Abhey Lamba - *ISI Group - Analyst*

Good. Thank you for your time, Tom.

Operator

Ladies and gentlemen, this concludes our call for today. Thank you, and have a wonderful day.