Migrate to New Enterprise Security Solutions the Right Way

Wed, Oct 12, 2022 6:47PM • 45:47

SUMMARY KEYWORDS
solution, data, technology, security, organization, deploying, rfp, guardian, data loss prevention, cybersecurity, ultimately, tim, vendors, run, managed services, migration, important, problem, critical, environment

00:00
Hello and welcome, everyone to today's webinar. I'm Charles Maddox and with the eye for group, and we're here to give you a webinar on cybersecurity data loss prevention. And I have our partner on the on the call with us today Digital Guardian. And they're going to give you an excellent overview of some of the DLP solutions that they have and, and also give some best practices on how to apply these in your in your organization. Again, my name is Charles Maddox with the eye for group. We are an enterprise transformation Consulting Group digital transformation, and we specialize in an agile project management skills program, Scaled Agile Framework. And also too, we offer some cybersecurity product solutions in DedSec ops solutions for our clients. And at this moment, I'll turn it over to Tim bando to introduce himself, Tim.

00:56
Great, thanks, I appreciate that trust. How's everyone doing today? So yeah, today, we're gonna talk a little bit about migrating to new enterprise security solutions, not necessarily a specific focus quite on DLP. But that could be a part of your enterprise stack, really, we want to do is kind of keep it general and talk about some of the best practices as you look at the new solutions in the market. But just real quick, a little bit about myself. So I am the seaso for Digital Guardian, I run our risk management compliance program and do all the internal security monitoring and response. But I also run our managed security services. So that includes managed detection and response data loss prevention, I help architect architect our EDR capabilities and do some sales enablement. But I'm happy to be on the call today. And you know, happy to look forward to meeting all of you guys, you have any questions, please let us know at the end of the call. I also like to introduce Alex who's on the call as well. He's with Digital Guardian. Alex, you want to introduce yourself?

01:48
Sure. Alex communities, I'm the subject matter expert in your trusted advisor when it comes to anything when it comes to data protection, responsible for sales development, Digital Guardian. And if you have any questions after this, or in the future, feel free to reach out to me, you receive my contact information. And let's just move forward and get Tim to educate us a little further.

02:17
Sounds good. Thanks, Alex. So what are we gonna talk about today? So difficulties with migrating to new security solutions, I think we all kind of run into this, whenever we're ready to make that decision of, you know, taking on, you know, a new solution for our environment, you know, reasons to replace technology that we currently have, maybe talk about steps that we take before we engage with vendors, you know, developing an effective RFP like a request for proposal document, how you go about doing project planning and drafting and issuing an RFP. We'll talk a little bit about migration planning. And then I like to always round off my my presentations with some tips from Tim. Alright, so couple quick stats, right, just one in 10 organizations say their current security solutions fully meet their needs. And a lot of times you kind of ask yourself, why is that? You know, did the vendor oversell the capabilities of that security solution? Does it not meet the current needs, because something happened over time where it no longer, you know, meets those objectives. A lot of changes happen over the years, right, as we've deployed security technology and solutions and, you know, really, ultimately could stem from Why not everyone is happy with, you know, the the stack that they've deployed, you know, nearly nine out of 10 companies don't have sufficient budget also to implement a totally effective cybersecurity solution. I used to work for, you know, large fortune 500 company, and even a budget for cybersecurity in an organization like that was around 1%, right of our overall IT spend, right? So you know, allocating enough budget for cybersecurity is absolutely critical. It really helps deploy, you know, the necessary technology and controls that you need in place to ultimately defend your network. A couple other ones, right 20% of IT managers who are victim to one or more cyber attacks, they can't really pinpoint how the attackers got into the environment. And this is why visibility is absolutely critical. You know, when you are deploying technology, you want to make sure that you have visibility across all of your systems, your entire network so that if a breach does occur, you're able to, you know, pinpoint what is the root cause or the initial entrance vector of that particular attack. And then finally, organizations that are spending 85% of the time investigating 99 issues, that's equivalent to around 41 days each year. So there's a lot of time being spent investigating things because they don't have that necessary visibility to ultimately answer the questions that they're looking to answer. So, a few difficulties that I've seen over the years, right with migrating to new security solutions. I think there is a huge lack of trust in the industry. And a lot of times that kind of stems back to maybe marketing departments or even some of the sales guys right where you have these buzzword bingo claims of these security solutions, be able to solve all of your problems. And that's just simply not always going to be the case. I think It's really important to when you're evaluating security solutions and technologies that you understand what is the exact capabilities that it will provide? And what are the outcomes, the solutions and the use cases that you'll be able to solve specifically with that technology? I think we also always look at our technology stack and say, how do we exhaust you know, what we have currently within the environment, right? Exhaust the old before we bring in the new, right, we've already invested in our technology we've already deployed, you know, the solution, is there any additional capabilities or functionality that we can get out of that solution without having to actually rip and replace? There's also a skill shortage we hear about this all the time, you know, I think in cybersecurity, finding talented resources is very difficult, right at times. So, you know, having that shortage and talent gap, you know, can be a problem, right? When it comes to deploying new technology and people to run that technology. I think there's some cultural divides that we run into. And then, you know, less than that, you know, but not least, of course, as I mentioned earlier, as budget, you know, do you have the necessary budgets to deploy this, you know, new security solution, because they're expensive, you

know, cybersecurity can be expensive, because you're ultimately trying to protect, you know, your environment, right, you're trying to protect your domain, and you want to make sure that you have all of those holes covered.

06:15

So why you may need to consider a new solution, right? Maybe your current solutions are underperforming. And over time, maybe your business model evolves, we also see new attack vectors that are commonly you know, coming up, you know, for example, state sponsored espionage attacks, right, there's all these different vectors of how they're breaching and getting into environments, a lot of times, it might just stem back to someone clicking on a link or an attachment. But these vectors are growing, right, the vulnerability landscape continues to grow, too, in a lot of these solutions that we have deployed, we've seen that through a lot of different technologies throughout the year where they've recently, you know, recently released bulletins around, you know, major bugs or exploits that are out in the wild, right, so we have to stay on top of those. Also, there's more secure solutions that are available today. Right, as time goes on, the more secure some of these solutions do become, you know, maybe you see a lack of support in your current capabilities, either from the vendor or, you know, lack of being able to support yourself, you know, lack of mobility, lack of insight and information. So there's a lot of different reasons why you might want to consider, you know, migrating to a new security technology. Jack Welch once said, If the rate of change on the outside exceeds the rate of change on the inside the end is near. And I think that's really relevant to what we're talking about today. Right? Because if you're not keeping pace with, you know, the threats on the outside, and you're not keeping pace and understanding what your threat landscape is, you're gonna have problems internally and a breach is ultimately inevitable. Right, so what are a couple of steps you might want to take before you engage the vendors, you know, you want to define the problem that you're trying to solve, right. And the criteria associated with that, you want to set milestones you want to create cross functional project teams, you want to take this serious, you don't want to just, you know, actively reach out to a vendor, have a couple of questions, and just hope that you're going to solve all these problems, you really want to be well defined in the exact use cases that you're looking to solve otherwise, you know, the vendor might not be able to really help you ultimately, I mean, vendors, a lot of times will tell you, they'll be able to solve 100% of your problems, but you want to have those exact use cases in mind. So that, you know, you know, specifically what you're looking to solve. You also want to seek industry guidance, maybe from from other, you know, peers in the in the industry, right, people who already already have the technique, maybe technology deployed, who have experience with the technology that you're interested in any recommendations or pitfalls that they might have, you know, come across during their deployment, that could save you a ton of time and headaches and heartaches, right, because ultimately, you don't want to get in bed with, you know, a vendor that ultimately doesn't perform with the security capabilities that you're looking for, you know, internally, I think creating a scoring system really helps you know, making a shortlist of vendors is also a really good idea. You don't want to have a list of 10 vendors that you're interested in, you want to really zero down to two to three top vendors for whatever technology that you're looking at. And then ultimately develop an RFP a request for proposal document that you send out to these vendors that you can cross compare, you know, each of those vendors capabilities. So what are the benefits of an RFP? I think they're pretty straightforward, right? I mean, it helps, organizationally, needs and forces you to define what your requirements are, right allows you to kind of cross compare, as I mentioned earlier, right and gets control of product demonstrations. It gets to think about what is your ROI, your return on investment, and ultimately produces an organized selection methodology. You really need to be organized when you are actively seeking out a technology so you understand exactly what you're getting into. So this is what the RFP strategy process looks like. Right? You're gonna go through a project planning phase, you're going to draft an RFP, you're going to issue that RFP, and then you're going to review the proposals and ultimately award the contract. You know, this this quote I don't know who actually said this, but it also seems pretty relevant. You know, software selection is like painting a building, right? The real work is in the preparation, and not the selection. And that's, that's important, right? So you want to be prepared upfront, before you go about and select the technology.

10:15
So in the project planning phase, you know, as you're going about, you really want to outline the scope of your requirements, right? What are you looking to solve, and you want to align that to business strategy, you want to make sure that you have a seat at the table with the executives. And you know, from a business perspective, you're looking to help also solve some of those problems, and really relay, you know, kind of that notion to upper management, that these security solutions will also help protect, you know, where the business is going from a strategic perspective, right, you want to make sure that you have a budget set, right, you have a timeline that's in place, and then the stakeholders are all there and they've reviewed, and they're on the same page, you know, once again, having that scoring criteria can be very critical, right, and ultimately determining what solution you want to go with, because then you can kind of cross compare and look at each solution, you know, together side by side, from a scoring perspective. You know, drafting the RFP, there's a lot of, you know, great templates that are already out there on the internet, if you've been, you know, researcher search, you know, it RFP templates, right, they're gonna have a lot of the stuff kind of predefined for you, which helps you get off the ground, you don't have to necessarily start from scratch, right, but, but having an RFP with an introduction, kind of a statement of purpose, you know, some background information in the scope of work you're looking to solve, that can really help, right with this overall process, you know, having a project manager that can develop the schedule of the project that you're working on, being able to come up with contract terms and conditions, and, you know, ultimately having a requirements for proposal really should all be a part of that that RFP, drafting phase, then you want to issue the RFP you want to send it out, you know, to those vendors, you know, we receive RFPs, all the time, I mean, weekly, almost daily. So these are things that we're used to receiving, you know, it could be a list of, you know, 20 questions, it could be a list of 100 questions in those RFPs, we make sure that we've outlined, you know, everything, you know, that that our capability is able to perform in terms of, you know, the functionality that you're looking for, and the use cases that you're looking to solve RFPs are absolutely great, right for kind of answering a lot of those questions that you might have. And then you want to review, write the proposals and award the contract, you know, once you go through that scoring exercise of, you know, looking at how the RFPs came back, and you know, what you're ultimately going to select, I think it's really important to, you know, to wait those decisions, right. And then ultimately getting numbers to on the cost of the security solution that you're you're looking to deploy that's, that's, that's another critical part, I've gone through a process where we've looked at three or four technologies, we kind of came down to, you know, the top two or three, and the one that I loved the most, of course, ended up being literally the most expensive, right? So you want to avoid kind of getting that sticker shock as well, you know, at the end, you know, getting those numbers upfront can be really

important, too, right? Because if you can't afford the solution upfront, I mean, don't even waste your time. I mean, yes, you can negotiate price, but also there's gonna be vendors, you know, in this industry that, you know, unfortunately, you're just not gonna be able to afford. Right. So that's another, you know, recommendation of mine is just making sure that you understand, ultimately, what is the cost, the total cost of ownership, what's the cost to deploy it? What's the cost of, you know, just running the solution? What's the cost of staffing? You know, is it something that you need to consider as a managed service? Do you have internal staff that can run it? Is there infrastructure that needs to be added, you know, internally within your organization? Or is it something that's all cloud based, right, all of these once again, are, you know, different questions and things that can be addressed in that RFP as a part of that process. So that's what that that that RFP strategy process looks like, right? You have the project planning, issuing, drafting the RFP issuing and then also reviewing the proposals, this is just kind of a summary of, you know, what that looks like in a in a single slide.

14:15

And then the, the real fun comes, right. And that kind of comes down to migration planning. You know, once you've gotten through, you know, the RFPs, you've selected, you know, the technology solution that you're looking to deploy. Now comes the plan, build run phase, right. And this is almost just as critical as even purchasing the technology because the last thing you want to do, right is select a solution and it takes a year, two years, even deploy that solution, because now your return on investment is out in the future, right? You're not receiving any return on that particular investment. And that's not going to make people at the top very happy so. So really, as you kind of go through this process, you have to break this down as well as you're migrating, you know, the old solution into the new solution. And that plan comes down with Having a strategy, right having an assessment or profiling, you know, prioritizing, you know, if you're doing data loss prevention, you want to have data requirements and classification requirements for how you wanted to find the data within your organization. You know, business logic and infrastructure dependencies, all that needs to be considered in that strategy phase of the plan, build run phase, right? You want to do an analysis, right, having a detailed migration plan in place an estimation of effort and time that's going to take place, and then you know, what's also really important is having a security and risk assessment conducted by, you know, by the CISOs organization, right. So, you know, security analysts or the seaso, for your company, you know, making sure that they evaluate what is the risk associated with taking out that old technology and putting in the new technology? Does that open up additional holes that maybe you weren't aware of, you know, are there gaps that are going to occur when you do replace that technology, because functionality has changed, you know, doing that security and risk assessment impact can save you, again, a lot of headaches later down the road, if you're not aware of them. So make sure that that's part of you know, the overall analysis phase. Then comes the design phase, right, and how you go about deploying it. So, you know, having network topology diagrams is critical. I used to be an auditor for like, seven years. And I feel like anytime I asked for network topology diagrams, no one really ever had them, they had things kind of like chicken scratch together in Visio diagrams, and nothing really ever made sense. But having an understanding of your environment is absolutely critical, right? Where are all your servers, you know, reside? What types of systems do you have having an asset management solution, so you know, you know, where this technology needs to be slated and how it protects your overall organization is absolutely critical. So, so if you don't have some of these preliminary, you know, items, within that design phase, it's, it's going to slow you down quite considerably, you know, talking about migration and deploying, and validating all that occurs, you know, in that overall design phase, and then you go into the transition phase, right. And this is where pilot testing occurs. This is where, you know, you take a selection or, you know, population sample of, you know, not everyone, but just a select few to make sure that this rollout is being effective, right? You're transitioning that, that support and the release management to other members in the organization, there's going to be a cutover and a decommission, to have the old technology, right? All that should happen in order. Because if you learn within that initial pilot testing phase, that things aren't going right, the last thing you want to do is hit fully deploy. And then you have, you know, a massive problem on your hands where it's affecting every end user, right, we've seen salute, we've seen issues like that, from time to time where, you know, maybe they didn't fully test it out on, you know, a number of systems maybe only tested on one system. But, you know, if they had tested on 10 to 15, they might have identified some interdependencies that didn't really work well with the technology that they were deploying, right. And that ultimately causes, you know, issues and instability in the operating system, which causes downtime, which causes helpdesk tickets, right? So you want to make sure you have a good population size, when you are going through that pilot testing phase.

18:10

Then comes operations, right, you know, training up the staff, making sure that you're monitoring all the data that's being generated offer that solution, I know, every single solution is a little bit different, I guess depends on, you know, what use case you're looking to solve if it's an EDR solution, or a DLP solution, right. But you want to make sure that you're you have analysts that are also monitoring that data, and that they're trained and equipped to do that, because that comes down to valuing or harvesting the value out of that product that you've just invested in, you know, if you're if you're just deploying a technology, it's generating logs, and you're not looking at that data or actually taking action on the data. What's the point? I mean, it's, it shouldn't be just for compliance, check off reasons alone, right, it should really provide value to your organization. And really, metrics should be built off of that, right? You know, what's the meantime, from an initial, you know, infection to detection, right? If you're looking at malware type metrics, or, you know, how effective is that solution, right, and, you know, some of the use cases that it is actually solving for you. So, you know, reporting those metrics up to the top really does help, you know, continue to sell the product, and also helps you get the renewal, you know, in the following year. And then finally, the improvement phase, we always want to continue to improve, right? You know, just because you've deployed a solution, and you have it in a stable state doesn't mean you don't want to continuously evolve that solution. You know, a lot of technologies have additional functionality, additional features, right, that you can leverage. And it's important to, you know, navigate through those and see what else can we turn on and, you know, kind of offer, you know, in that overall improvement phase so, so having that improvement phase at the end once you've kind of gone through the plan, build run phases is absolutely critical. So, some common, you know, migration pitfalls as well. Right. So not preparing a long term migration roadmap, right with accountable deliverables. I briefly touched on that you want to make sure that you have these deliverables, you know, through that migration plan, you want to make sure you have a contingency plan to for team members, right that are associated with the project. You know, if you, if individuals leave that organization and you don't have backup, that can be a problem, right. And that's where managed services and, you know, kind of outsourcing, that really does help, right, if you don't have a team that can, you know, do the monitoring and do the operations and the run and maintain it, you know, it's nice to have a managed services organization that can kind of continue that because, you know, they'll have the resources to do that. And day one, and if someone leaves, they already have backup personnel, so it's something you don't have to worry about. But if you're doing it internally, without it out, make sure you have contingency plans there. You want to also keep thorough documentation throughout that entire process. I mean, part of that is the contingency plan to so if someone leaves and there's no documentation on, you know, the deployment or how this thing works, right, that's gonna be a tough task for the next person stepping into those shoes, you know, to kind of fill them so. So make sure that you keep thorough documentation throughout that process. You know, you want to test thoroughly, right, we mentioned that throughout each phase in the migration. And, you know, not involving in house experts, even if migration is being handled by a vendor, avoid that, right, you want to have people internal into the company be a part of that process, right? Because even if you're outsourcing it as a managed services, it really should be an extension of your internal team, right, your internal security team or your internal ops team, so that you can work well with one another. If something does happen, right. So it's important to develop those relationships to with your vendor, you know, regardless of whether you're doing managed services, or if you're, you know, running it yourself.

21:40
So just a couple quick tips from Tim, to kind of round this out. You know, enterprise security is not about deploying and maintaining tools, it's about, you know, knowing how your business runs, and what data and apps are vital to it to your customers, right, while also fostering a strong risk management strategy to protect those assets. You know, having a ton of market leading security tools is not going to make your environment secure. I mentioned this earlier, you can spend millions and millions of dollars on security technology. But if you have one user that clicks on a stupid link, right, or an attachment, that's all it takes, right for the threat actor to get in through the backdoor. I mean, I've seen this countless of times, I would say 80% of our incident response investigations, leads back to someone clicking on a link. Of course, there's other avenues of attack, of course, but they're less less common, because this particular attack vector is tried and true, it's continued to work for all these years, and it will continue to work. You know, as long as you know, security awareness is not at the forefront, right of your employee culture, right within the organization. So, so make sure, although you might be deploying all this secure technologies, you also want to make sure that your employees are knowledgeable about cybersecurity, right, and that you do, you know, simulated phishing campaigns, right, so that they are aware that this stuff happens, right on a day to day basis, and you got to be careful, you know, use conferences and exhibitions, that you tend intelligently, I think, you know, I mean, this industry is great, it's got a lot of smart individuals, you know, but developing those relationships can be absolutely critical for you, I mean, especially like in the threat intelligence spaces, or, or any of those, right, like sharing Intel, and sharing your best practices that really helps you and your own organization as well, you know, become better and improve, right, so anytime I go to any of these conferences, Blackhat, def, con RSA, you know, network network, as much as you can LinkedIn, you know, with these individuals, you know, stay connected with them, because you never know, you know, when your paths are gonna cross or when you might need to reach out asking for, you know, some some information, and then approach security from an enterprise perspective, right? You know, building architectures that allow improved visibility into all network activities, right? helps you avoid those blind spots, right? I used to have a CIO or CTO that said, I'm not going to put up butter and jelly cybersecurity controls 10, that's all he ever said to me, I'm not going to peanut butter and jelly, I'm not going to put it everywhere, I'm just going to put it on, you

know, like, my most critical assets. But but the problem with that mentality was, it's not necessarily the the most critical assets were a threat actors were getting into it was the things that were, you know, overlooked, like the development environment, it was, you know, the employee laptops, not having the right visibility there, right, you need to make sure that you do have complete visibility across your entire scope. Otherwise, you're gonna miss that, you know, they're going to laterally move to those high risk assets. But once they're in the environment, they're in the environment, right, and they can establish a foothold. So it is important to avoid having any of those blind spots within your organization. So that kind of talks a little bit about right, migrating on to new solutions from older solutions. I do just want to quickly, you know, discuss what we do as an organization as a company, you know, Digital Guardian. We've been around for quite some time now since early 2002. You know, we're a unified data protection platform, right and we cover these five pillars, right data discovery, data classification, data loss prevention, and endpoint detection and response. And then Cloud Data Protection. And we have all this data that runs up into what we call our analytics and reporting cloud. It's big, massive, you know, Hadoop, Elastic Search back end that allows you to conduct threat hunting, right, pivot across vast amounts of information in order to solve problems, you know, right click functionality in order to, you know, respond to an attack or respond to maybe someone taking information or blocking on that sort of behavior. Right. So, so our platform, we look at it as, you know, a truly an ultimate, you know, data protection platform that can solve all those needs in terms of, you know, identifying what your most, you know, risky assets reside, and classifying that information, and then wrapping controls around that data. So that pretty much wraps it up for me from, you know, a slides perspective. Are there any questions at all on the call? I'll be more than happy to answer them. And Alex as well, feel free to join in.

26:04
Hey, Tim, so a question came in? Can Digital Guardian assist in the RFP process? Can Yep, in the RFP process.

26:24
I say this only because if you say yourself, it's not important. But Tim has actually put together a white paper ebook, on how to step by step, put an RFP process, an RFP, together all the way from gathering your requirements to that site selection, everything he talked about earlier, is actually available on our website as an ebook. The nice thing about it is that in conjunction with i Four, and as we can help you identify, where you have the weak points in your attack surface, you know, where you want to increase your security posture within your, your cybersecurity environment. So yes, the answer is, you have resources from Digital Guardian, to help you identify help you work within that process, to make sure that as Tim mentioned before, you're exhausting. And you're using, the technologies that you have, and then complementing those where you had your greatest security gaps in doing so. And as part of that, we want to make sure that we look at your entire landscape of where you have potential, what we call insider threat, or outsider threat, potential leak points. And it typically leads to a point is, who's looking at your data, and who's moving your data. So from a standpoint of our architecture, where we can look at what data is going or did it in motion, we can look at that data and say, that's sensitive and needs to be treated in this fashion. From the endpoint where all the endpoint data originates, we can then help you identify how to prioritize where you want your data to go, whether it should be classified or which be sensitive, or shouldn't be public. So there are different components within that. environment that we can help you with very long answer to a very short question.

28:41
I have one other question. So 10, you know, any, any comments on what platforms you guys operate on? And specifically like Microsoft, as well as any platforms you can speak on?

28:53
Yeah. So I mean, Digital Guardian operates across all platforms, you know, Mac, Windows, and Linux. And, you know, we're an agent based technology for data loss prevention EDR. But we also have a network appliance as well that can do data discovery and you know, email content inspection from a DLP perspective. So, so yeah, we do cover all operating system types.

29:19
All right, great. Can I also add, when it comes to platform, because platforms can be looked at as what operating systems run on, as Tim said, Windows, Mac, Linux, VDI, VMware kind of thing, but also the platform that the application sits on. So our software can sit in your environment, you own it, you control it, you manage it, we just provide you the support when you need it. The majority of our clients take it a step further. And they say, okay, hey, we're pretty good at what we do. But we're not very good at managing your application. So we'd like to have a hosted environment where Digital Guardian, hosts the environment. And we do that, on the AWS cloud. We manage it, we patch it, we maintain it, to make sure that everything that you're getting from our application itself is the highest fidelity that you can get. Other organizations and we're talking about 60% of the people that are become our clients do the managed service platform, the managed service platform is where Digital Guardian, analysts, architects, project managers, security, analysts, are able to then become your employees. You become a project manager and you tell us, these are the rules sets that I want to be put in place. These are the applications that I want, I want you work with Splunk, I want you work with X, Y, Z net scope, threat, threat over here. And we can put that solution together. As Tim mentioned earlier, one of the biggest challenges in increasing your security posture is having those resources, whether it be IT resources, human resources, or even what I call executive resources. One of the things that we've noticed now in specifically mid to larger enterprises, is that you now have somebody on the board that says, I am responsible for cybersecurity. In the past, that was not the case. Now that person has to be responsive to the board to say, how are you going to get there? How are you going to get from security posture one through five of one to at least three next year for the following year and five the following year, because the cost of a breach or the cost of a cybersecurity failure? breach, I use that term loosely, is tremendous. Whether it be on your reputation, whether it be on your stock, whether it be just on company morale, so platforms, on prem, SaaS, or managed services are provided for you, depending upon your current Crivitz. Law.

32:35
No problem. It just may be to piggyback on and maybe touched on it. But we are pointing out some of the differentiators of Digital Guardian versus kind of some competitive solutions out there in the market. Or Tim or I speak on that what are some of those differentiators specifically that Digital Guardian offers?

32:57

I'll take the first part. Okay, you get to the small difference. So when it comes to data protection, most industry veterans have been exposed to data loss prevention in the old school of thought. And when I say old school of thought, I mean, DLP was sort of an extension of your firewall, if you will. So there was a lot of compliance rules. And those rules need to be defined. And when I say that is okay, I want to see everything that is being uploaded from my endpoints for my users up to the cloud. When I say up to the cloud, it could be a an official site. Or it could be a Google. It could be Firefox, it can be opera, it could be Chrome, all those things. Now, the old school of thought is I need to put a rule in place that says every possible browser, I need to put the rule up with Oh, what about Duck Duck go now. Okay, now you have to update and maintain every potential browser that a file can go up. That's old school thought. Digital Guardian school of thought is we have complete visibility. And when I say complete visibility, it doesn't matter where that file is going to. We know that there's a file that's been uploaded to a specific destination. We've already monitored and record that. So from day one, day one, the minute you put our agent on to that endpoint, we wrote Part 100% of what's happening on that device, every upload every download every print, every scan, every cut and paste every copy to USB or DVD or print job. The reason why that's important is because we have the historical knowledge or record, if you will, of what's happening in your environment, the relevance of the rules, we always see everything, we now then are able to protect what's important, not just what you want to see. And so what really is important when it comes to a differentiator is as an example, Charles, you decided to leave your organization, you're going to give me a two week notice. And in my competitors environment, I'm going to put Charles on my watch list and see what happens what he does in the next two weeks. With Digital Guardian, we've been watching Charles, for the last year, I can run a report and tell you exactly what Charles has done. For the last six months. If you've been looking for a job you've interviewed, you've had your background you had an offer, we can then go back and say, Hey, we seen everything. Now we can tell you what you've done. Now, as part of your exit interview, we're gonna say, Charles, can you test the fact that you either destroyed or returned all that data? And so we then look at that data in a variety of different ways. One is content. What files it Charlson doubt that had content which is like social security number, or patent ID number or some something that effect? We also look from a context? Where did Charles send that file from? Was it an HR file? Was it an A source code file? Was it from a legal file, so not only do we have the content, but we also have a context. And with that combination, in addition to using information from Microsoft or from Bolden, James or Titus, for user classification, the data fidelity that you get is so high, those false positive or irrelevant? We give you true data that you need to keep that risk level down. Sounds good? Tim, you want to add anything else there?

37:45

Yeah, I mean, just, um, that was good. The one thing I would only add, and this is what I think love the most about our technology is we're the only solution that offers not only DLP, but also this EDR capability. So, you know, protecting data, not only from insider threats, but also external cyber threats, malware, you know, exfiltrating data over, you know, DNS protocols, things that are, you know, not typically, you know, not typical functionality that you'd find in a DLP solution, right. So it's nice to have a single solution, a single agent, right, that can do and have all of these different capabilities, right, in terms of protecting the endpoint, but also, more importantly, protecting your most sensitive asset your data.

38:27

Got it? Kind of a follow up question to that. And and maybe that's kind of piggybacking on that, is that unstructured data? How do you kind of discover and manage unstructured data with the solution? On that,

38:48
sent me on to that.

38:50
Oh, that's, that's, that's your real mouse?

38:55
No worries. So when you look at data, you have to look at it in two ways. One is data at rest. So that data at rest was going to be if you look at the slide there, the bottom right hand corner is data that is either in the cloud at your SharePoint, your OneDrive, your box, Ignite, okay? Or even your shares or your network attack storage. So we can look at that and say, Okay, how do we identify where there is potential data that can be quote, unquote, leaked. And the reason for that is in most organizations as they develop their storage strategy, if you will, have been very liberal on where they put that storage. So for example, I'm an accountant at XYZ company. I'm going to be doing work for ABC company. So I'm going to put their books in I'm gonna see books and their p&l, whatever the case may be sensitive counted into my OneDrive so I can go home, and then work out of that OneDrive very sensitive data that is available out there. So how we're able to deal with structured and unstructured data is the fact that our network appliance will go out and do data discovery on files, whether it be in the cloud, or whether it be on prem. And say, by the way, based upon the classification rules that we've set up during the initial setup stage, I noticed that that file has 50 of our count numbers, 50, names 50, so sphere numbers, 50, email, 50, phone numbers, and 50 addresses. Based upon that, I'm going to classify that as sensitive. And based upon the rules that you told me to put together, I'm going to take that sensitive data, move it from where it's at, whether it be on the cloud, or on prem into a secure server, but I'm not going to leave you high and dry, I'm going to pull a cookie crumb that says, If you come look for this data, it's over here, but it's under a secure server. And we're going to treat that data securely, so that from any point they're on, if you try to move that data or quote unquote, work from home with that data is either encrypted, or either secured in a fashion that can't be exposed to the public. That's data at rest from the unstructured data, data in motion that that is something that you're taking from I'm looking at a, your ERP system, your your SAP financial system, I've got the screen up front, I got your most sensitive clients, I took a screenshot, put it into an email and send it out. They didn't motion on that. Because it's sensitive data, because the screen that was up was confidential, I will prevent you from copying that unstructured data out so that we make sure that that sensitive data never leaves. Thank you for that.

42:31
Yeah, I'm not seeing any other questions coming through the chat. Any questions? LinkedIn Live community? If you guys want to put something in the chat, please do so. Otherwise, we're kind of getting ready to wrap up here. Any other kind of final comments? Tim and Alex, that you guys want to give the audience here in attendance and the recorded audience for viewing later?

43:03

Yeah, no, I mean, I just I appreciate the time. I appreciate everyone, you know, joining the call, I do want to just at least leave Alex's contact information. If you guys have any additional questions, you know, feel free to reach out to him via email or, or even his mobile device, but he doesn't want me giving that out. But there it is. That's what he's here for. But no, I definitely appreciate everyone's attendance here. Thank you.

43:26
Any last words, Alex, before we close out, because

43:30
I can't reiterate, reiterate enough what Tim said, we're here to help. We literally help 1000s of organizations, from the first steps of trying to understand where am I at risk? What tools and solutions? Do I need to prioritize in the biggest challenges that we see with most security leaders, whether it be a CISO? Or whether it be CIO or the security department is? Where do I prioritize my time? Second is where do I prioritize my dollars? That being said, the process that we just discussed in the beginning of this webinar make sense of how do I then prioritize what requirements that I have? Where do I put that into an RFP? Can somebody come help me and say, That is a great solution, but you're not optimizing it? Or who sold you that kind of thing. The whole point is, we're here to help. We've got hundreds of engineers and resources throughout the world to be able to sit down with you whether you need 30 minutes or 30 hours to help you out. So feel free to reach out, and we'd be glad to help you any way we can.

44:55
All right. Well, well, thank you so much, I guess house ads Digital Guardian. Appreciate your time and excellent webinar, excellent education for those in attendance and for, again for the future recorded sessions that I'm sure a lot of people will also listen to. So yes, please reach out and also to reach out to you to the eye for group as well. If you can't get a hold out, we will connect you with them as well. And yeah, we enjoyed you attending today's webinar, and please look forward to future Webinars coming every month. And so look at our calendar and we were happy to see you guys again. With that said, thank you guys so much. Thanks, Tim. Thanks, Alex, and everyone out there and LinkedIn and and our webinar. Have a great day. Thank you so much.

45:42
Thank you for group Thank you