

# SambaSafety's Mission to Reduce Risk Begins in its Own Datacenter

*Transcript of a discussion on how a driver risk management software provider protects their business customers from risk by protecting their own IT assets and workers using Bitdefender.*

[Listen](#) to the [podcast](#). Find it on [iTunes](#). [Download](#) the transcript. Sponsor: [Bitdefender](#).

**Dana Gardner:** Welcome to the next edition of [BriefingsDirect](#). I'm [Dana Gardner](#), Principal Analyst at [Interarbor Solutions](#), your host and moderator.

Security and privacy protection increasingly go hand in hand, especially in sensitive industries like finance and public safety. For driver risk management software provider [SambaSafety](#) protecting their business customers from risk is core to their mission -- and that begins with protection of their own IT assets and workers.

Stay with us now as we learn how SambaSafety adopted [Bitdefender GravityZone Advanced Business Security](#) and [Full Disk Encryption](#) to improve the end-to-end security of their operations and business processes.

To share their story, please join me in welcoming [Randy Whitten](#), Director of IT and Operations at [SambaSafety](#) in Albuquerque, New Mexico. Welcome, Randy.



[Whitten](#)

**Randy Whitten:** Thank you.

**Gardner:** Randy, you have a very interesting company. Tell us about SambaSafety, how big it is, and your unique business approach.

**Whitten:** SambaSafety currently employs approximately 280 employees across the United States. We have four locations. Corporate headquarters is in Denver, Colorado. Albuquerque, New Mexico is another one of our locations. There's Rancho Cordova just outside of Sacramento, California, and Portland, Oregon is where our transportation division is.

We also have a variety and handful of remote workers from coast to coast and from border to border.

**Gardner:** And you are all about making communities safer. Tell us how you do that.

**Whitten:** We work with [departments of motor vehicles \(DMVs\)](#) across the United States, monitoring the drivers for companies. We put a partnership together with state

governments, and third-party information is provided to allow us to process reporting for critical driver information.

We seek to transform that data into action to protect the businesses and our customers from driver and mobility risk. We work to incorporate top-of-the-line security software to ensure that all of our data is protected while we are doing that.

## ***Data-driven driver safety***

**Gardner:** So, it's all about getting access to data, recognizing where risks might emerge with certain drivers, and then alerting those people who are looking to hire those drivers to make sure that the right drivers are in the right positions. Is that correct?

**Whitten:** That is correct. Since 1998, SambaSafety has been the pioneer and leading provider of driver risk management software in North America. SambaSafety has led the charge to protect businesses and improve driver safety, ultimately making communities safer on the road.

*SambaSafety has led the charge to protect businesses and improve driver safety, ultimately making communities safer on the road.*

Our mission is to guide our customers, including employers, fleet managers, and insurance providers to make the right decisions at the right time by collecting, correlating and analyzing motor vehicle records (MVRs) and other data resources. We identify driver risk and enable our customers to modify their drivers' behaviors, reduce the accidents, ensure compliance, and assist with lowering the cost, ultimately improving the driver and the community safety once again.

**Gardner:** Is this for a cross-section of different customers? You do this for public sector and private sector? Who are the people that need this information most?

**Whitten:** We do it across both sectors, public and private. We do it across transportation. We do it across drivers such as [Lyft drivers](#), Uber drivers, and transportation drivers -- our delivery carriers, FedEx, UPS, etc. -- those types of customers.

**Gardner:** This is such an essential service, because so much of our economy is on four wheels, whether it's a truck delivering goods and services, transportation directly for people, and public safety vehicles. A huge portion of our economy is behind the wheel, so I think this is a hugely important service you are providing.

**Whitten:** That's a good point, Dana. Yes, it is very much. Transportation drivers are delivering our commodities every day, the food that we consume, the clothes that we wear, also the parts that fix our vehicles to drive, plus also just to be able to get like those Christmas packages via UPS or FedEx -- those are the essential items to our everyday living.

**Gardner:** So, this is mission-critical on a macro scale. Now, you also are dealing, of course, with sensitive information. You have to protect the privacy. People are entitled to information that's regulated, monitored, and provided accordingly. So you have to be across-the-board reducing risk, doing it the right way, and you also have to make your own systems protected because you have that sensitive information going back and forth. Security and privacy are probably among your topmost mission-critical requirements.

## ***Securing the sectors everywhere, all the time***

**Whitten:** That is correct. SambaSafety has a [SOC 2 Type II](#) compliant certification. It actually is just the top layer of security we are using within our company, either for our endpoints or for our external customers.

**Gardner:** Randy, you described your organization as distributed. You have multiple offices, remote workers, and you are dealing with sensitive private and public sector information. Tell us what your top line thinking, your philosophy, about security is and then how you execute on that.

**Whitten:** Our top line essentially is to make sure that our endpoints are protected, that we are taking care of our employees internally to be able to set them up for success, so they don't have to worry about security. All of our laptops are encrypted. We have different types of levels of security within our organization, so that gives all of our employees a way to ease their comfort so that they can concentrate on taking care of our end customer.

*Our top line essentially is to make sure that our endpoints are protected, that we are taking care of our employees internally to be able to set them up for success, so they don't have to worry about security.*

**Gardner:** That's right, security isn't just a matter of being very aggressive, it also means employee experience. You have to give your people the opportunity to get their work done without hindrance -- and the performance of their machine, of course, is a big part of that.

Tell us about the pain points, what were the problems you were having in the past that led you into a new provider when it comes to security software?

**Whitten:** Some of the things that we have had to deal with within the IT department here at SambaSafety is when we see our tickets come in, it's typically about memory usage as applications were locking up the computers, where it took a lot of resources to be able to launch the application.

We also were seeing threats getting through the previous antivirus solution, and then just the cost, the cost of that solution was increasing month over month. Every time we would add a new license it would seem like the price point would jump.

**Gardner:** I imagine you weren't seeing them as a partner as much as a hindrance.

**Whitten:** Yes, that is correct. It started to seem like it was a monthly call, then it turned into a weekly call to their support center just to be able to see if we could get additional support and help from them. So that brought up, "Okay, what do we do next and what is our next solution going to look like?"

**Gardner:** Tell me about that process. What did you look at, and how did you make your choices?

**Whitten:** We did an overall scoping session and brought in three different antivirus solutions providers. It just so happens that they all measured up to be the next vendor that we were going to work with. Bitdefender came out on top and it was a solution that we could put into our cloud-hosted solution, it was also something that we could work with on our endpoints and also to be able to ensure that all of our employees are protected.

*Bitdefender ... was a solution that we could put into our cloud-hosted solution, it was also something that we could work with on our endpoints and also to be able to ensure that all of our employees are protected.*

**Gardner:** So you are using GravityZone Advanced Business Security, Full Disk Encryption, and the [Cloud Management Console](#), all from Bitdefender, is that correct?

**Whitten:** That is correct. The previous solution for our disk encryption is just about exhausted. Currently we have about 90 percent of our endpoints for disk encryption on Bitdefender now and we have had zero issues with it.

**Gardner:** I have to imagine you are not just protecting your endpoints, but you have servers and networks, and other infrastructure to protect. What does that consist of and how has that been going?

**Whitten:** That is correct. We have approximately 280 employees, which equals 280 laptops to be protected. We have a fair amount of additional hardware that has to be protected. Those endpoints have to be secured. And then 30 percent of additional hardware, i.e. the Macs that are within our organization, are also part of that Bitdefender protection.

**Gardner:** And everyone knows, of course, that management of operations is essential for making sure that nothing falls between the cracks -- and that includes patch management, making sure that you see what's going on with machines and getting alerts as to what might be your vulnerability.

So tell us about the management, the Cloud Console, particularly as you are trying to do this across a hybrid environment with multiple sites?

## ***See what's secure to ensure success***

**Whitten:** It's been vital for the success of Bitdefender and their console that we can log on and we can see what's happening. It has been very key to the success. I can't say that enough.

And it goes as far as information gathering, dashboard, data analytics, network scanning, and the vulnerability management - just being able to ensure our assets are protected has been key.

Also, we could watch the alerting that happens to ensure that the behavior is not changing from machine intelligence or machine learning (ML) so that our systems do not get infected in any way.

**Gardner:** And the more administration and automation you get, the more you are able to devote your IT operations people to other assets, other functions. Have you been able to recognize, not only an improvement in security, but perhaps an easing up on the man hours and labor requirements?

**Whitten:** Sure. The first 60 days of our implementation I was able to improve return on investment (ROI) quickly. We were able to allow additional team resources to focus on other tickets and also other items that came into our work scope within our department.

Bitdefender was already out there, and it was managing itself, it was doing what we were paying for it to do -- and it was actually a really good choice for us. The partnership with them is very solid, we are very pleased with it, it is a win-win situation for both of our companies.

*Bitdefender was already out there, and it was managing itself, it was doing what we were paying it to do ... the partnership is solid ... it is a win-win situation.*

**Gardner:** Randy, I have had people ask me, "Why do I need Full Disk Encryption? What does that provide for me? I am having a hard time deciding whether it's the right thing for our organization."

What were your requirements for widespread encryption and why do you think that's a good idea for other organizations?

**Whitten:** The most common reason to have Full Disk Encryption is you are at the store, someone comes in, they break into your car, they steal your laptop bag or they see your computer laying out, they take it. As the Director of IT and Operations for SambaSafety, my goal is to ensure that our assets are protected. So having Full Disk Encryption on board that laptop gives me a chance to sleep a little easier at night.

**Gardner:** You are not worried about that data leaving the organization because you know it's got that encryption wrapper.

**Whitten:** That is correct. It's protected all the way around.

**Gardner:** As we start to close out, let's look to the future. What's most important for you going forward? What would you like to see improve in terms of security, intelligence and being able to monitor your privacy and your security requirements?

## ***Scope out security needs now and down the road***

**Whitten:** The big trend right now is to ensure that we are staying up to date and Bitdefender is staying up to date on the latest intrusions so that our software is staying current and we are pushing that out to our machines.

Also just continue to be right on top of the security game. We have enjoyed our partnership with Bitdefender to date and we can't complain, and for sure it has been a win-win situation all the way around.

**Gardner:** Any advice for folks that are out there, IT operators like yourself that are grappling with increased requirements? More people are seeing compliance issues, audit issues, paperwork and bureaucracy. Any advice for them in terms of getting the best of all worlds, which is better security and better operations oversight management?

**Whitten:** Definitely have a good scope of what you are looking for, for your organization. Every organization is different. What tends to happen is that you go in looking for a solution and you don't have all of the details that would meet the needs of your organization.

Secondly, get the buy-in from your leadership team. Pitch the case to ensure that you are doing the right thing, that you are bringing the right vendor to the table, so that once that solution is implemented, then they can rest easy as well.

Every company executive across the world right now that has any responsibility with data, definitely security is at the top of their mind. Security is at the top of my mind every single day, protecting our customers, protecting our employees, making sure that our data stays protected and secured so that the bad guys can't have it.

*Security is at the top of my mind every single day, protecting our customers, protecting our employees, making sure that our data stays protected and secured so that the bad guys can't have it.*

**Gardner:** I'm afraid we will have to leave it there. You have been listening to a sponsored BriefingsDirect discussion on how driver risk management software provider

SambaSafety protects their business customers from risk, beginning with the protection and management of their own IT assets and workers.

And we have learned how SambaSafety adopted Bitdefender GravityZone Advanced Business Security and Full Disk Encryption to improve the end-to-end security of their distributed operations and important business processes.

So please join me now in thanking our guest. We have been here with Randy Whitten, Director of IT and Operations at SambaSafety in Albuquerque, New Mexico. Thank you so much, Randy.

**Whitten:** Thank you, Dana. I appreciate it.

**Gardner:** I'm Dana Gardner, Principal Analyst at Interarbor Solutions, your host and moderator for this ongoing series of BriefingsDirect discussions. A big thank you to our sponsor, Bitdefender, for supporting these presentations.

Lastly, thanks to our audience for joining. Please pass this along to your IT community, and do come back next time.

[Listen](#) to the [podcast](#). Find it on [iTunes](#). [Download](#) the transcript. Sponsor: [Bitdefender](#).

*Transcript of a discussion on how a driver risk management software provider protects their business customers from risk by protecting their own IT assets and workers. Copyright Interarbor Solutions, LLC, 2005-2020. All rights reserved.*

**You may also be interested in:**

- [For a UK borough, solving security issues leads to operational improvements and cost-savings across its IT infrastructure](#)
- [How an Architectural Firm Retains Long-Term Security Confidence Across a Fully Virtualized and Distributed Desktop Environment](#)
- [Regional dental firm Great Expressions protects distributed data with lower complexity thanks to amalgam of Nutanix HCI and Bitdefender security](#)
- [How MSPs Leverage Bitdefender's Layered Approach to Security for Comprehensive Client Protection](#)
- [How a large Missouri medical center developed an agile healthcare infrastructure security strategy](#)
- [Kansas Development Finance Authority gains peace of mind, end-points virtual shield using Hypervisor-level security](#)
- [How a Florida school district tames the Wild West of education security at scale and on budget](#)
- [The next line of defense—How new security leverages virtualization to counter sophisticated threats](#)
- [Cybersecurity standards: The Open Group explores security and safer supply chains](#)