

## ***XDAS Standard Aims to Simplify Creation of Audit Trails from Complex and Distributed Systems***

*Transcript of a BriefingsDirect sponsored podcast on an emerging standard aimed at easing governance and compliance in heterogeneous environments. Recorded live at The Open Group's 23rd Enterprise Architecture Practitioners Conference and 3rd Security Practitioners Conference in Toronto.*

[Listen](#) to the [podcast](#). Download the podcast. Find it on [iTunes/iPod](#) and [Podcast.com](#). Download the transcript. Learn more. Sponsor: [The Open Group](#).

**Dana Gardner:** Hi. This is [Dana Gardner](#), principal analyst at [Interarbor Solutions](#), and you're listening to BriefingsDirect.



Today we present a sponsored podcast discussion, coming to you from The Open Group's [23rd](#) and the associated 3rd Security Practitioners Conference in Toronto, the week of July 20, 2009.

We're going to take a look at an emerging standard called [XDAS](#), which looks at audit trail information from a variety of systems and software across the enterprise IT environment.

This is an emerging standard that's being orchestrated through The Open Group, but it's an open-source standard that is hopefully going to help in compliance and regulatory issues and in the automation of heterogeneous environments. This could be increasingly important, as we get into [virtualization](#) and [cloud computing](#).

Here to help us drill into XDAS, we're joined by [Ian Dobson](#), director of the Security Forum for The Open Group. Welcome, Ian.

**Ian Dobson:** Hello.

**Gardner:** We're also joined by [Joël Winteregg](#), CEO and co-founder of [NetGuardians](#). Welcome, Joel,

**Joël Winteregg:** Hello.

**Gardner:** First off, not that many people are familiar with the audit trail issue. We've, of course, heard a lot about log files over the years, and the information from variety of systems in IT. What is the problem set that we're working on and why did The Open Group get involved, Ian?

**Dobson:** We actually got involved way back in '90s, in 1998, when we published the XDAS Standard. It was, in many ways, ahead of its time, but it was a distributed audit services standard. Today's audit and logging requirements are much more demanding than they were then. There is a heightened awareness of everything to do with audit and logging, and we see a need now to update it to meet today's needs. So that's why we've got involved now.



A key part of this is event reporting. Event reports have all sorts of formats today, but that makes them difficult to consume. Of course, we then generate events so that they can be consumed in useful ways. So, we're aiming the new audit standard from XDAS to be something that defines an interoperable event-reporting format, so that they can be consumed equally by everybody who needs to know.

**Gardner:** Joël, tell me a little bit about why you got involved. What was the problem that you identified that needed to be improved?

### *Single standard is easier*

**Winteregg:** My company is working in the area of audit event management. We saw that it was a big issue to collect all these different audit trails from each different IT environment.



We saw that, if it was possible to have a single and standard way to represent all this information, that would be much easier and relevant for IT user and for a security officer to analyze all this information, in order to find out what the exact issues are, and to troubleshoot issue in the infrastructure, and so on. That's a good basis for understanding what's going on the whole infrastructure in the company.

**Gardner:** As it stands now, audit information comes across helter-skelter. There isn't a single way. It's dependent upon the vendor, the actual device, and/or the software.

**Winteregg:** Exactly. There is no uniform way to represent this information, and we thought that this initiative would be really good, because it will bring something uniform and universal that will help all the IT users to understand what is going on.



**Gardner:** Also, there is currently very little emphasis on the analysis of this audit trail information. Most of the solutions that are available are just simply to harness and collect it.

**Winteregg:** Yes. There is a lot of effort spent on collecting and then normalizing all this information, while the most important effort, the analysis of this audit trails, is left behind, because it takes so much effort to understand these trails.

If you take, for example, logs from [Cisco](#), [Nortel](#), [SAP](#), and so on, each different vendor is using another language. It is like understanding French audit trails, Chinese audit trails, or German audit trails. There is no uniform way to provide this information.

Then, for auditors or administrator, it is really costly to understand this information and use it in order to get relevant information for management to have metrics and to understand what's really happening on the IT infrastructure.

**Gardner:** Why is this different from log information? The audit information is something that tells us about what's going on within an event, for example.

**Winteregg:** Audit information deals a lot with the accountability of the different transactions in an enterprise IT infrastructure. The real logs, which are modulated to develop strong meaning for debugging applications, may be providing the size of buffers or parameters of an application. Audit trails are much more business oriented. That means that you will have a lot of accountability information. You will be able to track the who, the what, and the when in the whole IT infrastructure, which is really important these days with all these different regulations, like [Sarbanes-Oxley \(SOX\)](#) and the others.

**Gardner:** So, those folks who have to comply with regulations -- maybe it's the payment card industry, or specific regulations for specific industries -- need to create this audit trail. Right now, it's expensive, and the XDAS solution is designed to simplify and automate that.

### ***Complying with regulations***

**Winteregg:** Exactly, because each IT user has to define how they will collect this information in order to comply with all these regulations. For example, the banking industry has [Basel II](#) or SOX, which have a big impact on auditing and accountability management. Each company, each bank, has to deal with its own defined strategy to analyze these trails, to collect them, or to store them.

With a standard like XDAS, it will be much easier for a company to be in compliance with regulations, because there will be really clear and specific interfaces from all the different vendors to these generated audit trails.

**Gardner:** And this is an open-source standard, so it's under the [Lesser General Public License \(LGPL\)](#). Is that correct?

**Winteregg:** Yes. The standard will be open, but there is a Java implementation of that standard called XDAS for J, which is a Java Library. This implementation is open source and business friendly. That means that you can use it in some proprietary software without having to then provide your software as an open-source software. So, it is available for business software too, and all the code is open. You can modify it, look at it, and so on.

**Gardner:** This is available for examination and download at [Codehaus](#). Is that correct?

**Winteregg:** Yes. It's on the [Codehaus platform](#).

**Gardner:** Why is this important, as we move towards heterogeneity that spans not just systems but sourcing, for example cloud, a supply chain, or [software as a service \(SaaS\)](#)? Compliance still needs to be adhered to and regulations need to be complied with. Yet, many of these systems are no longer under your roof.

**Winteregg:** In distributed environment, it's really hard to track a transaction, because it starts on a specific component, then it goes through another one, and to a cloud. You don't know exactly where everything is happening. So, the only way to track these transactions or to track the accountability in such an environment would be through some transaction identifiers, and so on.

Collecting all the different logs from all the different components of a cloud is really useful, because you collect everything in a single point and then you have all this information available for analysis and correlation. So, you can correlate maybe a transaction ID between all the different transactions.

Then, you can drill down into this information to track the whole transaction without having to connect to each different component of the cloud. So, it's really useful to remotely collect this information in order to enhance all the accountability aspects of this computing method.

**Gardner:** Of course, it's going to grow more important. What about in a virtualized environment, where perhaps you're still inside of your own IT organization, but you've got virtualized instances of applications and services? Sometimes, those come and go, depending on the elasticity and efficiency that you're seeking. Logging and auditing also perhaps would disappear. Is this something that can be useful in the context of a highly virtualized environment?

### ***Similar to cloud***

**Winteregg:** Yes. That's a similar context to the cloud-computing environment. We had an example like this at Geneva State in Switzerland, where the SAP system was moving around to several different instances. Sometimes, the service is on specific machine and a minute later, it's on another machine.

All the different instances will be sending this information to a place where you can analyze it through, maybe, usernames. You don't really care at the end exactly where the transaction or the processing happens. You only care about collecting the information and then analyzing all of this in a single point. So, there's less effort spent on collecting each different point of this information, because everything is already into a single box, a single place.

**Gardner:** Please tell me where are we in terms of the maturity of this XDAS standard? Is this something people can use already? What additional work and/or acceptance does this need to go through before it's enterprise ready?

**Winteregg:** The standard was mainly done by people from Novell, like [David Corlette](#) or [John Calcote](#), who are involved into defining the standard. It is at a draft stage right now. It is available for consultation and for feedback as a draft, but as we think that pragmatic approach is much more efficient in the definition of such a standard.

That's why, even if it's only a draft, we've started to already develop an open-source library, like XDAS for J, which enables IT users and developers to try to include this library into their testing program or business application, in order to get audit trails in a good and understandable format. We believe that having such a tool before the standard is strongly defined will help in enhancing all the different aspects of the standard.

**Gardner:** What about the role of the vendors, the suppliers of these devices and software and appliances? What do they need to do in order to make this standard more pervasive?

**Winteregg:** The best thing would be to have some feedback about how easy it is to use and how easy it is to understand or if there are some use cases that use the standard. We started another pragmatic approach, based on the Agile development process of software development, which is made up of use cases and test-driven development.

Through these different iterations, we'll bring a more efficient standard. So, we're waiting for some feedback from vendors and users about how it is easy to use, how helpful it is, and if there are maybe some use cases -- if the scope is too wide, too narrow, etc. We're open to every comment about the current standard.

**Gardner:** Well, great. We've been learning about an audit trail standard that's emerging. It's called XDAS, and we certainly encourage people to take a look at it as a way of adhering to compliance in complex environments and across virtualized and cloud and extended enterprise activities.

We've been joined in our discussion here by Ian Dobson. He is the director of the Security Forum for The Open Group. We've also been joined by Joël Winteregg, CEO and co-founder of NetGuardians. Thank you, Joël.

**Winteregg:** Thank you.

**Gardner:** This is Dana Gardner, principal analyst at Interarbor Solutions, and you've been listening to a sponsored BriefingsDirect podcast from The Open Group's 23rd Enterprise Architecture Practitioners Conference and the associated 3rd Security Practitioners Conference here in Toronto, the week of July 20. Thanks for listening and come back next time.

[Listen](#) to the podcast. [Download](#) the podcast. Find it on [iTunes/iPod](#) and [Podcast.com](#). Download the transcript. Learn more. Sponsor: [The Open Group](#).

*Transcript of a BriefingsDirect sponsored podcast on an emerging standard aimed at easing governance and compliance in heterogeneous environments. Recorded live at The Open Group's 23rd Enterprise Architecture Practitioners Conference and 3rd Security Practitioners Conference in Toronto. Copyright Interarbor Solutions, LLC, 2005-2009. All rights reserved.*