Steve Visconti, President & CEO, Xiid, Discusses Marriott, ID Management and Why Xiid Solutions Are Impervious To Attack

"In The Boardroom" On SecuritySolutionsWatch.com

NEW YORK, NEW YORK, UNITED STATES, December 5, 2018 /EINPresswire.com/ -- SecuritySolutionsWatch.com: Thank you for joining us today, Steve. One will read at Xiid.com, that ...

Steve Visconti, President & CEO, Xiid

" Xiid.IM Identity Access Management is based on Xiid's unique and patent-pending SealedChannel™, which greatly minimizes the attack surface in comparison to any other identity management solution available today. Unlike all competitors, our technology cannot be broken into, simply because there is no way for attackers outside your network to reach the authentication agent, nor any way to even try to directly attack your Active Directory / LDAP servers. In SealedChannel's reverse approach, the authentication agent is the active component that connects outbound, creates a twice-encrypted and twice-signed channel, and retains full authority over which authentication requests are pulled in and handled. We also developed an identity masking feature which allows you to log into your web app with an anonymous name utilizing your real identity against your on-premise directory without compromising that directory. If a SaaS or cloud service provider really wants to protect the clients identitiy, they will use our One-time-ID solution (OTID). OTID sends only a one-time-code which replaces both the User ID and the Password thus giving the ultimate identity protection."

> We are honored to have Steve Visconti, President & CEO, Xiid, join us "In The Boardroom" to discuss the Marriott breach, identity management and Xiid solutions which are impervious to attack"
>
> *Martin Eli, Publisher*

It seems to us that your timing in launching Xiid could not be better with all the recent headlines about identities exposed or stolen from many major sites:
Marriott: https://techcrunch.com/2018/11/30/starwood-hotels-says-500-million-guest-records-stolen-in-massive-data-breach/
Cryptolocker - NotPetya - WannaCry:
https://www.csoonline.com/article/3212260/ransomware/the-5-biggest-ransomware-attacks-of-

the-last-5-years.html
Equifax: https://www.ftc.gov/equifax-data-breach
Ticketmaster: https://www.zdnet.com/article/ticketmaster-breach-was-part-of-a-larger-credit-card-skimming-effort-analysis-shows/
Uber: http://fortune.com/2018/04/12/uber-data-breach-security/
My Heritage: https://www.reuters.com/article/us-myheritage-privacy/security-breach-at-myheritage-website-leaks-details-of-over-92-million-users-idUSKCN1J1308
Orbitz;https://www.usatoday.com/story/tech/2018/03/20/800-000-orbitz-cards-compromised-breached/442277002/
and the ransomware attack on the city of Atlanta: https://www.cnn.com/2018/03/27/us/atlanta-ransomware-computers/index.html

Steve Visconti: Yes, the industry has failed to spend the time and resources required to protect the individuals most important asset, their identities. Xiid is making it easy and cost effective for companies to deploy a hardened identity system by utilizing Xiid.IM. We approach the market by educating the service providers, the enterprise and even individual consumers. All have a vested interest in in keeping their identities safe.

Moreover, today several news outlets are reporting that GCHQ (British Intelligence) is asking messaging companies like Facebook/WhatsApp, Apple, Signal, Wire, Wickr, to allow "lawful eavesdropping" on their private and encrypted communications. The stakes have never been higher, we must do everything possible to protect individual identities.

SecuritySolutionsWatch.com: Before drilling down into exactly how Xiid works, please tell us about your background Steve and your team at Xiid (https://www.xiid.com/leadership.html).

Steve Visconti: I have been a serial entrepreneur with over 30 years in Silicon Valley high-tech companies. My experience in developing company go-to-market strategies from an executive leadership has been in both startups and public companies including Cisco Systems, Airespace, Proxim, Ascend, Chipcom, and Banyan Systems. I have been involved in 7 startups leading to 4 acquisitions and 2 IPOs.

Our co-founder and CTO, Federico Simonetti has an impressive and unique set of experiences which make him uniquely qualified to understand the problem from a 360 degree view, thus his solution to the problem is with a zero cyber-attack surface. His background as the original former ethical hacker (DDT) was known worldwide, entrepreneur having started and run four technology companies with four successful exits. As a side activity Federico was a professor of operating systems security at the University of Milan for 7 years. He also developed software for multiple law enforcement agencies including an Artificial Intelligence investigative platform still in use today.

Guido Pellizzer – Founder and Chief Engineer continues to demonstrate his masterful ability to code in 10+ development languages including assembly, C, C++, C#, Java, Pascal, Delphi, Basic, Javascript and more. Guido is an expert in security, reverse engineering, encryption, SQL, noSQL, REST services, cloud architecture.

That is the core of our very dynamic and as I said, uniquely qualified to solve this problem.

SecuritySolutionsWatch.com: How does Xiid work and how does it prevent the breaches we just mentioned above?

Steve Visconti: Our patent pending Twice Encrypted, Twice Mutually Signed, Two-Layer, Websocket (T3W)technology is a unique, purpose built technology platform that provides a very secure double-encrypted channel that arbitrates between a cloud-based service and the on-premise network without opening inbound ports on the enterprise firewall. The secure channel can then be used for a variety of services including in phase one, Identity and Access Management with Opaque / Anonymous user identities. In later releases, encryption key management and related services, ubiquitous database access, remote digital signature, object and document access from and to on-premise file servers. Xiid.IM with SealdChannel is the only product on the market with No Attack points!

In summary, this is why both public and private enterprises need Xiid....

·Zero Attack Surface through SealedChannel – no port forwarding and no copies of identities in the cloud
·Xiid OTID is the only Username-less and Password-less authentication product available today.

·Certificate Based Authentication support which does not rely on tomcat or windows IIS.
The full stack is integrated into the Xiid agent safely behind the enterprise firewall.
·Anonymous and Opaque user identities – allows users to protect their actual identities and UPN from cloud applications.

We will have more updates about developments at Xiid in early 2019....please stay tuned !

In the meantime, watch our video
(https://videos.weebly.com/uploads/1/1/6/4/116438053/xiid_118.mp4)
and check out our blog (https://medium.com/hybrid-security-superheroes).

SecuritySolutionsWatch.com: Thanks again for joining us today Steve and we look forward to those updates!

For Steve Visconti's discussion on SecuritySolutionsWatch.com
http://www.securitysolutionswatch.com/Interviews/in_Boardroom_Xiid_Visconti.html

For more information: www.Xiid.com

****
About SecuritySolutionsWatch.com
www.SecuritySolutionsWatch.com features thought leadership interviews about IT, IoT and security solutions. Our flagship "In The Boardroom" program, now in its 15th year, has delivered outstanding content about solutions from leading global brands such as: 3M, AMAG Technology - A G4S Company, ASSA ABLOY, Cisco Security, Cyberinc, Dell EMC, HP Cybersecurity, Fujitsu, Gemalto, HID Global, IBM, ImageWare, Intel, SAP, Siemens, Stanley Security, SONY, Unisys, and Yahoo, just to name a few.

What's YOUR authentication, cybersecurity, physical security, mobility, or "smart" solution?
What's YOUR Blockchain or FinTech solution?

We invite you to please join us "In The Boardroom" at www.SecuritySolutionsWatch.com.
For a quick tour to see exactly how your brand will be featured, please contact Ali Eng on our publishing team via
email: ALE@SecuritySolutionsWatch.com, or phone: 1+914.690.9351, or, LinkedIn:

https://www.linkedin.com/in/ali-eng-a8a41015b/

For more details, please click here: www.SecuritySolutionsWatch.com/Main/Jan2018.pdf
And for our Media Kit, please click here: www.SecuritySolutionsWatch.com/MediaKit.html

****

It's FREE...our monthly newsletter with thought leadership content from leading security experts.
Please click here: www.SecuritySolutionsWatch.com/newsletters/newsletter_2018_11.html
And please visit us on Twitter here: www.twitter.com/SecStockWatch

****

All content which appears on SecuritySolutionsWatch.com and in this Press Release is subject to our disclaimer: www.SecuritySolutionsWatch.com/Main/Terms_of_Use.html

****

Martin Eli, Publisher
SecuritySolutionsWatch.com
+ + +1 9146909351
email us here
