CEOCFO Magazine

ceocfointerviews.com

Issue: December 19, 2016

Innovative Solution Uses Behavioral Analysis to End the Risk of Data Exposure on Stolen Active Laptops, Computers, and Mobile Phones

Active technology protects the mobile workforce by Locking down devices at the moment of compromise

Ryk Edelstein
Chief Executive Officer

Cicada Security Technology
http://cicadasecurity.com/

Contact:
Ryk Edelstein
888-514-2896 / 514-509-5219
ryk@cicadasecurity.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

"Cicada Security Technology's relationship with Intel Security, and recent integration of Cicada PDP with the McAfee Security platform, has enabled us to not only create value for our respective technologies, but also helps us gain exposure to a larger market base."- Ryk Edelstein

CEOCFO: ***Mr. Edelstein, what is the Cicada Security Technology approach to security?***

Mr. Edelstein: To best answer that question, I really should explain how we came to be. We initially developed the Cicada Physical Data Protection (PDP) technology to address the data privacy needs of a client with a tens of thousands of laptops in use by their mobile work force, and an annual theft rate of close to 1,000 devices per year. In every case, each of the laptops either contain stored confidential data, or have network access to data which the company has an obligation to protect. Protecting data on an inactive computer can be addressed with authentication and encryption technologies; however, in this case, their concern was the protection of accessible data on active and authenticated laptops stolen while in operation.

In our initial mandate our objective was to identify a process, or product capable of preventing data exposure under these conditions. We soon discovered, there was no available solution. Not willing to accept defeat the client extended our mandate to conduct two studies, the first being a study of the behavior and actions occurring during the theft or tamper of a laptop or other mobile end point device. The second study was focused on inventorying available system features and resources on laptops, tablets and mobile phones, which could be used to reliably identify the physical actions identified in the first study. It was learned that that these devices failed to provide reliable resources to detect theft or tamper. As a result, we developed and patented the Cicada PDP hardware and software necessary to adequately address this problem.

The obligation of organizations to comply with increasingly complex data privacy regulations, paired with the trend in office space reduction, has resulted in a growing population of mobile workers all in need of adequate security against incidental data exposure occurring due to the attempted theft or tamper of a laptop, mobile phone, or tablet. It soon became evident that there was a market for Cicada PDP technology and that it was certainly not a solution looking for a problem

CEOCFO: ***How are you able to come up with a way when either others had not or people have not tried?***
Mr. Edelstein: Realizing the challenge we faced could not be resolved using existing technology, we needed to take a different approach than others would normally consider. While all other security technology vendors have focused on

protecting data against threat with authentication, virus, Malware, encryption and perimeter security, we have observed that the one vulnerability which cannot be addressed by these technologies is the ability to detect risk posed by physical sources of threat.

By taking a fresh approach at security, and our willingness to develop custom designed hardware to detect the physical actions which are attributed to theft or tamper, we are able to reliably detect and prevent the consequential exposure of confidential information when an active and authenticated laptop, mobile phone, or tablet is stolen or tampered with.

CEOCFO: ***Were you too far ahead or are people ready for it?***
Mr. Edelstein: Until recently we had been at a point where we are addressing a problem slightly ahead of the industry's curve. Being a veteran of the IT security industry, one of the many things I have noticed is that nobody talks about a problem unless they know of a solution. Cicada PDP is an important data privacy solution to a very common vulnerability, and we are becoming more topical right now as we gain visibility.

When we first started Cicada, I would say that we were moderately ahead of the market; however, in our first year of development, we managed to get the interest of Intel Corporation's Anti-Theft Feature Set group, a team of engineers and product specialists who were developing what could be described as an innovative hardware enabled security technology. The management of this group, while researching complementary technologies became intrigued by our work, and requested a meeting to discuss the potential alignment of our innovation to their work. As it turned out, they were looking at building a similar technology in-house to study how physical threat detection could benefit their efforts to build market for their antitheft product. The result of our introduction to Intel enabled us to establish to benefit from a collaborative partnership with Intel during our early stages of development.

CEOCFO: ***Would you explain the technology?***
Mr. Edelstein: I will give you an actual example. If we think back during sequestration of the Federal Government, organizations and departments reduced their floor space at a very fast rate. Employees who were once protected by an access controlled office and a guard in the lobby, were sent off to work from home. This action created a situation where computers which can access confidential information, are now being used outside of the confines of the protective environment once afforded by the office. As a result, should one of these devices be used in a café, or other public venue, any active laptop left unattended, even for a moment, stands a high probability of being stolen. Once an active and authenticated device is stolen any stored, network or cloud accessible confidential information can potentially become exposed to an unauthorized party.

Cicada PDP monitors trigger points from both the Cicada PDP device and the host device, to identify and analyze behavioral actions, enabling us to discern legitimate user activity from threat. Some of the actions we monitor include motion, power, network and Bluetooth states, as well as USB and writable media insertion or removal, amongst other actions. Once triggered, PDP uses a user defined policy model to instantly invoke responsive alerting and protective actions. These actions can include system lockdown, the issuance of alerts to an enterprise Security Event Information Management (SEIM) platform, and the issuance of instant alerts to the user and security management. PDP will even activate a siren on both the computer and the PDP device as a distraction to the perpetrator, drawing attention to the compromise.

A simple illustration of what Cicada PDP does could be the example of somebody using their computer in a coffee shop, who momentarily steps away from their computer. At this moment somebody attempts to steal the laptop. Cicada PDP instantly locks down the computer rendering data and programs absolutely inaccessible until the authorized user disarms it.

CEOCFO: ***How do you prevent false alarms?***
Mr. Edelstein: The person who is using the computer, tablet or mobile phone, being aware of the Cicada system will disarm the Cicada PDP before causing a potential trigger action to occur. Alternately, when a thief attempts to steal or tamper with a Cicada PDP protected device the system will trigger and go into lock down. Even if they try to disconnect our Cicada PDP USB device from a protected computer it will cause the system to trigger as well. Only the user can disarm it.

In more extreme cases, where absolute data protection is necessary, we can invoke dismount that encrypted storage, or the destruction of cryptographic keys used to secure communications, stored files, or complete hard drives, so that even if somebody were to bring that machine back to life, they would not be able to access any data. In this situation, a false alarm requires an administrator to restore the crypto keys to reactivate the system.

CEOCFO: ***Who is using Cicada today? What types of organizations?***
Mr. Edelstein: The Cicada was initially developed for use by a client in the power utility sector. Today, the Cicada PDP is used in both the US and Canadian Federal Government, and is under evaluation by a number of US Federal Government departments and agencies.

CEOCFO: ***Are you able to protect desktops as well as laptops?***
Mr. Edelstein: Yes, typically somebody is not going to get up and walk away with a desktop, but Cicada PDP provides an effective means to detect tamper of both desktops, servers and any device with a USB port and an operating system we can wrote a driver for.

CEOCFO: ***Are potential customers skeptical? Do they believe once they see a demo? Do they still wonder if it really will work? What has been the response?***
Mr. Edelstein: As with any new technology, there is always going to be skeptics, and the biggest challenge that we have face as a startup developing an innovative technology is that everybody is waiting for somebody else to commit to the technology. Our recent involvement with Intel Security, as a member of their Security Innovation Alliance (SIA) partnership program, enabled us to integrate Cicada PDP with McAfee's event management platform, and Data Exchange Layer (DXL) cross vendor integration technology.

Intel Security appreciates the benefit of what we add to McAfee client experience, and our relationship with Intel Security helped us get past the skepticism. The added benefit of our integration with the Intel DXL framework, is the ability for other vendors to easily integrate their technologies with Cicada PDP. As an example, if an encryption, authentication or any other DXL compliant vendor wanted their product to have visibility to theft or tamper events in real time, DXL affords this capability without the need for extensive integration effort.

CEOCFO: ***Do you see your strategy of engaging with Intel Security as a better way to reach potential customers? Does it matter?***
Mr. Edelstein: Our relationship with Intel is critical to our market development. We exist in a David versus Goliath type market. As an innovator of disruptive technologies, one often feels like a man shouting in a very larger field, getting attention and awareness is a big challenge. Cicada Security Technology's relationship with Intel Security, and recent integration of Cicada PDP with the McAfee Security platform, has enabled us to not only create value for our respective technologies, but also helps us gain exposure to a larger market base.

The value of this relationship goes both ways, as McAfee can now offer clients an enterprise security platform which provides visibility to physical threat, something no other vendor can offer today.

CEOCFO: ***Are people becoming more accepting of using your technology? There seems to have been some resistance to the use of external hardware.***
Mr. Edelstein: Hardware based technology faces some resistance, and I agree with your statement. But in this case, the device is necessary. When we started this in our conversations with Intel's Anti-Theft Feature set group, one of the topics we discussed was the notion of embedding our technology this into laptops, computers and mobile devices. We all agreed that as an external device the technology could be ubiquitous allowing someone to travel with their Cicada and plug in to any computer anywhere in the world, enabling them to demonstrate physical security on that device. Although USB devices may be seen as an inconvenience, many of us carry around the USB thumb drive in our pocket or purse or our laptop bag.

CEOCFO: ***Might an individual use it on their own instead of through their company?***
Mr. Edelstein: Absolutely. One of the visions we had when developing the technology, was that although the technology is well aligned to enterprise and government use , we also see the Cicada PDP being an well aligned to students or anyone working in a library or public space. Computers are frequently stolen out of a university libraries, coffee shops and airports, and the Cicada PDP would benefit anybody who is concerned about preventing identity theft or data privacy.

CEOCFO: ***What is the business model for you?***
Mr. Edelstein: We value performance and efficiency, and have adopted a channel sales model by engaging with strategic partners covering a number of geographic regions and industry vertical markets. Learning from my past experience running companies involved in the security solution provider market, I came to develop a very strong appreciation of the channel sales structure affords agility and the ability to engage those who own relationships in the markets we expect to develop. As the developer, our role is to establish a foundation which enables our channel partners to succeed in building markets for our product. This model affords us agility to build a strategic market presence without having to support our own organic sales operation.

CEOCFO: ***Where are you right now?***
Mr. Edelstein: We have completed our first round of production and are shipping product. Those who are presently working with us have an evolved understanding of risk and security, and appreciate the vulnerabilities we address. We are presently working on building stronger visibility with strategic clients in the government and enterprise markets, as well as cross-platform alliances with other security technology vendors.

On the development side, our mobile version of the product is still under development. As we will not be using a USB connected device, we had to approach mobile technology using an entirely different strategy.

CEOCFO: ***Is there essentially one product and one service?***
Mr. Edelstein: We are focused, and very interested in keeping it simple. Presently we are producing the Cicada PDP USB device; the mobile version should be available shortly. Aside from the PDP product, we offer a monitoring subscription service which allows Cicada PDP users to get alerts when their device is triggered. Our current objective is to establish the Cicada PDP as the go-to solution for protecting confidential data against exposure occurring due to end point theft or tamper.

CEOCFO: ***With so much going on in security and so many approaches, how do you breakthrough with what is a very common sense, easy to understand approach?***
Mr. Edelstein: Cicada Security Technology is a company which is not in competition with anyone. We are not working on building a better antivirus, firewall or anti ransomware product. We are interested in partnering with technology companies, such as Intel Security, to add complementary value to their security solutions.

The value of some integrations may not seem evident at first glance, but once all parties look at the big picture, the value statement is compelling. One such example would be integrating Cicada PDP with wireless network technology. The ultimate vision being that we enable a wireless network to flag a compromised device, disallowing it access to secure network resources. Likewise, Cicada PDP can be integrated with an encrypted USB storage device to ensure that once the host is compromised, access to secure data on the encrypted device is halted. The options seem endless.

CEOCFO: How do you handle ***resistance or pushback?***
Mr. Edelstein: On occasion, when we are faced with pushback it is often attributed to a failure to understand the purpose or operation of the technology. This is often rectified by explaining the application of the technology relative to the client's business and privacy needs.

When engaging with potential technology alliance partners, our success in developing meaningful engagements is based on our ability to illustrate mutual values presented in a common vision demonstrating how the integration of our technologies afford our respective clients added functionality, while creating a competitive edge over other vendors.

CEOCFO: ***Why pay attention to Cicada Security right now?***
Mr. Edelstein: Data loss resulting from the attempted theft or tamper of a laptop or mobile device is a big concern which should be an issue for anyone responsible for data privacy. We are gaining a lot of attention from those responsible for the absolute protection of data within their organization, as a means to limit their exposure to risk caused by human error, and a targeted attack at the endpoint.