SANS

Analyst Program

WhatWorks

WhatWorks in Deploying Effective and Efficient Key Management Services Across All Business Services

unbound security

Introduction

Business damages from cyber attacks have made it clear that sensitive business information and application must be better protected. Increased enforcement of national- and state-level privacy laws, as well as the need to secure data across multiple cloud environments, has highlighted the need for reliable and transparent data encryption services to protect information while enabling business access.

During this SANS WhatWorks, Mathew Newfield, CIO and CSO at Unisys, will provide details about the selection and deployment of Unbound Security's CORE Key Management product across the Unisys business environment. The deployment supported code signing, digital certificates, and encryption key management across the entire business services life cycle, from app dev to service delivery and transaction support.

About the User

Mathew Newfield joins the Executive Leadership Team with expanded responsibility for the IT and Security functions for Unisys effective January 2021 reporting to the CEO. He joined Unisys March 2018 as the Corporate, Chief Information Security Officer with responsibility for design, development, and implementation of the company's corporate information security and risk programs across all regions and functions. Newfield has over 19 years of experience in Information Technology with a focus on Security, Software as a Service Operations, Risk Auditing and Management, and International Mergers and Acquisitions.

About the Interviewer

John Pescatore joined SANS as director of emerging security trends in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems and "the occasional ballistic armor installation." John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008 and is an NSA-certified cryptologic engineer.

Question

Matt, tell us a little bit about your background and the role you play at Unisys.

Answer

My name is Mathew Newfield. I am what's known as the CSIO, or chief security and infrastructure officer. I run both our security function as well as our IT function for the corporation.

Question

With that dual-hat role, who do you report to?

Answer

Exactly. I report to our CEO and chairman.

Question

Unisys is a very big company. For the data security initiative we are going to talk about today, can you give us an idea of the scope?

Answer

It's corporatewide. When we roll things out to the organizations through my offices, we want to make sure they are corporate standards so that everybody is utilizing the same capabilities, especially when we are establishing a baseline.

Question

What were the business issues that started you looking at encryption/key management technologies and solutions?

Answer

The initial reason we really wanted to focus on this was that while we were already doing cryptographic key management, everybody was doing it differently. They had different standards and different technologies in place. That resulted in very uneven capabilities.

Everybody had their own processes, or lack thereof, which caused some internal impacts. It wasn't just someone forgetting about a cert revocation or expiration. It was trying to track down the who behind the environment. We realized we needed to standardize in order to build out our processes and make sure that people are given enough time, enough notification, enough escalation so that we don't run into those problems anymore.

Question

Were your requirements just for managing keys for bits in motion, like SSL, SSH, etcetera, or are you also doing any persistent data encryption that you wanted to be covered as well?

Answer

That would be yes, yes, and yes, with code signing included as well as a high-priority requirement. We needed a capability to make sure that the code that we're developing is not being modified without the appropriate permissions and that we're able to show internally that the code is correct as inputted into the environment. That was really critical for us.

Question

Since this was going to involve buying a product, it was going to take some funding. How were you able to justify the expense?

Answer

You always have to convince people. But luckily for me, it wasn't a very difficult convincing exercise. With the costs, complexity, and staff needed to do this in

the old, uncentralized way, we were able to realize and demonstrate actual cost savings. I think a lot of organizations are in that same boat. That's what made it an easier conversation.

Question

How did you evaluate alternatives? Did you use RFPs? Bake-offs?

Answer

We are required to do that. As part of our own processes, we don't just pick a singular solution and run with it. We went through a bake-off. We had multiple vendors in our controlled environments come in and provide us with solutions. We worked with each of those vendors to scope it to an appropriate need, so we were really doing an apples-to-apples comparison.
Some vendors have better add-ons, some have no add-ons capabilities. But we really wanted to focus on the core functions around key management. We did a pretty lengthy trial among our different vendors. We narrowed it down and ultimately decided that Unbound was the clear winner.

Question

What were your top evaluation criteria that ultimately led to choosing Unbound?

Unbound had the ability to work very closely with us to take feedback, both positive and negative, and resolve issues in a short period of time and support us through implementation.

Answer

Features and functionality were important but that's not really what drove it for us. One of the biggest criteria for us is the ability to partner with our vendors, especially ones that we deemed critical. Unbound had the ability to work very closely with us to take feedback, both positive and negative, and resolve issues in a short period of time and support us through implementation.

Not just as a vendor, but we wanted someone that was able to come in and demonstrate industry-leading expertise. I run a PKI team with a group of cryptographic experts that work in my organization. I wanted them to be wowed. I wanted them to feel like the company we chose not only had a great product—that's just table stakes. I wanted them to feel like the people we work with on a day-to-day basis were amazing. That's what really pulled Unbound ahead. All the way up the stack we ran into experts.

For this capability, we're not one of these organizations that is buying millions upon millions of dollars' worth of the Unbound product. Still, high-level people and experts wanted to be a part of the conversation, wanted to lend their expertise. They brought a high level of knowledge about what we were doing that wowed our team.

Then, obviously cost, making sure that this was not going to get out of control. A lot of the other platforms had really cheap entry costs but were really expensive long-term support costs, which was not the case with Unbound.

Question

Centralized PKI/key management has always sounded good, but often the speed of business has meant centralized services can't keep up with business needs. How did you avoid that problem when rolling out the Unbound services?

Answer

I have a very specialized team that's focused on it. The head of that group is a direct report to me. Effective and efficient key management has touchpoints across our entire life cycle, from something like code signing all the way up to making sure all of our applications are functioning correctly. It spans everything from making sure our SDLC is functioning correctly to assuring that our corporate website is safe and available. As the CIO, I want to make sure that that environment is up and running.

To make sure we understand evolving business needs, we do very regular reviews together. We go through a lot of detail and do a lot of testing. We also have a business partner process here at Unisys where the PKI team meets with all of our business leads and their teams to ensure that everything we're doing is meeting the business goal.

We do a lot of listens and learns. We do a lot of brown bag lunches where we just want to have conversations to hear, for example, a pain point they may be having or an escalation point they may not feel is working correctly so that we're constantly evolving. Our goal with this to be completely transparent is for nobody outside of my group to even know the name Unbound.They should not care about what product we are using or have to understand cryptography. The services should just work for them.

It's about putting in something that's really frictionless and secure so that the business leads and their teams can focus on the job at hand, which is nothing around cryptography, key management. None of that. It's about getting what they need to get their products out the door securely and quickly.

Question

Once you selected Unbound, what was the process for going operational?

That's why we emphasized the vendor's ability to really be a partner. We need to go to market and find a partner that has a product that makes what we do easier, more auditable, more sustainable, more scalable, and can give us that 24/7 confidence that we need.

Answer

I believe that if you're going to deploy an operational business capability, there are some fundamentals that have to happen every time. There has to be a dedicated person or persons within my organization from the vendor who has to be involved in every step of the implementation, especially for an organization of our size with our complexity.

We documented everything we'd done in the bake-off as lessons learned, including some of the actual config work. I had a small, but dedicated group working very closely with Unbound to get us deployed. We set up your typical Gantt milestones through the implementation with success criteria for final sign-off.

The sign-off at the time was by me because I was the CISO at the time of this deployment. Our CIO retired at the end of last year, which is why I took this new dual role. He and I both worked together to make sure that all requirements were met and there was a clear path to success. My sign-off required sub-sign-offs of all the business executives to make sure that they were getting what they needed. It was complex.

Question

Did you deploy everything at once, or was it a phased rollout?

Answer

It is a continuing and evolving phased rollout. We are continually deploying this and looking to expand our relationship with Unbound. We focused with the IT side of the house first so we could eat our own dog food before bringing in the business apps. If it did not work out, I did not want to take our organization down or cause a lot of problems. Two critical concepts for our IT services are to be frictionless and, when we deploy, to do no harm. We're not breaking the business. We're not adding costs where there does not need to be additional cost added.

Question

From what you know now, after two years of experience with providing key management services using Unbound, are there some lessons learned, things you would've done differently as you got started that you can pass on to the audience?

Answer

I think we came at this initially with a bit of blinders on. We limited our scope too much. What ends up happening, depending on the size and complexity of your organization, is, you can get past maybe milestone one or milestone two and feel good because that is showing green. But not looking far enough ahead led to delays on our side in expansion.

I recommend really making sure that you spend the time up front to understand the entire scope of your "north star" project so that you really know when you're going to claim ultimate success. That is truly key to the implementation team and the business side feeling like real business gain was realized, that you didn't stop halfway there.

Question

Is the Unbound key management capability used in a traditional data center environment only, or does it extend to cloud-based systems?

Answer

We're a majority cloud-base as it is today. We have a mixture of both. It is multi-cloud since we use more than just one cloud provider. We actually call it multi-hybrid cloud because we still have data centers for some of our projects of our environments and then tied into two clouds as well. It's a mixture. Our core PKI infrastructure, that is still on prem.

Question

Can you give us an idea of the pricing model for this?

Answer

For us, it was number of devices and number of certs, because there are certain environments where the device count doesn't really matter.

Question

What is the administrative side of providing these centralized services?

Answer

It's a limited team. We run a really tight infrastructure and security team here. We could have, theoretically, added a lot of people to that organization to get the capabilities we now have with Unbound, but the team came back and said, instead of us just expanding this group, let's really focus on centralizing and streamlining what we're talking about.

That's why we emphasized the vendor's ability to really be a partner. We need to go to market and find a partner that has a product that makes what we do easier, more auditable, more sustainable, more scalable, and can give us that 24/7 confidence that we need.

Question

While there is a lot of focus on managing SSL certificates and encryption keys for production systems, SANS has seen a big need for key management that gets integrated into app dev/DevOps. Are you seeing that?

Answer

I could not agree more. That is the primary expansion area for us. You can definitely judge the quality of an app dev organization by their demand for this. The old legacy mentality would see this as a "barrier to success" as compared to really modern app dev leaders and engineers who view this as a necessity to be successful securely. They've been our number-one driver for growth.

Unbound brought a high level of knowledge about what we were doing that wowed our team.

Question

Are there metrics you keep or collect to show business value from your investment in key management services?

Answer

Wherever possible we do quantitative analysis and reporting to show a cost-benefit analysis for the implementation. But it is always hard to quantify risk reduction, so there we use qualitative factors and comparison to industry norms.

Unbound has some really good metrics that they provide us. Again, acting as a partner, they've been very responsive in providing input to my security and risk committee presentations that have been appropriate for what I report up on the success of this program.

Question

What sort of support did you use from Unbound as you went operational?

Answer

I'm a big believer in and doing implementation projects together. I find that if a company is just going to sell me a product, then walk away, we're going to run into problems because nobody knows their product, their ins and outs, and the best way to configure, manage, and maintain the environment than the people who created it.

We really went into the implementation together. We paid for services and support, not just when we had a problem or if we had a problem, but really to do the implementation as a team. Even the sales lead, who was part of this engagement, stayed on with us through the entire implementation process. He and I were meeting weekly. When he was in the area, we would even meet together pre-COVID to have the conversations, to see where we were, to go through what he was hearing from Unbound. I would go through what I'm hearing from my side, just to make sure things stayed on track. We did it as a partner.

We have a procurement organization that does an amazing job with doing the analysis and evaluation through our third-party risk management program. We put Unbound right through the TPRM program that we have, which is everything from NDAs to MSAs to SOWs, to having them fill out and maintain certain STIG questionnaires and doing all of the normal stuff big companies require.

Unbound was one of the few organizations I deal with that never had an escalation of non-responsiveness. They took it really seriously. I was very excited, because for a lot of large corporations, how well a potential partner gets through your procurement process, to me and to a lot of organizations, really shows you what kind of company they are. If they can't get through my procurement process, how are they ever going to help me do a deployment with this organization?

Unbound was one of the few organizations I deal with that never had an escalation of non-responsiveness. They took it really seriously. I was very excited, because for a lot of large corporations, how well a potential partner gets through your procurement process, to me and to a lot of organizations, really shows you what kind of company they are.

Question

Final question: Is there anything I didn't ask that you'd like to bring up, that you think is important about your use and experience?

Answer

I would say the one thing that we didn't discuss that is a key criteria for me when determining who we're going to partner with is how innovative that organization is. I'm looking for companies and partners that are pushing the boundaries of what is possible in their world, in their scope, be it encryption, email, whatever the area is.

When you're having the conversation, talking to them not about what they built or what they built six months ago but what they're building and where they're going and why, I think lends itself to a successful partnership because in the IT and security world, if you roll it out today, when it goes live, you're already behind.

If the company you're partnering with is the same product but they're doing these little point upgrades on a regular basis, minor little features, or they're doing a twice-a-year feature upgrade that doesn't really give you a lot, then to me, that will put you behind the times. I'm looking for partners and organizations that are driving us instead of the other way around.

I really felt like Unbound has been doing that. Even the meetings I have today with some of their executives, when we get on calls it isn't about it would be great if you did this thing we launched three years ago, but it's talking about where they're going and why we should catch up to them. That is a very powerful conversation to have with a partner and something that excites me and my organization.

About Unbound Security

Unbound Security is the global leader in cryptography and empowers enterprise customers worldwide to confidently secure, manage and authenticate all critical business transactions, information, identity and digital assets – anywhere, anytime. Unbound Security CORE is the enterprise platform of choice for secure key management, trusted by many of the world's largest banks and Fortune 500 companies. Unbound Security is a recent recipient of the Deloitte Fast 500 award and is headquartered in New York, with research and development facilities in Tel Aviv. Learn more at www.unboundsecurity.com and follow us on LinkedIn and Twitter.

About SANS WhatWorks

SANS WhatWorks is a user-to-user program in which security managers who have implemented effective Internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned.