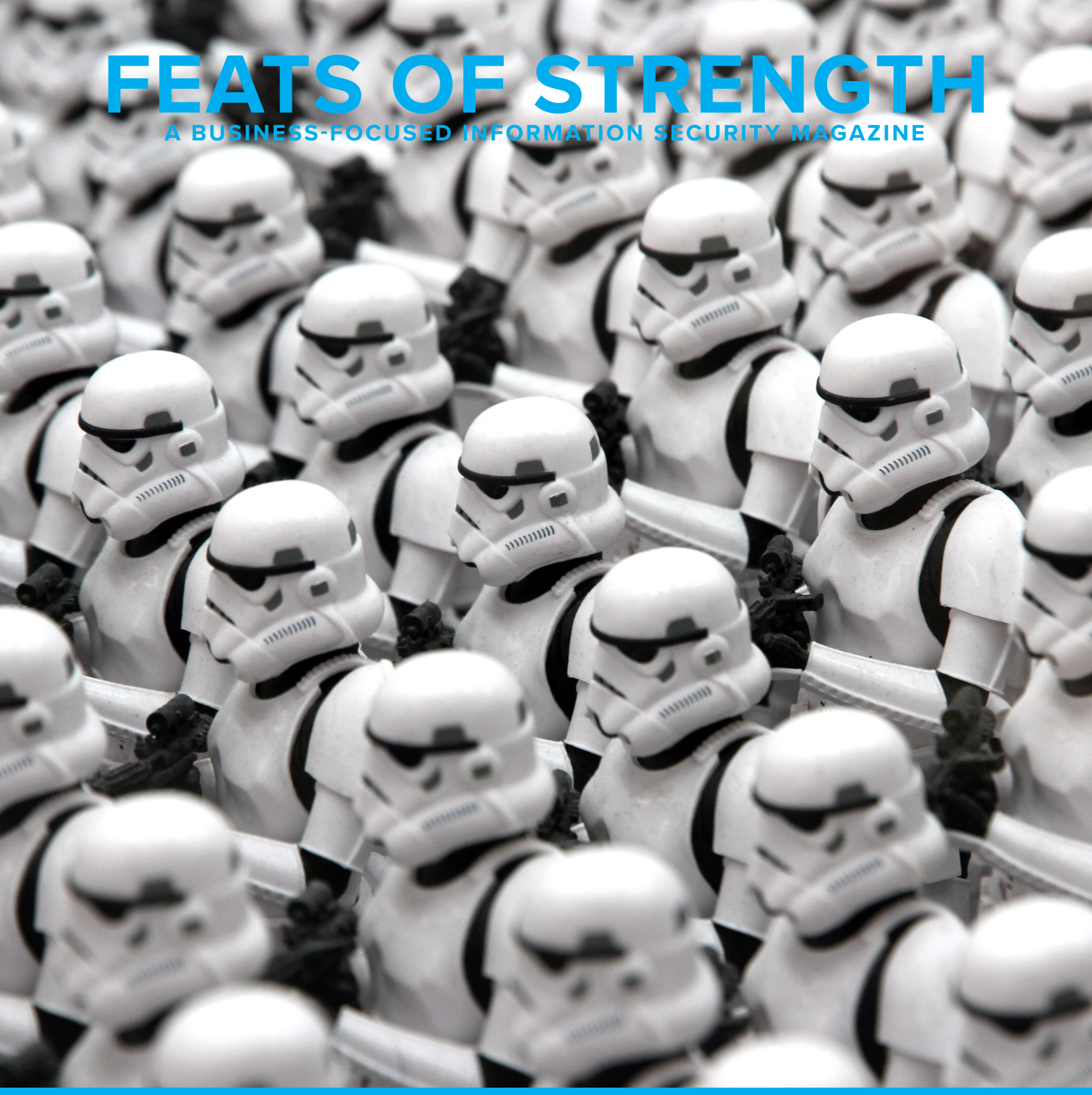
FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE



CLEARING THE SECURITY PRODUCT CLUTTER

When everything looks the same, how do you invest in new technology?

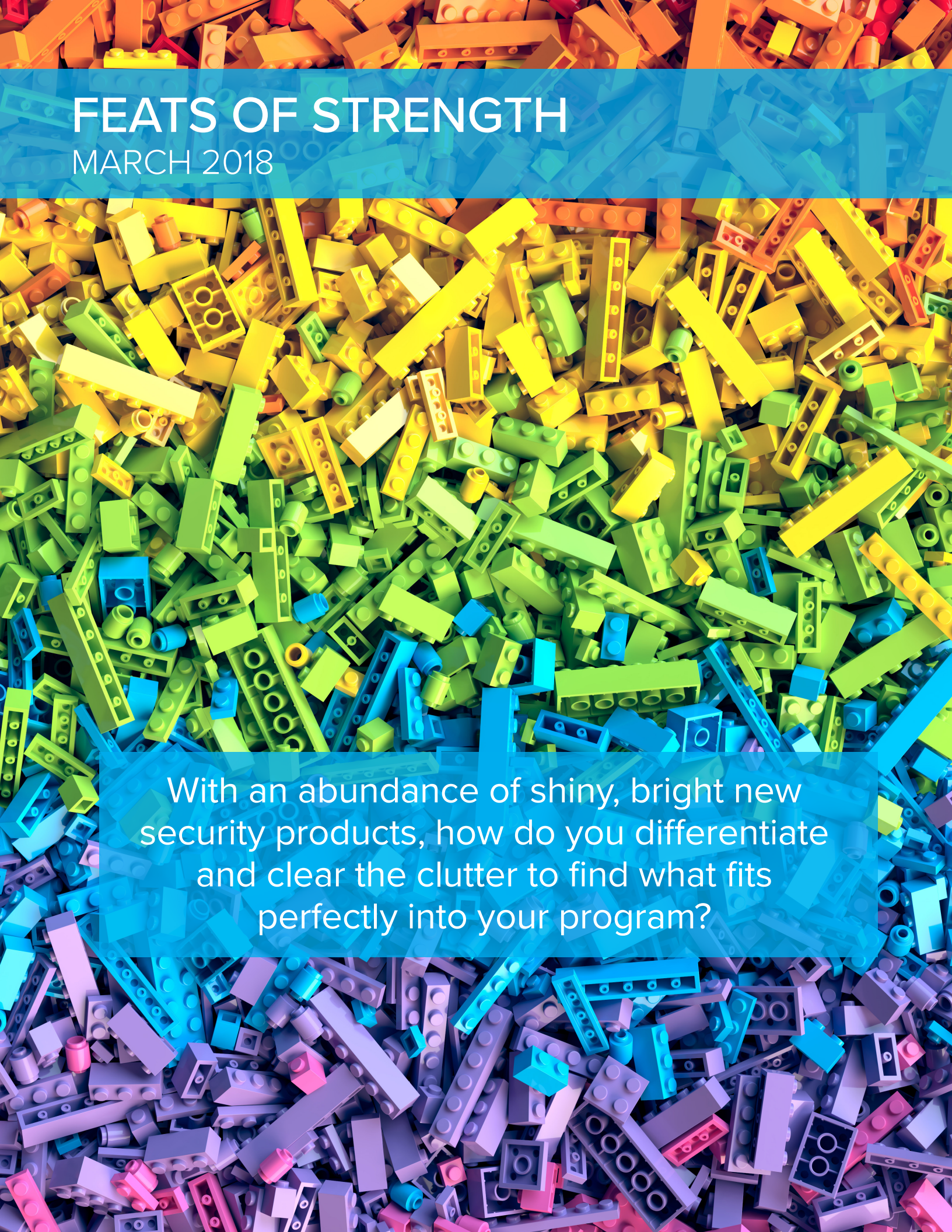
March 2018

WWW.KLOGIXSECURITY.COM 888.731.2314

K logix
Confident information security

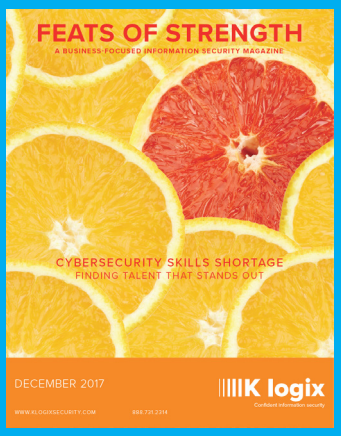
FEATS OF STRENGTH

MARCH 2018



With an abundance of shiny, bright new security products, how do you differentiate and clear the clutter to find what fits perfectly into your program?

TABLE OF CONTENTS



To view past issues, visit:
www.klogixsecurity.com/feats-of-strength

Magazine Created By:

K logix

Magazine Contributors Include:

Kevin West
CEO, K logix

Katie Haug
Director of Marketing, K logix

Kevin Pouche
COO, K logix

Stephanie Hadley
Content Manager, K logix

Marcela Lima
Marketing Coordinator, K logix

Contact Us:
marketing@klogixsecurity.com
617.731.2314

We provide information security strategic offerings, threat and incident capabilities, education/awareness, and technology services. We craft our services to address specific customer and industry challenges. One of the ways we do this is through our thought leadership, business-focused publication Feats of Strength. Through 100+ CISO interviews, we extract trends in order to provide services that align business to information security.

LETTER FROM

KEVIN WEST

CEO

YOUR PROBLEM IS OUR PROBLEM

Daily, I hear differing answers about the number of security products in the marketspace. They vary from 1,000 up to 2,500, depending on who I speak with.

The barrage of security vendor calls CISOs receive is almost unfathomable. On a regular basis, they receive calls from companies boasting the next greatest product that will make their lives easier.

The uptick in security companies stems from 2017 marking the largest amount of VCs funding cyber security in history. With cyber incidents making headlines such as Equifax and Uber, the world has taken notice and smart entrepreneurs continue to capitalize on this profound awakening into the value of protecting organizations.

The interviews we conduct with CISOs to feature them in our magazine includes many discussions around this topic and we hear the same thing. They are often confused on how to differentiate between vendor messaging and they refuse to rely on industry publications as a source for unbiased information about products.

My message to CISOs is: your problem is our problem. I too receive countless calls and messages from security vendors wanting to partner with K logix. And I too see a lack of accountable, agnostic and extensive research to differentiate between the cluttered marketspaces.

This challenge raises two questions - with all the clutter, how do you separate the signal from the noise to make solid decisions? How do you know when you need to invest in a new solution versus operationalizing what you already have? We set out to answer these questions.

SEPARATING SIGNAL FROM NOISE IN A CLUTTERED MARKETSPACE

Sometimes relying on the opinion of your peers for making technology investments is not enough. And while we know this is the approach most CISOs take, we sought out to find a solution to sort the signal from the noise in cluttered marketspaces.

We created a charter to agnostically evaluate, analyze and test security products in different marketspaces in order to provide the security community with our results. Many teams lack the time to painstakingly understand the business and technical requirements for a new product while being able to pair that with a sound evaluation process.

We started with endpoint security, and to-date have evaluated seventeen endpoint security

products over a two year period. Our second testing area was the Cloud Access Security Broker marketspace and we spent six months testing eight products. Our testing is weighted and scored dynamically based on specific use case requirements.

OUR GOALS ARE SIMPLE

My advice to CISOs is to save themselves time, money and team effort by leveraging agnostic third party research. Here's the benefits of doing so:

Eliminate the noise: Save time and money evaluating products that don't meet your business and technical requirements.

End user impact: Understand the impact various products might have on worker productivity and performance.

Efficacy: Understand efficacy performance levels for the different solutions, and what dependencies those rates are based on.

Time to Value: Spend weeks completing an evaluation that could take your organization many months to complete.

Board-level Preparation: Ensure you have evidence-based documentation to support the findings, enabling security leaders to confidently present to the Board for justification and approval.

BEFORE INVESTING, EVALUATE

If we take a step back, CISOs must keep in mind that before addressing the cluttered marketspace and investing in new technology, they need to understand the importance of evaluating all products already in their security programs. Many solutions are purchased to solve a point problem, without considering the impact to operations, overall risk landscape and total financial allocation.

Recently, a K logix customer with eighteen security technologies wanted to gain a holistic picture into their investments from an operational, financial and risk perspective. After speaking with them, they realized they significantly lacked the time, people or process to evaluate their investments, yet they required justification for new technology product purchases.

K logix interviewed security leadership and technology caretakers and implemented our strategic investment evaluation process. Then, operational maturity scores for each product were determined, technologies were mapped to alignment with SANS CIS and the financial allocation for each SANS CIS were reviewed. This presented the customer with a picture into what areas of their investments they needed to consolidate, where divesting in investments was key to saving budget and areas that required investing in new technologies to meet alignment with control areas.

In research done at K logix, only 24% of organizations who conducted an assessment of their security investments were fully aligned with the most critical SANS CIS areas one through five. Furthermore, on average, organizations saved 20% of their budget by divesting in products. This enabled them to save money and time, and make justified budget decisions in any new investments.

WHAT WE'VE LEARNED

There's a chance the cyber security startup bubble may burst or lessen in the next few years, yet the trail of clutter will remain a challenge for many security leaders. The confusion in the market came through loud and clear from our CISO community, and we established agnostic research and testing processes to address this. Our Internal Research Department has tested the Endpoint and Cloud Access Security Broker marketspaces and is currently undergoing testing of the privileged access management space.

We also heard from CISOs about how they needed to operationalize and concisely understand their current investments before investing in any new products. Born from these challenges came our Security Investment Assessment.

Ultimately, we understand security programs may be overworked and tight on budget. We aim to collectively collaborate with them to understand their business and technical needs, then help them achieve their goals for budget justification, executive alignment and limited impact on their teams' time. The CISOs we featured in this issue discuss many of these challenges. I hope you enjoy reading this issue of Feats of Strength and if you face any of these challenges, reach out to let us help you strengthen the business of information security in your program.

KEVIN WEST is the founder and CEO of K logix, a leading information security company based in Brookline, MA. K logix helps create confident information security programs that align with business objectives.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

SHAUN BELDERS
CISO, BBDO

HEADQUARTERS: New York City

EMPLOYEES: 15,000+

ANNUAL REVENUE: $1.78 Billion

ADDRESSING SECURITY IN A CREATIVE ENVIRONMENT

Shaun Belders is the new CISO at BBDO Worldwide, one of the world's largest advertising agencies. As the agency's CISO, he is tasked with building a mature security program to effectively support the company's creative workforce, inspire confidence from agency clients, and improve productivity.

Belders credits his MBA with preparing him with the right mindset to achieve these objectives. He says, "There needs to be a strong tie between security and business. As an industry [information security], I think we are getting there. We are starting to see this line of thinking trickle down from CISOs to lines of business managers. Security can, and should, align with business. It can be a competitive advantage, and a productivity enabler."

In the position of CISO at BBDO Worldwide for less than one year, Belders already understands how security plays a vital role in revenue and customer growth for the agency. As Belders explains, "BBDO relies heavily on name and brand reputation. If we do not have the security that our clients require, or if they are not confident that we can protect their marketing data, they will quickly turn to our major competitors. We can be the best advertising agency in the world - and I think we are - but if we cannot prove security effectiveness to our clients then we will not win their business."

The importance clients place on BBDO's security posture incited Belders to solidify security as a competitive advantage. He says, "I've been involved in client reviews in the past, and security controls, or lack thereof, are absolutely why a business would choose to work with you or not."

BRINGING MATURE SECURITY TO A CREATIVE ENVIRONMENT

Before joining BBDO Worldwide, Belders met with the agency's CIO and CFO to understand the company's commitment to security. In those conversations, it became clear to him that the company also understood the critical importance of maturing their security program. "In those initial conversations, I tried to gauge their commitment level, and understand what their response might be to my recommendations. I came out of those meetings feeling they would be receptive to my insight."

"My number one objective at BBDO is driving the maturity

"There needs to be a strong tie between security and business. As an industry [information security], I think we are getting there. We are starting to see this line of thinking trickle down from CISOs to lines of business managers. Security can, and should, align with business. It can be a competitive advantage, and a productivity enabler."

of our program. When I came onboard, the program was about two years old, and largely client-driven," Belders comments. He says since BBDO is an advertising firm, they were not as regulated or as focused on security as his previous employers. For the first few months, Belders has focused on covering the basics - improving security hygiene, deploying basic toolsets, and updating policies.

While Belders may be a first time CISO, he is a security veteran with experience in the private sector, previously at Bloomberg, in the defense/intelligence industry, and as a security professional running the firm he started with a friend before leaving to join Bloomberg. He says one of the biggest challenges in any new role is understanding the political dynamics of the company. "I need to understand who the different players are and make sure that I am interacting appropriately with all of them. There is a learning curve to understanding the specifics of any organization."

Process and technology also play a large role in BBDO's security efforts. In terms of process, one of the first things Belders is looking at improving is security during the employee onboarding and off-boarding processes. With regards to technology, Belders is assessing systems already in place and identifying gaps.

"In the first few months as a new CISO, you have to understand the many aspects of information security and that there will be gaps in each domain. You cannot just focus on one. You need to make a list of observations and prioritize. For example, are there controls that are completely missing?"

MOVING TO THE CLOUD WITH SECURITY FROM THE GROUND UP

Belders says "working with the business as opposed to being an outside force" is critical to the success of his program.

For example, at BBDO there is a strong push to the cloud as the agency embraces digital transformation. He says, "The business benefits are clear, and I understand that. There is significant cost-savings and increased speed of execution. For me, it is important that I am right there at the ground floor of those conversations with the CIO and IT team. My focus is on helping them move to the cloud securely."

Belders continues, "It is easy to get CFO buy-in for the cloud because he can plainly see the cost savings. But digital transformation requires an additional layer of security. We already have on-premise security, but the cloud is completely different."

"At BBDO, we are such a mobile workforce. We rarely issue desktops and even then, it's usually in addition to a mobile device. Creatives like to move around and they like their Macbooks. Because we are so mobile, we are already cloud-focused. We use collaboration tools like Slack and Microsoft Teams to drive productivity. In an ideal world, we will have nothing on premise anymore. So, the question is how do we keep track of everything and secure what we need to secure? There is no longer any trusted network."

He explains, "At BBDO we are in a good position since we are starting our digital transformation with security in mind. It is much easier to drive effective security when you are in it from the beginning."

Belders goes on to say the security industry in general still has work to do in regard to appropriately addressing digital transformation. "We have toolsets for basic compliance, but with regards to securing the whole domain I think that there is not yet a complete security strategy for the cloud."

TACKLING CHALLENGES WITH THE HELP OF PEERS

Whether he is tackling the challenge of securing BBDO's digital transformation, or identifying the best technologies to mature the agency's security posture, Belders relies heavily on his peers inside and outside of the company for guidance.

"Internally, I have a great relationship with our Director of Infrastructure, who has been with the agency a long time. He helps me understand the technologies we have in place, and identify issues of concern," says Belders.

Externally, Belders leans heavily on other CISOs, both those he meets at small events, and those he has known for some time. He connects with them regularly in person and on dedicated Slack groups to help keep abreast of industry innovations and to share best practices in a safe, confidential manner.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

DAVID FAIRMAN
CISO, ROYAL BANK OF CANADA

HEADQUARTERS: Toronto, Canada

EMPLOYEES: 85,000+

ANNUAL REVENUE: $35.2 Billion

"We do have regular updates with our board; our goal is to give them a level of comfort that we're covering our bases and that we're measuring and managing that risk for them. It's about keeping them current so that they are able to support and challenge us."

- DAVID FAIRMAN

MAKING A MARK ON RBC'S CYBER SECURITY PROGRAM

Into his role as Chief Information Security Officer at the Royal Bank of Canada for three years, David Fairman had the opportunity to come in and build a business-focused cyber security strategy. He states, "It was an opportunity for me to take a global role at a large financial institution and really build that program ground up."

Fairman exemplifies a concise business-enabler and confident leader, who came into the organization with a strong priority of gaining deeper engagement with business leaders. He explains, "It's about understanding and having more dialogue, better relationships, more insight into what our business partners are trying to do and how they're thinking in terms of how they're operating. Understanding how we can be proactive by helping them achieve their goals, so they want to move into a new market and want to launch a new product. Then we're fully armed to support them."

THE FOUR PILLARS OF FAIRMAN'S STRATEGIC PLAN

After gaining clear alignment with executives and acquiring a solid understanding of the corporate mission and goals, Fairman put into place his strategic plan. His strategy consists of four pillars:

Cross-function operating model. Coming into the organization, Fairman knew it was not just a technology problem he needed to address, it was much broader and presented a clear business issue impacting processes and services. Multiple parties within the organization had to come to the table to recognize the role they play across the entire security program. Fairman comments, "You need to help them understand the impact their team has to the overall, bigger picture of protecting the bank."

Strategic partnerships. The first focus for Fairman rests on large vendor strategic partnerships who help the organization build cyber security capabilities. These vendors are leveraged to implement capabilities to protect customers, shareholders and employees. The second element is understanding the startup community and becoming an early adopter in key technologies to help drive their roadmap and maturity. The third part is partnerships with academia in terms of exploring research projects that may help solve emerging security challenges. The fourth is strong ties with law enforcement and intelligence agencies.

Talent and culture. Fairman strongly supports his team, comprised of positive, energized people who understand the core value resting on customer trust. He continually develops and matures this culture, and his team, by enabling a fast-paced, exciting and leading edge cyber security program.

World class cyber security capabilities. Fairman built the program around the NIST cyber security framework with an emphasis on aligning to the five pillars of identify, protect, detect, respond and recover. In regard to understanding the maturity of the program, he says, "We need to understand where we want to grow or end, and what our endpoint looks like. I'm very passionate about the API economy and providing services for our business partners and internal teams, so they can move and be as agile as they need to be, without us holding them back. We need to give them a solution."

BOARD ROOM AND BUDGET ENABLEMENT

Throughout his tenure at the Royal Bank of Canada, Fairman developed a two-way dialogue during board meetings, and empowered board members to recognize security as a true enabler. Presentations consist of a threat landscape overview, top risks affecting the bank, progress with strategic goals and the current status of key metrics.

"We do have regular updates with our board; our goal is to give them a level of comfort that we're covering our bases and that we're measuring and managing that risk for them. It's about keeping them current so that they are able to support and challenge us," explains Fairman.

When it comes to budget, Fairman advises other CISOs to make a clear case for explaining the impact in a business context. He encourages CISOs to talk about critical business processes or the critical assets at risk, and the revenue generation or criticality of the process that might be at risk. For board and executives, this approach provides a real-world case – it's meaningful.

"I think it's really beneficial to have that open conversation, which certainly helps define the budget needed in order to be successful," comments Fairman.

PHASING INTO FUTURE GROWTH

Currently in phase two of his three to five year cyber security strategy, Fairman designates a clear priority on continuing to mature his four pillars and build world class cyber security capabilities to protect the bank.

Clearing the Security Product Clutter

"You clear clutter through understanding where the industry is seeing trends. You need to understand the ecosystem and see what other large organizations are doing. Once you see a few other organizations down the path of a particular capability or solution choice, that probably says something in itself. Secondly, we have multiple innovation and accelerator labs that we leverage to test specific use cases. We have innovation labs in Orlando, New York, Toronto, San Francisco, and we are now starting to delve into Israel."

CYBER SECURITY VC FUNDING: IS THE BUBBLE ABOUT TO BURST?

ADDRESSING THE SILVER BULLET SYNDROME

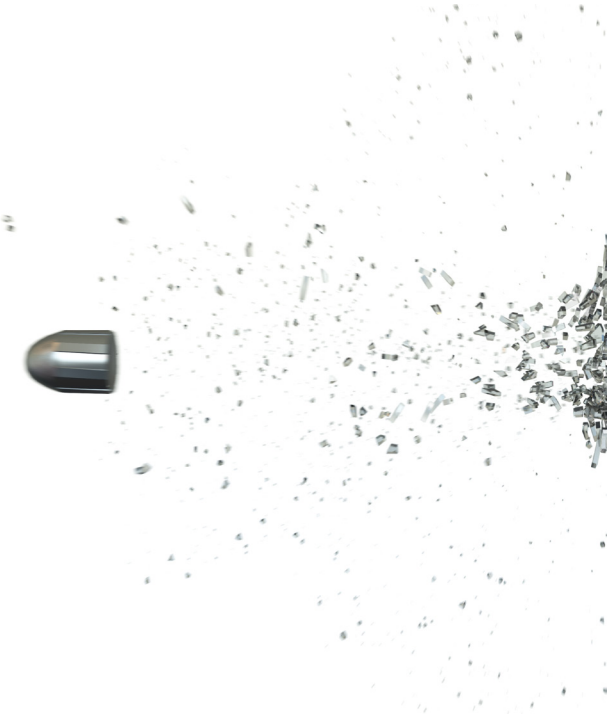
By **Katie Haug**, Marketing Director

The cyber security industry boomed in 2017. Globally, cyber security investments ranked third in overall VC spending. According to Pitchbook*, VC firms invested $7.6 billion in cyber security companies last year, up from $3.8 billion in 2016. The number of cyber security-related investments jumped to 548 in 2017 from 467 deals the year before.

Average investments typically range from $500,000 to $5 million, however in 2017 investments were larger funds at faster rates.

As a result of the increased emphasis placed upon cyber security and strong growth of the market, Gartner predicted global cyber security spending to reach $96.3 billion through 2018.

However, many experts believe this unprecedented boom is beginning to produce a 'silver bullet' syndrome with overvalued startups and a strong market correction on the horizon.



WHY THE BOOM?

2017 marked the largest amount of capital funding in history for the industry. The evolving technology ecosystem has become ripe for the taking as billions of funding dollars are at play.

Cyber security headlines rocked the news in 2017, including WannaCry and data breaches at Equifax and Uber. It was clear that VC firms took notice more than ever before.

VCs see potential to influence the competitive nature of startups they invest in, thus reaping clear financial benefits. In an interview with InfoSec Magazine, Venture Capitalist Nazo Moosa says, "Entrepreneurs often operate in the here-and-now, becoming very tactical and may need support to gain an overview of where markets are heading. Our ability is to sit above that and give a better view of the competitive landscape. It's about strategic focus, support of merger and acquisition activity, growing the contact base, helping to commercialize and scale their business."

THE VC PLAYERS

Investors are following the money and corporations and governments are increasing their spending on cyber security amid growing concern about vulnerabilities and breaches.

According to CIO Dive*, the four largest cyber security

VC firms invested **$7.6 billion** in cyber security companies last year. Up from **$3.8 billion** in 2016.

The number of cyber security-related investments jumped to **548 in 2017** from 467 in 2016.

fundings in 2017 ranged from $100 million to $180 million, and NEA and Accel were the most active investors with nine deals each.

Most active investors in cyber security deals since 2013:

1. **Accel**
2. **New Enterprise Associates**
3. **Bessemer Venture Partners, Intel Capital**
4. **Andreessen Horowitz, Sequoia Capital**

While many venture firms reap great profit from these startups, there is potential downside and risk due to the growing number of startups to choose from. In an interview with CNBC, Rick Grinnell of Glasswing Ventures says, "One of the biggest threats to cyber investors is that their technologies may be proven to have holes or be exploited. If they are, their value essentially becomes negative."

SILVER BULLET SYNDROME

Many experts believe a market correction is on the horizon in this overly crowded market. A large number of startups are now recognized as overvalued with potentially overpriced products.

In an interview with the Financial Times*, Norman Fiore, general partner at Dawn Capital, a venture capital group that is a keen investor in cyber security start-ups, says, "I don't want to call it a bubble, but you did have valuations that ran away. You had lossmaking businesses growing fast but burning through lots of cash. There has been a move back to looking for companies with sound business models."

Considering the year ahead, investors may be forced to painstakingly examine some of the more inexperienced cyber security startups before making projections about performance. There is a clear 'silver bullet' syndrome impacting the market and the best advice for VC firms is to avoid hype products at all costs.

Alberto Yepez, Founder of Trident Capital Cyber Security, the largest global capital firm focused on cyber, shares what he takes into consideration before investing (excerpt from an interview with Panda Security Mediacenter*):

"We look at five different areas — so this is a good note for entrepreneurs!

Number one, we're really market driven. We like to get a sense of what the areas are where no commercial technologies exist so emerging solutions can be funded. So we look at, how big is the market?

Number two, we look at the intellectual property — how hard it is to replicate the solution.

Number three we look at the go-to-market strategy — how the company can scale not just by selling one at a time, but by creating alliances. Which is one of the basics to reach a global audience.

Number four we look at the team — whether the people have the experience, the context, the knowledge, and the relationships to be successful.

And number five, we often look at the co-investors. The investor group is important, because companies go through several iterations and several fund-raisings, so you need investors that are committed to support a company through all this."

*Sources:

Pitchbook; 2017 Year in Review: The top VC fundings & investors in cyber security.

Financial Times; Investors cool on cyber security start-ups that promise silver bullets.

Interview from Panda Security Mediacenter; Guest Collaboration with Alberto Yepez

CIO Dive; 2017; As VC investment booms, AI and cybersecurity startups rake in the big bucks

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

DAN BOWDEN

VP & CISO, SENTARA HEALTHCARE

HEADQUARTERS: Norfolk, VA

EMPLOYEES: 28,000

ANNUAL REVENUE: $6 Billion

"I knew executive leadership and the board wanted me to come in and be successful. I was assured I would be given both authority and support to make the program effective. I was ecstatic about this opportunity and all conversations about the program were very easy. From the beginning we talked about what needed improvement and what we could do about it."

- DAN BOWDEN

BUILDING A SECURITY PROGRAM AND TEAM FROM THE GROUND UP

Dan Bowden, vice president of information security and CISO of Sentara Healthcare for over one year, had the opportunity to rebuild Sentara's cybersecurity program after significant transition of IT leadership. His current role marks his second time building a program and he continues to leverage previous experience to make an impact at Sentara. He comments, "This opportunity at Sentara appealed to me because I wanted to work in a larger scale health system and extend my professional network."

In his first interview and exposure to Sentara, Bowden began to map out how the security program rebuild would proceed. He says, "I knew executive leadership and the board wanted me to come in and be successful. I was assured I would be given both authority and support to make the program effective. I was ecstatic about this opportunity and all conversations about the program were very easy. From the beginning we talked about what needed improvement and what we could do about it."

These initial conversations included his CIO, who Bowden describes as a business-minded, tech strategy expert. He continues, "Sentara's CIO is a brilliant technologist who brings a different cadence to the role." Strong alignment with executives, paired with emphatic support from the entire organization, provided Bowden a solid foundation for making his mark.

CREATING A TEAM IN A COMPETITIVE JOB MARKET

When Bowden first started, he was basically the only person on the information security team, however, he developed a strong plan to overcome this challenge. He says, "My biggest concern was how we would staff the team. Virginia is a very competitive market, with defense and military contractors competing in the same tight talent pool as us."

Bowden's solution was simple and clear – to grow his team organically. He explains, "I recruited a few team members from IT at Sentara to convert to information security. I also developed a pipeline of student staff from Old Dominion University, Regent University, Thomas Nelson Community College and Tidewater Community College."

He continues, "I leverage my experienced people to work on complex risk-laden tasks, while also developing the skillset of the student staff who can work on more basic day-to-day needs. The ability of the students to support us will expand as we grow with them." Currently, Bowden's team includes twenty full-time employees and ten student staff. He expects the team to grow twenty percent during each of the next two years.

Investing and growing the future cyber security workforce is important to Bowden. He encourages CISOs to tap into this well of trainable and adaptable talent. He explains, "We all know there is a shortage in the cyber security workforce, but what are we doing to fix the problem? At Sentara, we are developing student staff into the future workforce. I encourage everyone who is worried about the skills shortage to get involved with university students, and even get involved with STEM programs at the high school level. Some people believe artificial intelligence will replace everything and solve the problem. I think we will always need intelligent people exercising good judgement."

ADVICE FOR NEW CISOS BUILDING SECURITY PROGRAMS

Since he successfully architected two security programs from the ground up, Bowden offers advice to CISOs embarking on similar journeys. He says, "First, understand how the organization identifies and manages risk. Understand which data needs to be protected and how well-prepared the company is to deal with major incidents. Those are the things that should drive your early conversations."

Soon after his arrival, Bowden and his team rolled out two-factor authentication to 60,000 users in 120 days. He says the experience was a complete team effort involving the entire organization. He remarks, "Marketing and communications were heavily involved in the roll out. It was not about the technology, it was about the entire organization buying into why we needed two-factor authentication and supporting our efforts. Early successes like this are important to increase confidence and help to establish that information security is an organization-wide effort."

Now that the initial set up of the program is complete, Bowden and his team are focused on managing risk and supporting business goals. "Like others in the health care industry, we are working to provide better service to patients and plan members. Part of that is rolling out a digital mobile platform to get more, and better, information into our patients' and members' hands," he says.

Bowden ensures the actions of his team and decisions they make are directly correlated to supporting the overall business goals and priorities. He comments, "Because of the complexities within health care, our digital mobile platform is a very iterative process, and as the security team we have needed to be very flexible. Our priority is to make sure that the business can keep advancing as we continually assess risk in an efficient and timely manner."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

SHANNON RAMSAYWAK

CISO, KIND

HEADQUARTERS: New York City

EMPLOYEES: 800

ANNUAL REVENUE: $727 Million

"Security was one of many risks to the business the board identified, and made it a point for the business to address. So, it was clearly a board-sanctioned directive to start a security program."

- SHANNON RAMSAYWAK

OFFENSIVE TO DEFENSIVE SECURITY

A little over two years ago, Shannon Ramsaywak undertook the first-ever role of CISO at KIND, the healthy snack and granola bar company based in New York. Two pivotal things drove Ramsaywak to join the rapidly expanding organization – building a program from scratch and the full support of KIND's board. Ramsaywak says, "Security was one of many risks to the business the board identified, and made it a point for the business to address. So, it was clearly a board-sanctioned directive to start a security program."

In an incredibly brief period of time, KIND successfully expanded their global footprint and significantly grew their product offerings, yet lacked an established security program. He says, "I was brought in to bring the business from an all offensive approach, to expand and include a defensive cyber strategy. KIND grew so large, so quick because it was mainly concerned with growing the brand. However, after achieving such high growth, we found that we had many imitators and aggressive competitors we had to fend off. My role was to provide them with the defensive strategies they previously lacked."

During the interview process, Ramsaywak shared his thoughts on what type of data he planned to protect at KIND. He answered with a clear-cut description of five levels of data, as he sees it. He explains, "The first level is open data such as sharing our latest bar with the public. Second level is internal communications. Third is sensitive corporate information such as stock valuation. The fourth level is regulatory, so anything that requires a mandate or law like PCI or HIPAA. The fifth level is the formulas of our bars, including our supply chain, from the initial purchase to our end product. That's very sensitive, so those are the things that we're looking to protect most."

BUILDING BLOCKS OF A SECURITY PROGRAM

Ramsaywak's first phase of security initiatives was the "black and white" phase, addressing the most critical items. He determined the risks to the organization, then discovered the risk exposure level. These levels included critical, high, medium, low and very low risk. He next approached the business and laid out the risks, and how they correlated to a specific risk exposure.

"What's your risk tolerance posture? Are you risk adverse or are you risk tolerant? Once we found that, we married those two ideals into how we remediate. The very first directive I got from my boss was that we are very open when it comes to our user-base and our team members going to the internet and using tools to collaborate. But we are extremely risk adverse when it comes to the things that matter most to us," explains Ramsaywak.

He says, "Segregation, segmentation, antivirus, endpoint protection, firewalls, VPN, all of the black and white stuff is complete." He originally anticipated the first phase to take up to three years, but due to diligent work and board and C-Suite support, completed it in two.

The next phase for Ramsaywak includes transforming a security operations and security hard-line approach into a risk program. He comments, "Last year, we started the risk program and we're doing an assessment of all the departments and systems. We started with our critical departments, our New Product Development (NPD), HR and Finance departments."

UNDERSTANDING COMPANY CULTURE

The dynamic, young culture at KIND represents a "plugged in" workforce, who work off laptops and mobile devices. Ramsaywak realized it would be challenging to protect his employees and company data in this type of environment, which is a stark contrast from the highly risk adverse and "locked down" state government agency he came from. He explains, "What I had to do was understand the culture and then take a step back from the technologies. I had to come up with a concept of protecting the organization while still allowing the organization to keep its' ethos of the way it does business. And in that, I discovered that everyone wants to collaborate in real-time around the world which means work in the cloud, Google Docs, Dropbox, etc. It's not really the idea of Google or Dropbox, it's the idea of a tool that people can use anywhere to transfer information and get things done instantly."

After an initial discovery phase, Ramsaywak began to build out concepts to fix and enable, without limiting his employees. He comments, "I needed the concept to solve the issues the company had, and do it securely, so it wasn't a matter of coming in and implementing only what I knew. I think we have to allow ourselves to grow and be a little bit vulnerable in order to be better and to deliver better to the organization."

Not only did Ramsaywak implement policies and technologies that properly aligned with the company culture, but he started a heavy security awareness training campaign. Beginning with executive support, he achieved buy-in by emphasizing the criticality of their users being more educated and better aware. He says, "Our awareness program paid off in dividends because our end user infection when I first started was 6.7 a month, out of a group of 400 people full time and another 400 part time. Our infection rate has dropped to .15 a week or .5 per month. So, we've dropped from seven people per month to one person every two months."

Ramsaywak continues, "Focusing on where you have the greatest needs, whether it's your end user, your configuration or your vulnerabilities is very important. I found focusing on the end user in this day and age, with everything being open and bringing your own device, is one of the most effective ways."

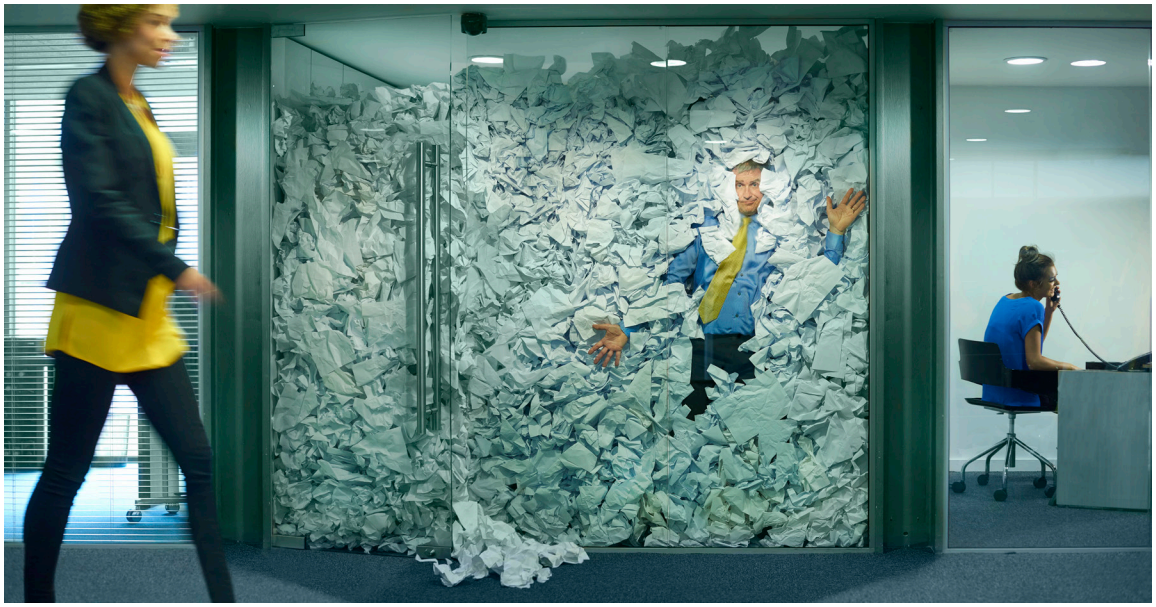
FOCUSING ON FUTURE GROWTH

Once per quarter, Ramsaywak participates in an Enterprise Risk meeting along with the CEO, COO, CFO and General Counsel. He provides valuable updates on progress within their risk program, and continues to align himself with key executives. They also discuss plans for growth and how security plays a role in vital initiatives.

Building out his program to ensure it keeps pace with growth goals set by the organization's leadership is imperative to Ramsaywak. He comments, "As the organization grows, we're growing with it. The company has grown by at least 40 percent since I've gotten here. KIND has a very aggressive goal by the year 2021 and I have already built out what my organization will look like for this year and then next year and the following year in order to enable the business to achieve its goals."

From the Word of CISOs:

How do you clear the security product clutter?



With over 2,500 security technology companies as of January 2018, and 2017 marking the largest influx of VC money into the cyber security market, the clutter of security products is even greater than before. Vendor messaging has become convoluted with similar pitches touting the next greatest 'silver bullet' and the top industry publications provide limited guidance. CISOs tells me the rise in number of booths at large industry conferences has become inconceivable and overwhelming.

Through over 100 CISO interviews in this magazine, I have learned a tremendous amount from the candid, insightful conversations with these leaders. I have asked almost all 100 CISOs similar questions and consistently receive a multitude of varying answers, yet there's one question I ask that constantly receives the same answer. 'Do you believe the marketspace is cluttered?'. 95% of the time the answer is vehemently, 'YES!'.

I follow-up with asking, 'what are you doing to clear the clutter and make new technology purchases?' Almost 100% say they chiefly rely on their CISO peers to learn more about product capabilities, use cases and comparative benefits. They typically combine the recommendations of peers using the product, with independent research and conversations with the infosec community at conferences or events. Not one CISO I've spoken with trusts industry publications or vendor messaging as the lone source for purchase justification.

The CISO community is powerful – these leaders often put unwavering trust and reliance on their peers for advice, mentorship and recommendations. One large component of these connections is helping clear the clutter in the security product marketspace to protect and enable their organizations. I am happy many use this magazine as an opportunity to connect with CISOs whose profiles they read, to learn more from their experiences and grow their networks even larger.

I selected a few key, thoughtful answers CISOs provided to questions surrounding clearing the clutter. As a reader, please don't hesitate to reach out if you are interested in connecting with these CISOs, or any others we have featured in the magazine.

By Katie Haug
Director of Marketing

What do CISOs look for when purchasing new products?

"Back in 2006 you could name all the mainstream security companies in a breath, but now every company that has something interesting gets VC funding. It makes things hard. For us today, I will only look at tools that I know can address a looming risk. Does the tool manage a looming risk? Can I implement this tool completely and optimize it in my environment? Is the company sound and does it have good references? Only after these three criteria are met can we move on to bake-offs and POCs," says Angelo Longo, CISO of Casino Hotel Resort

He continues, "The reality is that a lot of security products are purchased on a whim and then implementation is difficult. Sometimes results do not meet expectations. These are the systems that add little value, waste budget and create inefficiencies. I am looking for plus, plus, plus. I want to expand my ability to see and understand my architecture and understand the threats involved. If a solution cannot address that issue then it is just more noise. I want to reduce noise but add value."

What questions should CISOs ask security product vendors?

Dan Bowden, CISO of Sentara Healthcare says, "All the major product spaces are cluttered. As we become more mature in dealing with threats, vendors are introducing niche products that can do one specific thing really well. I told a vendor today, 'what you are showing me is better than what I have, but not better enough to justify going through the trouble of converting. Your product is an A+, but I have an A- product right now, and that is doing the job just fine.'"

Who should CISOs rely on to understand product differentiators?

"No one tells you where they are terrible. So, to get the truth, I talk to peers and I do as much reading as I can. I ask hard questions in the sourcing environment. Tell me what you do not do well and show me your roadmap to address it. I look for independent research. Lots of times it comes from universities. PhD students write great papers and they have no skin in the game at all. They are not funded by vendor marketing," says Tom Meehan, CISO of ControlTEK.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

ANGELO G. LONGO
CISO, RESORTS CASINO HOTEL

HEADQUARTERS: Atlantic City, New Jersey

EMPLOYEES: 2,000

ANNUAL REVENUE: $200+ Million

"I needed to understand what the business is and how it functions. What are the tools we have? How do they work and where do they fail? These are the questions I needed to ask as I moved the company to a more strategic model."

- ANGELO LONGO

MANAGING THE COMPLEXITY OF AN INHERITED SECURITY PROGRAM

"A friend says that complexity is the enemy of security," says Angelo Longo, CISO at Resorts Casino Hotel in Atlantic City, New Jersey. He continues, "I drive towards basic security in practice, so when we look at new buzzwords and marketing terms, we can understand if and how they will add value to our environment."

Longo is new to the position of CISO at Resorts Casino Hotel. He inherited a security program built by a few predecessors. As one would expect of a program with more than one previous leader, there is some redundancy of products and potential for unnecessary complexities.

Longo strives to remain intent on streamlining the program to run more efficiently. As he explains, adding the latest and newest products to the environment does not always help. "Think about a motorcycle. You can have shiny rims and handlebars but you still need a good engine. The shiny stuff may add value, but in the end the whole motorcycle needs to be smooth and stable. The rider needs to be able to handle it."

Whether Longo is analyzing new technology or existing investments, he prioritizes how those systems work and integrate with the current architecture. He also considers what they will enable in the future and constantly looks for value add. He comments, "Can these systems share data with each other? Do they integrate successfully, and do they support our five-year strategic plan?"

Longo points out the process of reducing noise may happen naturally and organically. He explains, "Look at the products that are implemented, but are not getting used.

Examine the products used by only a subset of the team. For example, we had a product implemented to help with updates but only a few people on our team used it. The old method worked better and faster. Perhaps with education or training we could have more people using the newer solution. We also have to consider that a better idea for us may be to reduce expenditures and move that product out of our environment."

TAKING FIRST STEPS IN EVALUATING A SECURITY PROGRAM

Longo came into an established security program with systems and procedures already in place, and had the opportunity to conduct extensive evaluations when coming on board. To help with these evaluations, he relied on existing team members to gain a clear picture of the environment.

He explains, "I needed to understand what the business is and how it functions. What are the tools we have? How do they work and where do they fail? These are the questions I needed to ask as I moved the company to a more strategic model. My understanding of how the organization worked was filtered through the people I had interactions with. My team is excellent, and they have been helpful in this exercise."

Longo is focused on ensuring the organization's security stack is built in a way that adds visibility and value to his program. He says, "I'm the consumer of the data these security products bring to the forefront. The operations team will operate them, but I am the consumer and I need to be able to make sense of the data as a whole."

He continues, "It is a multi-vendor product stack in the environment. I am not saying I want to move to a single vendor, but I do need the data from all the systems to be presented in a way I can consume. I need to be able to understand that if three systems are alerting me about a threat, that it may actually be a single threat."

THE GAMING INDUSTRY PRESENTS UNIQUE CHALLENGES

Traditionally, CISOs grow up in a specific industry, however Longo's eighteen-year information security career spanned many industries, from defense contracting to finance, and manufacturing. This broad experience prepared him for the different challenges presented by working in the gaming industry.

Due to heavy regulation in the gaming industry, Longo and his team report into the audit committee. Longo explains how this makes sense for the company, and fits into his overall beliefs about how security should be structured in any organization. He explains, "I do not believe information security belongs under an IT organization. You must be able to look at security policies and procedures and everything within the company, not just from the standpoint of the wires. You have to understand how the business is structured in order to secure it. If you are in the IT organization, security becomes very tech-centric and compliance becomes focused on technology, security becomes focused on up-time."

He continues, "The gaming regulations require that my position dictates framework and compliance to the CIO. That is really why I took on this role."

Longo explains how the two groups - security and operations - co-exist in this arrangement. "I set the security standards. The operations team needs to adhere to the policies and procedures. Then I audit them for compliance. I do vulnerability analysis and penetration testing. We look at various aspects of the organization to determine abnormal user interaction."

Longo recognizes the high-profile target placed on the gaming industry, both on and off-line, for attackers who see it as a cash-rich enterprise. He believes digital transformation, and the gaming industry's increasing online emphasis, will present additional security threats and challenges.

"I believe the gaming floors themselves will become more mobile than they are now. Our clients will change and people who are gambling will have different expectations. We will evolve from a geo-centric point of view to a more mobile point of view. We are going to need to provide access to mobile users to make wagers, make deposits, and accept payouts. That will be an ongoing point of vulnerability for all of us in the industry. People will target our online services in different ways."

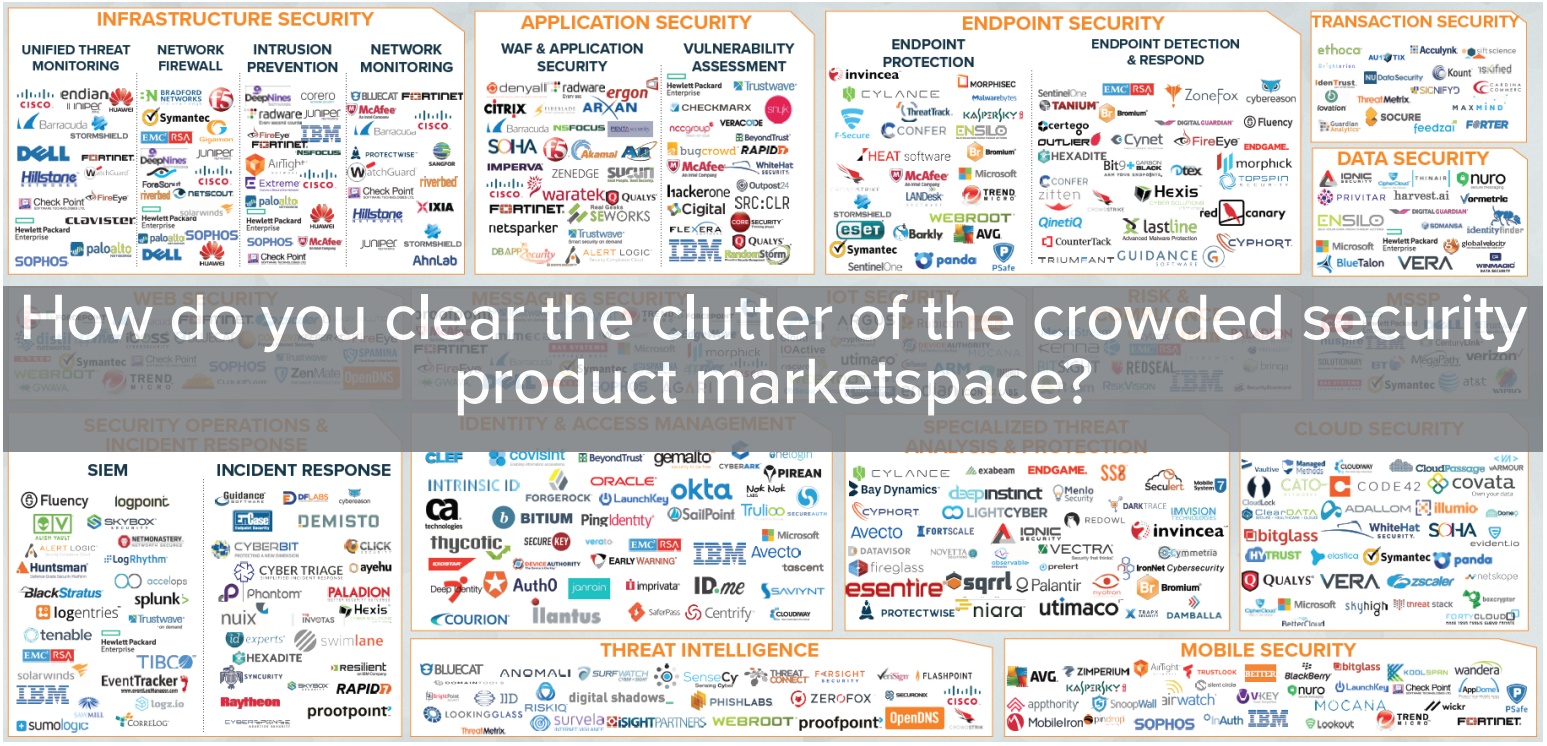
Longo believes IoT presents its own growth opportunities for the gaming industry, and will bring unique security challenges to Resorts Casino Hotel. For example, he says, "At some point in time will you be able to ask Alexa to put $500 on the Eagles vs the Redskins? Probably, yes. Given that fact, what do we need to do to enable secure, safe, and legal transactions?"

These are the types of challenges Longo would like to discuss with peers. He says his goal for the coming year is to create a community of local security leaders in the gaming industry. He says, "As we drive towards industry compliance, I want to also establish a committee or group of security professionals that works toward making information security bigger and stronger at a local level."

HOW TO ADDRESS THE CLUTTER?

We've discussed the topic in-depth, now let us show you how K logix helps.

K LOGIX DEPARTMENT OF INTERNAL RESEARCH



We've analyzed these spaces:

- Advanced Endpoint
- Cloud Access Security Broker
- Security Information & Event Management
- Identity & Access Management
- AND MORE IN 2018

Our results clear the clutter, let us help you:

- Accelerate your time to value
- Increase security efficacy without impacting IT or user credibility
- Give leadership justification to make them look as good as possible

Learn more about K logix's Department of Internal Research and Security Investment Assessment.

K LOGIX SECURITY INVESTMENT ASSESSMENT

How do you measure the impact of your current security investments?

How do your security investments align to identified risk?

Our Security Investment Assessment service helps clients assess the posture of their security product investments through the lenses of:

OPERATIONAL IMPACT	FINANCIAL COST	RISK MITIGATION
· How well investment achieves established goals	· Justification for sun-setting investment	· How well investment identifies and mitigates risk
· How well investment keeps pace with business requirements	· Justification for future investment decisions	· Alignment to risk framework score
· Operational maturity score	· Clear visibility to over/under investment risk areas	

About K logix

We provide information security strategic offerings, threat and incident capabilities, education/awareness, and technology services.
We craft our services to address specific customer and industry challenges.
One of the ways we do this is through our thought leadership, business-focused publication Feats of Strength.
Through 100+ CISO interviews, we extract trends in order to provide services that align business to information security.

To learn more about our services, visit us: www.klogixsecurity.com

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JO BENTLEY

CISO & SVP ENTERPRISE RISK MANAGEMENT, BOSTON PRIVATE

HEADQUARTERS: Boston, MA

EMPLOYEES: 764

COMPANY ASSETS: $8.1 Billion

"For us, our biggest priority and challenge right off the bat was stabilizing the relationship between the enterprise and regulatory environments to ensure a sensible approach to security."

- JO BENTLEY

"There is an underlying principle in security to do the right thing," explains Jo Bentley, CISO and SVP in Enterprise Risk Management at Boston Private. She continues, "We are not tasked to do what is convenient or what is easiest, but to do what is right for the organization."

From her first days on the job, this principle formed the foundation for Bentley's approach to security at Boston Private. She explains, "I understood that, like any financial institution, we faced security concerns. We see that quite often in security, where CISOs are hired because there are significant risks that must be addressed."

CREATING AN INFORMED ASSESSMENT

With years of experience understanding the goals and processes of CISO responsibilities, Bentley's first step after joining the company was to evaluate the environment and gather her own understanding of the challenges the organization faced. She stated, "It is important to identify the issues you can see, not as much what you hear, but what you can see from your own analysis. This is how you develop a good baseline for the program."

Armed with support and a strong team, Bentley approached establishing a solid and foundational baseline with a standard as a backdrop (SP 800-53) through leveraging three components. These included interviews, product analysis and review of regulatory outputs.

Bentley suggests concise conversations with various stakeholders as the first step in the process. These conversations should not focus on specific problems, rather on an overview and examination of the environment. Next, she says, "Perform a quick analysis of the products that are a foundation of the program. Understand what products they

are, the problem(s) they solve and their coverage." Finally, since the company is in a heavily regulated environment, Bentley and her team reviewed all audit and regulatory outputs to gain an understanding of what external parties see. She explains, "You can create a decent assessment of the security posture of the environment with those three elements."

IDENTIFYING GAPS IN A REGULATORY ENVIRONMENT

"Once the initial assessment is done, you can verify and validate the findings. From there you can identify the gaps to help you lay out a roadmap of where you need to go," continues Bentley.

She points out that many of Boston Private's initial challenges stemmed from a familiar issue for financial services organizations. "As you can guess, in many financial service companies, security starts from a compliance perspective. Since many CISOs come to security with a risk management approach, this can create fundamental issues when you start interacting with simple processes."

"For us, our biggest priority and challenge was stabilizing the relationship between the enterprise and regulatory environments to ensure a sensible approach to security."

Bentley reports into the Chief Risk Officer, a reporting structure that facilitates the company's move towards a risk-based security program. She explains, "I understand that many assume the CISO will report into the Head of Technology, but to me the Risk Officer makes more sense. Technology is a peer and stakeholder of mine, but security is not just about technology. Security provides the foundation for the enterprise to operate in terms of business functions, processes and interactions. We enable trust and safety in business using a mix of technology, process and people. So, while technology is very important to security, it is not the only entity in the stack."

TAKING A PRACTICAL APPROACH TO THE BOARD

Bentley possesses a strong background of interacting with executive and board members, which continues to evolve as she furthers in her career as CISO. She believes CISOs and security teams consistently hold an important role and perform an overall vital function in Board meetings. She feels the current industry assumption that Boards are elevating cybersecurity to a higher level may be overstated. She explains, "As much as we, as an industry, talk about aligning closely with the Board and collaborating with the Board, we have to remember that we are not the only gig on the block."

She suggests CISOs remember that while cybersecurity may sometimes be an uncomfortable topic for the Board, it is not the only topic they will cover in any given meeting. Bentley explains, "It's not really all eyes on you. Yes, we have an entry into the Board now, but I do not think we necessarily have the spotlight. In most cases there are multiple topics and risk areas the Board will discuss each meeting. Cybersecurity is just one of the things that they care about."

Given the time and bandwidth constraints of the Board, Bentley suggests letting the Board chart the course of the conversation. "In most cases, what the Board wants to talk about may not be what I want to talk about. It is my job to find ways to work that in, while being respectful of time and opportunity. Is the Board interested in what we have to say? Yes, of course. But let's not give the impression that this is easy. Cybersecurity is not the Board's only concern."

While the Board sets the agenda for their conversations, Bentley always comes prepared with reports and metrics outlining the security program's progress. She explains, "We have particular parts of our program that go to the Board for approval. Those include policies and specific programs. The Board is judicious in its review of these items, and they ask detailed questions which demonstrate they have understood and reviewed what is presented to them. They look for updates and progress on the strategy and a go-forward plan. They have informed opinions on strategy."

Bentley explains how recently, her organization's Board and executive teams expressed increased interest in understanding how security may support and enable digital transformation. The crux of the issue is speed. Bentley says, "The executives want to understand how they can embrace digital transformation in a secure environment. They ask, 'as I am trying to go fast, what will slow me down?' They wonder if security will impede the transformation."

Bentley alleviates executive concerns about security constraints by keeping her team focused on enabling the organization to move forward. "We anticipate requirements that are two to three years ahead of the rest of the organization. We listen to their priorities and clear a path forward for them. In this way, we are able to provide the organization with world-class structures and foundational elements so that the company can achieve the level of excellence expected from the overall business strategy."

We Asked Our Partners: **How Do You Differentiate in a Cluttered Marketspace?**

Here are their responses.

ForeScout is transforming security through visibility. Detailed visibility drives every aspect of enterprise security. The ForeScout platform provides comprehensive visibility into what's on the network—including traditional systems (infrastructure, PCs, laptops, tablets, smartphones, etc.), BYOD, IoT devices and operational technologies. It automatically categorizes these systems and assesses their security posture, then continuously monitors them to detect whether their security posture changes. We provide sophisticated access control to allow compliant devices onto the network while blocking non-compliant or compromised systems until they are made safe.

Today's enterprises typically have a dozen or more security products operating as independent security management silos. This disjointed approach prevents coordinated, enterprise-wide security response, allowing attackers more time to exploit system vulnerabilities. It also results in manual, inefficient processes that can't scale to address the growth of BYOD and the IoT.

ForeScout helps enterprises tear down operational silos that exist between multiple security and IT management tools. To achieve this, we partner with other security vendors to make their solutions and ours smarter by sharing information in real time and automating workflows and processes—making cybersecurity vastly more effective.

Our partner integrations, offered as ForeScout Extended Modules, use the power of ForeScout CounterACT®. These Modules bring the visibility, policy-based access controls and remediation functionality of CounterACT to many security tools that would otherwise lack enforcement capabilities. Enterprises can then share contextual device data and automate policy enforcement across disparate solutions, bridge previously siloed IT processes, accelerate system-wide response and more rapidly mitigate risks.

Okta was founded in 2009 with a unique proposition: building identity management from the ground up as a cloud-based service. Our core differentiation lies in our ability to connect people and technology, and we've grown significantly in our ability to do so – today reaching nearly 4,000 customers around the world and surpassing a major corporate milestone with our IPO in April 2017.

What specifically sets us apart? We've continued to extend our ability to enable any organization to connect any combination of people and the technologies they need to be productive. With more than 5,000 cloud and on-premises integrations in our network, Okta today has by far the broadest and deepest technology catalog in the industry. We've also added capabilities to make those connections simpler and more secure not only within an organization, but with partners and customers – and today, Okta's identity-driven approach to security establishes us as a leader in helping organizations connect, protect and manage millions of identities. And don't just take our word for it: Okta has been named a category leader by both Gartner and Forrester.

Currently, there are **over 2,500 security technology organizations**, and **CISOs often struggle to differentiate and understand value** between them.

Read how these companies **stand out**.

Centrify provides Zero Trust Security through the power of Next-Gen Access.

As traditional network perimeters dissolve, security professionals must discard the old model of "trust but verify", which relied on well-defined boundaries. Instead, strengthen security levels by implementing an "always verify" approach for everything — including users, endpoints, networks, servers and applications.

The Centrify Zero Trust Security model assumes that untrusted actors already exist both inside and outside the network. Trust must therefore be entirely removed from the equation. Centrify's Zero Trust Security assumes users inside a network are no more trustworthy than those outside the network. It presumes that everything (users, endpoints, networks, resources) is untrusted and must be verified first so that security is not compromised.

Centrify's Next-Gen Access (NGA) offers an integrated set of mature and proven technologies and capabilities — including single sign-on, multifactor authentication, mobility management, privilege management and behavior analytics — that are aware of every device, know every user, limits access and privilege intelligently, and constantly learns and adapts without impacting user experiences.

Through a unified, integrated services offering, Centrify provides identity services across applications, endpoints and infrastructure for all users, without sacrificing best-of-breed features. Organizations may consider approaching Zero Trust by implementing IDaaS, MFA, EMM, PAM and User Behavior Analytics (UBA) technologies from separate vendors, but disparate solutions leave gaps and are expensive to separately license, implement, integrate and maintain your already cluttered set of security technologies.

For more information on how you can implement Zero Trust Security across your organization with Centrify, visit Centrify.com/ZeroTrust.

Antivirus and other endpoint solutions have focused on binary and signature-based malware prevention since the 1980s—but today, attacks are sophisticated and executed in different ways. SentinelOne is shaping the future of endpoint security through its unified, converged platform that autonomously prevents, detects, and responds to threats in real-time for both on-premise and cloud environments. The SentinelOne platform tackles problems legacy antivirus and many other next-generation endpoint security solutions simply can't – and replaces legacy antivirus solutions in 80 percent of new deployments.

SentinelOne protects against all threat vectors pre-execution, on-execution and post-execution, and since it is powered by AI and machine learning, SentinelOne does not require any prior knowledge of an attack to detect and remediate. Its automated EDR capabilities can deploy rollback functionality post-execution to return a computer to a pre-infected state. The platform is equipped with a 360-degree view of endpoints and threats from inception to termination which powers forensics and policy enforcement.

The platform provides full threat hunting visibility without needing to decrypt and re-encrypt traffic as it travels across the network. This holistic approach allows for maximum prediction, detection, and response on file-based and fileless attacks online or offline, with a minimal system footprint.

SentinelOne is the only vendor in the space to offer a cyber threat protection guarantee program with financial assurance of $1,000 per endpoint, or up to $1 million per company, if it is unable to block or remediate the effects of a ransomware – taking endpoint security to the next level.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

TOM MEEHAN

CHIEF STRATEGY OFFICER & CISO, CONTROLTEK

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 59 + 300 contractors

REVENUE: Undisclosed

STARTING OFF ON THE RIGHT FOOT

Now nine months into his role as Chief Strategy Officer and Chief Information Security Officer at CONTROLTEK, Tom Meehan's positive relationships with the Board and CEO began during the interview process. He explains, "It was probably one of the more transparent interviews that I've ever had. The Board was open to discussing what they did and didn't know. There were no barriers to the discussion. It was different from what I usually experience. Many companies see cyber security as a necessary evil, but at CONTROLTEK it was quickly apparent the company wants to be as advanced as it can be for the security of customers and employees."

This is Meehan's first time as a CISO and he comes to the position with a strong background as an entrepreneur and experienced leader. He believes his transition into the role at CONTROLTEK proved straightforward and wholly supported by the organization. He continues, "While my responsibilities have changed, it is still a job that requires me to get into the weeds and understand what the business needs in order to run. I started out here the same way I have in other positions. I focused on learning as much about the business and consuming as much information as I could. I did not come in expecting to change things, but just to understand as much as I can and help the business grow."

During his first three months in the organization, Meehan focused on policy, education and security awareness. He says, "In my first 60 to 90 days I was observing the company culture and developing an understanding of what the physical security standards were, and what software and policies were in place. From there, I focused on delivering a security solution that makes our customers and in-house team feel comfortable and confident."

With almost a year under his belt, Meehan continues to emphasize a business enabling approach. He explains, "Nine months is not a long time, but I have absorbed the culture and I am establishing a balanced approach to buying product and implementing policy, procedure and ongoing education about threats to the business. I am focused on reinforcing good habits. I am working closely with the IT team to understand their strategy. I am avoiding doing anything that will cause unwarranted business disruption."

Meehan encourages new CISOs to validate their strategic plans with an additional third party. Early on, he made changes to the

security program based on his third party confirmed analysis. These changes put into place systems and procedures he knows will support the business. He says, "It can be hard to get past the ego of it for a CISO, but when you are making decisions that will impact the customer, it is important to confirm your opinions and evaluations with a trusted party. Have someone with a high degree of credibility come in and see if they come back with the same recommendations."

From a tactical perspective, Meehan is focused on security product solutions to add value and protect the business. "I'm not keeping up with the Joneses. People like to play with new toys, but I want to focus on what will really protect us. I keep apprised of new solutions by talking to peers and taking the advice of people whom I trust."

When it comes to risk, Meehan describes himself as low-tolerance, but believes risk must be measured and assessed. He explains, "In certain places, I have higher tolerance for risk because we need the efficiencies. As an example, I have a higher tolerance for risk related to the people in our New Jersey office than our staff that needs to travel to Russia or China to conduct business. We deliver location-based protections when our employees are in higher risk markets. We increase monitoring when they are there."

PROTECTING THE CEO, CUSTOMERS AND EMPLOYEES

Meehan reports to the CEO, demonstrating a shift from how most organizations structure their teams. Furthermore, the CIO reports to Meehan. He believes this structure makes sense when you consider the ever-increasing dependency CEOs have on the security program of their companies.

He says, "My role is to protect the CEO. He is highly visible, like any CEO today. I think we will see a shift in a lot of organizations where there will, at minimum, be a dotted line between the CISO and CEO. Almost all significant breaches these days lead to the CEO resigning. If I were the CEO, I would want to make sure I have all the information I need about the security program and that I am getting it right from the source."

This reporting structure makes sense for CONTROLTEK's business, and provides clear advantages for Meehan. He explains, "The first benefit of reporting to the CEO is access. We interact almost daily. I can bring my concerns right away and get a fast response. It also makes sense when we talk about education and security awareness in the company. I educate the top person first, and information flows from there. My conversations with our CEO are focused on the business and how security can impact, not impede, operations."

Meehan's conversations with the Board also put security in terms of the business. He says, "All Boards recognize cyber security is important. I make sure I talk through the business and explain how information security technology, process and procedures impact operations. What impact will this security solution have on the customer, brand or the bottom line? How do we protect everyone in the room and our customers? While Boards recognize cyber security is a technical issue, they do not need or want to get in the weeds about it."

Meehan says the Board is thoughtful and interested in hearing about the security plan. He continues, "They want to understand how the plan plays a role in managing risk to the business. They have thoughtful questions about how we balance prevention and awareness with response. Because I typically only have 10 to 30 minutes with the Board, I like to anticipate their questions and have responses already prepared."

GROWING WITHIN THE ROLE

As Meehan looks forward, he is focused on continued growth and developing his leadership skills. He plans to continue to rely on his peers and look outside of the information security industry for motivation. "Often, I speak about leadership with someone who is 25 years my senior, and holds an executive position in sales and marketing at a very large company. There are so many other ways to gain valuable knowledge. The depth of information available to us today is amazing, from what you can watch on YouTube to podcasts you can listen to in your car. Not to mention social gatherings and online platforms where we can engage with other information security community members."

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

CLEAR THE SECURITY PRODUCT CLUTTER

WHEN EVERYTHING LOOKS THE SAME, HOW DO YOU INVEST IN NEW TECHNOLOGY?

MARCH 2018

K logix

WWW.KLOGIXSECURITY.COM
888.731.2314