# FEATS OF STRENGTH

A BUSINESS-FOCUSED CYBERSECURITY MAGAZINE

# HOLISTIC CLOUD SECURITY

## REDUCE COMPLEXITY & PROTECT THE BUSINESS

### Interviews in this issue:




JUNE 2022
KLOGIXSECURITY.COM
617.860.6485


K logix

FEATS OF STRENGTH

# HOLISTIC CLOUD SECURITY

JUNE 2022

# FROM THE *Editor*

Dear Readers,

Cloud security and having a strong, holistic strategy continues to be top of mind for security professionals as businesses transform, employees work outside the office, and new threats continue to evolve. Security teams are becoming even more involved in cloud discussions, ensuring security is baked in and making a positive impact on progress. Moving to the cloud in any capacity is inevitable at most organizations, and the importance of security's role in cloud strategies is vital.

We speak with customers on a regular basis about their challenges and approaches to cloud security, and while no two programs are the same, many struggle with protecting data and users while managing multiple technologies. There are two concepts discussed in this issue of the magazine – Secure Access Service Edge (SASE) and Cloud Native Application Protection Platform (CNAPP) that address this challenge. SASE and CNAPP are key components to a holistic cloud strategy, both reducing complexity by integrating multiple technologies into one coherent platform. The end goal of both is to protect data and users as they access resources located in cloud infrastructures, providing end to end security.

In this issue of the magazine, we interviewed security leaders who share their experiences, including:

On page 4, Nicole Kinney, BISO, Fifth Third Bank, discusses her role and if SASE is a buzzword

On page 6, Allan McGuy, Director of Product Security at Cengage shares his approach to tying security metrics and business objectives together

On page 8, Sydney Gelb, Senior Information Security Consultant, K logix shares how organizations should address cloud-based risks from both internal and external sources

On page 10, hear from Dan Garcia, CISO, EnterpriseDB about how his organization underwent a digital transformation journey from a strategic and technical perspective

On page 12, Greg Kyrytschenko, Deputy CISO, Guardian Life discusses why investing time and resources into understanding technology and business problems helps to implement effective controls in the cloud

On page 14, Roger Vann, Senior Information Security Consultant, K logix breaks down the newer to market concept of CNAPP

We hope you enjoy reading!

*Kevin West*

CEO, K logix


**Magazine Contributors:**

**Katie Haug**

VP Marketing, K logix

**Kevin West**

CEO, K logix

**Kevin Pouche**

COO, K logix


**About K logix: Cybersecurity Advisory and Consulting Services**

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.

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 hundreds of CISO interviews, we extract trends in order to provide services that align business to information security.


www.klogixsecurity.com/feats-of-strength

Marketing@klogixsecurity.com

617.731.2314

# NICOLE KINNEY

**Business Information Security Officer**
**Fifth Third Bank**

**HEADQUARTERS:** Cincinnati, OH

**EMPLOYEES:** ~20,000

**REVENUE:** $8 Billion
(Reflective of Fifth Third Bancorp, the indirect parent company of Fifth Third Bank, National Association)

Nicole Kinney did not have a traditional path into technology or security, but her vast business background enabled her to drive positive changes across organizations throughout her career. In her undergraduate studies at UMass Amherst, she studied areas of management and building construction technology, design, and psychology. She gained a highly versatile interdisciplinary education and landed her first job as a project manager at a technology organization serving the Farm Credit Banking industry. Here, she had an opportunity to self-educate on many different technology topics and wear multiple hats outside of project management. She explains, "I gained exposure to relationship management, configuration management, test plan development, and things like transitioning the organization from a waterfall approach to agile software development methodologies. With all that, I got a bug for technology and ended up moving to a large insurance organization in their rotational technology leadership program and continued to really expand on that broad discipline of different skillsets."

While working in the rotational leadership program, Nicole was part of rotations in areas such as quality assurance where she built out a team working on their billing systems, as well as identity and access management, bringing transparency into who has access to what, and setting up initial risk assessment and risk management work. She explains, "I also focused on the business where I embedded myself at a program management level to understand their technology portfolio and how I could help move that along to serve their different business needs and strategies. Coming out of that program, I wanted to really push myself to grow my technical skillset because I felt that I needed to have a stronger technical foundation and experience as a practitioner to be a more effective technology leader."

During this time, Nicole was exposed to information security when she worked on a team focused on email and web cyber security controls. She began as a technologist on that team and worked to grow her technical skillset from implementing changes, configuring different systems, and managing the vendor relationships. Over the next several years, she worked her way into a team management position where she led a team and programs such as helping the organization move from completely on-prem email filtering infrastructure to a cloud-based solution. She comments, "It was a multi-year multimillion-dollar program that was really satisfying to see complete, and work through all the complexities of doing a project like that in a very large multi-national organization."

After spending more than nine years at the insurance organization, Nicole moved to her current role, Business Information Security Officer at Fifth Third Bank. A little over one month into her new role, Nicole says she is excited for the opportunity to shift towards a different type of leadership with exposure across the entire enterprise leveraging her soft

> *"What I value most is open, honest, respectful communication, I think getting that dialogue going, making sure that everyone has a voice, is part of the conversation and is included is so important."*

and technical competencies.

## IMPORTANCE OF SHIFTING LEFT

After working on projects during her career related to cloud migrations, Nicole strongly believes in the value of a focus on shifting left by getting security involved in development from the beginning. She explains, "It's an unfortunate experience when you've got a technical team that has developed, coded, worked up, and created something, then they're at the end of that journey and ready to go use it, and you find out that security was left out. You are now facing the possibility of having to do a lot of re-work and you're not able to responsibly publish something to market knowing there are risks or gaps that could cause security problems. I think that's something that all organizations are really working on doing, and part of why the role that I'm in now is so important to me. I really have a chance to continue to bring that security mindset upfront and partner with the technology teams across the organization to help provide guidance and consultancy, to enable them to do their best work."

One of Nicole's mentors had the motto that 'security isn't no, it is how', something she believes perfectly sums up the shift left mentality. She sees her charge as a security professional to be a resource, understand what other departments are trying to do, and help them do so in the most secure way possible.

## LEADING WITH PURPOSE

Nicole says her goal is to strive for continuous improvement and always find ways to make the areas she has influence over incrementally better. She found the key to enacting that kind of change is to invite open communication and listen to feedback. By hearing what people have to say, then working with them to experiment and try out different changes, you move toward an ideal state progressively, and together.

She continues, "What I value most is open, honest, respectful communication, I think getting that dialogue going, making sure that everyone has a voice, is part of the conversation and is included is so important. For me, people and relationships really matter most, it's not about what you're doing, it's about how you get it done, and making sure you do that in a way that really focuses on your customers, your network of people involved and all the stakeholders. I believe in the servant leadership concept. I'm very service-oriented and focused on enablement and how I can give my team what they need to be successful. I also really value the concept of going slow to go fast and making sure you have a clear strategy and vision of what everyone is driving towards before you just rush into implementing. This is important because it helps prevent a lot of confusion or wheel spinning. Most importantly, I believe in trying to have a little fun wherever you can. Our work is very, very serious, it's important, and it can be very stressful and anxiety-provoking at times, so trying to manage that stress by finding ways to bring enjoyment and some fun to the work wherever possible can really go a long way."

To continue to grow and learn, Nicole believes in plugging into different professional networks, peer groups, as well as dedicating time to independent reading and research.

Attending conferences are also a valuable tool for Nicole to network and learn, she comments, "Conferences are great for staying up to date on all the different products and tools that are out there, and now they're starting to be in-person again. One of my favorite parts of going to conferences is the interaction you get with your peer groups and being able to strike up casual conversation with people across different industries and from different companies and hear how they're doing things. One of the more recent conferences that I was at had many talks on how the criminal enterprises work just like a company. They're working within a network, they're working together and sharing information and we need to do the same. The more you can share information and knowledge across different peers and different networks, the better for getting a sense of what kind of attacks are happening and what kind of targets are sought after."

### SECURE ACCESS SERVICE EDGE (SASE)

"SASE is a little bit of a buzzword, and a current trend. It goes back to the fact that the same security principles apply, whether you are operating on-prem or in the cloud. It's about defining those trust perimeters and understanding what is trusted versus what isn't, and how you manage that as the culture of technology is evolving to have even more sharing and connectedness. It comes back to enabling that increased sharing and connectedness while being able to have the right switches to turn on and off to protect what is yours, or quickly identify and contain if something were to be compromised or get out of control, it is a tool you can use to make sure that you're protected from that kind of threat activity and that it doesn't have free access to move across your technical ecosystem."

# ALLAN MCGUY

**DIRECTOR OF PRODUCT SECURITY**
**CENGAGE**

**HEADQUARTERS:** Boston, MA

**EMPLOYEES:** 4,500+

**REVENUE:** $1.23 Billion

Allan McGuy earned his bachelor's degree in Mechanical Engineering and his master's degree in Quality Systems Management. He began working at Cengage, a global education technology company, in 2017. He was initially hired as an IT Security Project Manager where he was responsible for assessing, planning, and organizing IT security initiatives, programs, and activities. His role was focused on all aspects of IT including infrastructure and platform leadership. His responsibilities included creating the security program roadmap, driving security best practices, producing meaningful project reports, co-leading the Incident Response Team, and many other duties that positively impacted the company's security program. In 2019, Allan transitioned to Director of Product Security. His philosophy from the beginning was to become true partners with the application owners.

> *"By partnering with application teams, walls are broken down and security has an opportunity to expand throughout applications."*

For Allan, educating application owners is key to forming a strong symbiotic relationship to positively impact the business and drive growth. This also gives security an opportunity to expand into SAST, DAST and penetration testing. According to Allan, "By partnering with application teams, walls are broken down and security has an opportunity to expand throughout applications. I recommend starting with senior leadership and educating them in a proactive way. After getting the buy-in from senior leadership it is important to build trust. Being part of the team with our development partners enabled us to execute testing adoption thus improving the security posture of out applications."

## TYING SECURITY METRICS TO BUSINESS OBJECTIVES

Allan feels it is important to tie security metrics to business objectives. He comments, "The biggest challenge for product security is providing the business an accurate account of the security posture of each application." His team has created a security maturity rating that takes into consideration the adoption of targeted security practices for each application and the mean time to remediate security vulnerabilities. This allows the business to measure the security profile of each application. Allan publishes quarterly metrics for each business unit who takes the data and builds initiatives for their next quarterly

planning process to address the security posture. When building the application security posture Allan says, “We use the OWASP SAMM model as a guide for the security practices such as testing, vulnerability management, training and guidance.”

## LEADERSHIP

Allan believes in empowering his team to grow and evolve. He explains, “I like to plant seeds with my team members, I don’t necessarily give them precise direction. I do not like to come across as a know it all and I always rely on team members to brainstorm together.”

Allan has had an opportunity to hire staff through Apprenti, a non-profit nationally registered tech apprenticeship program.

He says, “I like working with Apprenti because it often includes people who want to re-career themselves. Once we select someone, they go into a six-to-nine-week training program and have opportunities to obtain applicable industry certifications. After this initial training program, the employee joins our team, and we provide additional training for approximately one year. After the first year, an evaluation is performed to determine if the employee will stay within our group, or move on to other areas of the organization to learn new skills. Currently, there are three people on my team that are from the Apprenti program.”

> *“I like to plant seeds with my team members, I don’t necessarily give them precise direction. I do not like to come across as a know it all and I always rely on team members to brainstorm together.”*

To continue to grow and learn, Allan believes in attending conferences and participating in educational courses provided by the organization.

He comments, “At Cengage, we are a learning institution, and our goal is to help the learner, period. We put together courses like Skill Up where members of the technical organization were educated on all customer facing applications. We also have had design challenges (hypothetical business solution), where different people across the organization get together. I participated on a team of five and didn’t know anyone on my team beforehand. We did a design challenge for one hour per day for five days and it was a great opportunity. We offer so many courses to our external customers through our Work for Skills business including security courses with Infosec and all those courses are for our team members as well. There are constantly opportunities for my team and I to learn.”

Allan believes his team’s success is based on many things. He says, “We have chosen some very good testing tool partners; we have an excellent Chief Information Security Officer who believes in the product security vision, and we have an amazing product security team who is highly skilled in security and partnering with the application business owners and development teams.” Allan trusts and provides coaching support to his team which has enabled them to be a catalyst to all applications thus lowering Cengage security risk.

# CLOUD VULNERABILITY AND SECURE ACCESS SERVICE EDGE (SASE)

By Sydney Gelb, Senior Information Security Consultant, K logix

The concept of the cloud became a mainstream phenomenon in the mid-2000s when companies like Google, Amazon, and Microsoft released their own cloud computing platforms. As with any change to the norm, organizations were, at first, apprehensive to the adoption of this foreign concept. Yet despite hesitation, now in the year 2022, "according to Right Scale's annual State of the Cloud Report" (WebTribunal), 94% of enterprises are utilizing the cloud within their environment. Whether via a hybrid model or pure cloudification, companies are recognizing the benefits of virtualization and establishing them internally. Yet while cloud providers offer a layer of protection from their own repertoire of security tools, organizations need to be prepared to address cloud-based risks that may come from both internal and external sources.

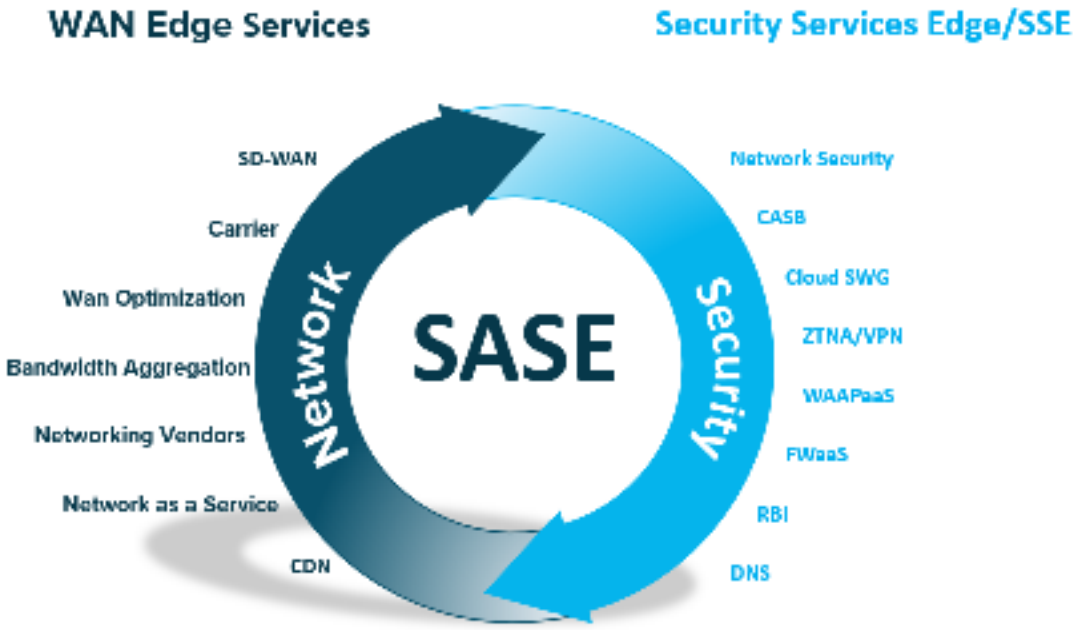
With changing environments comes changing risks and responsibilities, a notion that SecurityScorecard published in a post titled Top 5 Security Risks of Cloud Computing. "Cloud computing introduces another element in that the responsibility of addressing and mitigating…risk is split between the cloud service provider (CSP) and the organization." Well, if we're going to understand the actions necessary to mitigate risks, we must first understand what risks are present within the cloud computing environment.

Many companies, like KPMG, suggest that one of the most imminent threats present in the cloud is the risk of data security and regulatory risk. "This can cause business interruption, loss of revenue, loss of reputation, or regulatory incompliance" (KPMG). As previously mentioned, CSPs do have their own set of protections for their users. However, their customer organizations have limited visibility over their controls. Additional worries stem from "unauthorized data access by a service provider and/or less control over who sees what data" (KPMG). Other concerns such as potential data leakage have similarly arisen.

So, with risks that seem to be multiplying despite efforts to quell threats via cloudification, how is an organization to ward off said threats? A more traditional route of protection might be for organizations to mature processes and programs such as Data Loss Prevention (DLP) and Regulatory Compliance. Ensuring policies and procedures are in place that define roles and responsibilities for the likes of prevention, detection, and response will enable businesses to utilize internal resourcing for impact minimization.

Furthermore, the performance of regular audits and/or assessments will provide organizations with the understanding of their gaps as compared to industry-standard or regulatory frameworks. These assessment outputs will enable companies to fill in the blanks and ensure their security programs are robust enough to ensure maximum preservation against old, new, and future risks and threats.

There are progressive solutions emerging in the cloud space such as SASE (Security Access Service Edge). "SASE is the convergence of wide area networking (WAN) and network security services like CASB, FWaaS, and Zero Trust, into a single cloud service model" (K logix). Essentially, the baseline benefits of SASE lie in its ability to cut "complexity and cost" (NetworkWorld). Utilizing a SASE model also allows for the condensing of vendors present within an entity's environment, easing burdens and threats posed by the existence of too many vendors. In addition to the aforementioned benefits of SASE, benefits include the application of least privilege access, enhancement in staff efficiency due to "centralized, role-based management" (Versa), and optimized performance. As is apparent, since its inception in 2019, SASE has provided companies with significant benefits that extend beyond those included




in this discussion. As such, it is recommended that a consolidated platform such as SASE be considered by businesses globally.

With the outbreak of COVID-19, organizations saw a dramatic shift to remote work, disabling the ability to directly oversee employee activity. The move to a work-from-home model also brought about challenges such as network interruptions. Other benefits of procuring SASE include increased security utilizing policies. Said policy setting "also simplifies authentication processes by applying appropriate policies for whatever resources the user seeks based on the initial sign-in" (NetworkWorld). In other words, SASE allows for heightened access security regardless of user or device location.

As the security world moves away from traditional methods of data protection and environmental security, the existence of the cloud is gaining accelerated relevance. While most organizations have prepared for or already enabled cloud-based digitalization, the cloudified world is one step ahead, forcing organizations to now consider the benefits of various types of cloud computing. SASE is just one of the many solutions that will become continuously more prevalent over the coming years. The time is now for organizations to begin to bolster cloud security through the use of these new and improving models, staying ahead of the curve and ensuring minimal impact to environments.

### Interested in SASE?

K logix provides comprehensive technology and program advisory services to help organizations determine their SASE maturity and actionable/prioritized steps to meet their SASE goals. Our experienced team of researchers have analyzed SASE vendors and their capabilities, enabling customers to align their requirements and determine the best fit SASE vendors. If you are interested in learning more about K logix's SASE offerings, reach out to one of our experts: info@klogixsecurity.com.

By Sydney Gelb, Senior Information Security Consultant, K logix

Sources:

https://webtribunal.net/blog/cloud-adoption-statistics/#gref

https://securityscorecard.com/blog/top-security-risks-of-cloud-computing

https://assets.kpmg/content/dam/kpmg/ca/pdf/2018/03/cloud-computing-risks-canada.pdf

https://www.klogixsecurity.com/blog/k-logix-a-year-in-review-2021

https://versa-networks.com/sase/benefits.php

# DAN GARCIA

**CISO**
**EnterpriseDB**

**HEADQUARTERS:** Bedford, MA

**EMPLOYEES:** ~800

**REVENUE:** Undisclosed

Dan Garcia first became interested in information security over a decade ago when he attended an RSA conference as a collaboration architect. He explains, "I was trying to determine a way of measuring digital engagement between employees and departments, as a way of justifying and continuing investments in this area. At RSA, I attended a session about SIEMs that discussed the purpose of collecting telemetry on user behavior and system activity to be able to replay events in a way that helps the forensics process, which is core to incident response and security operations. When I looked at it from an analytical perspective, I realized that it could allow me to evaluate digital employee engagement, assess inter-departmental communication, and identify opportunities to drive employee retention."

At the time, his organization was investing in a security analytics program that required a leader with a different mindset to approach the detection and response problem. He made the jump to security and decided early on not to specialize in one area in security, but to take a strategic view to his career progression in information security.

> *"My risk management experience allowed me to make better investment decisions and to better communicate risk to business leaders."*

Dan has worked in engineering and architecture, core fundamentals of security. He says, "The security operations experience enabled me to understand how to detect and respond to events across the enterprise, while my risk management experience allowed me to make better investment decisions and to better communicate risk to business leaders. On the product side, my focus was on driving the roadmap and strategy that aligned with understanding customer needs and improving customer protection. This led to corporate development collaboration and M&A execution of targets that helped build a 6-billion-dollar business. It's been a career evolution into different new areas of information security, where there's always a lot to learn, and I worked never to stay stagnant in one area."

Currently, Dan is two months into the CISO role at EnterpriseDB (EDB), a global software and services organization that enables businesses and governments to harness Postgres, the world's leading open-source database.

## RESPONSIBILITIES

Dan has three main areas of responsibility in his role. First is to ensure that security investments EDB makes in product and development help drive business growth, and that they are compliant with SOC2 industry requirements, with an eye on FedRAMP.

The second area of his responsibility looks at reducing information technology risks. This involves putting in place the people, process, and technology controls that help reduce the frequency of adverse events or reduce their impact if they occur. Lastly, he has a focus on customers, their needs around security and how that translates into the EDB Postgres product portfolio.

Underneath that, Dan manages standard security operations, incident response, and control engineering, as well as educating the stakeholders who own security objectives, as they need to be successful to support the overall program.

Dan's top focus areas to continue to mature and improve the security program include establishing a unified control set across the company and establishing governance. He comments, "We will be focusing on building up our competencies in the security operations space to enable better incident response capabilities and to optimize the existing investments in the security stack. Additionally, we will be investing time and resources to put in place stronger device and identity management capabilities across the organization. This will involve pushing WebAuthN and adaptive authentication, establishing good network segmentation, and the operational ability to tie all these resources together with the right visibility into the activity within the environment."

He continues, "We have made many investments in technology, and in the next 12 months we'll be working on the integration and operationalization. I'm resisting the urge to rip and replace and focusing instead on the current portfolio of solutions to make them integrate really well, rather than trying to optimize one or two new tools. In the long run, this approach will lead to a better overall information security outcome across the organization."

## CLOUD TRANSFORMATION & SASE

As a traditionally on-premises software company, the cloud-based EDB BigAnimal product has gone to market with customers on the platform. Dan says initial investments have been made in EDB's digital transformation journey, and they are focused on having security baked in from the start. He comments, "From a security perspective, this leaves me with the job of integrating the cloud capabilities with the corporate security stack and unifying the environment with a common set of controls. It's important that our control framework supports the differences that exist in system architectures."

> *"If you can tap into your team members' self-mastery, understand what they care about, give them work that aligns with their interests and freedom within a framework where they can operate, you generally get very good outcomes."*

From a Secure Access Service Edge (SASE) perspective, EDB has made investments in a market-leading platform that will support part of their secure computing environment for employees. Adding this to a strong endpoint management and identity strategy will build up their zero-trust principles with on-going micro-segmentation work being done within the cloud.

## LEADERSHIP

Dan believes in being a strategic and structured leader who looks at company goals, establishes a vision that supports its growth, and aligns the work to the interests of the individuals on his team or on other teams. He says, "My leadership style is more about empowering individuals and allowing them to grow in the space where work needs to be done. If you can tap into your team members' self-mastery, understand what they care about, give them work that aligns with their interests and freedom within a framework where they can operate, you generally get very good outcomes."

A technologist at heart, Dan always seeks to understand new trends, architectures, and challenges. Working at a product company has opened up the need for him to be proficient in a number of new business domains such as product development, marketing, go-to-market, and speaking with customers about their needs. This makes his role more dynamic than traditional CISOs, where there is a need to have enough foundational knowledge in these domains in order to have the expected impact.

Dan concludes, "Learning how to translate information security to better support corporate development and drive business growth has been one of the most rewarding aspects of my career since jumping over from financial services."

# GREG KYRYTSCHENKO

**DEPUTY CISO**
**Guardian Life**

**HEADQUARTERS:** New York, NY

**EMPLOYEES:** 9,500 employees + 2,700 financial representatives

**REVENUE:** $1.9 Billion

Greg Kyrytschenko has worked in IT and security roles for over twenty years, giving him broad exposure to every facet of the business. He comments, “I became interested in security over twenty years ago. I remember watching certain movies and solving certain problems and thinking it would be a cool career to protect networks, computers, & software. When I started, the field was very immature, people knew you had to protect computers, but no one really knew how to protect them. I began my career in IT right out of college working in credit card fraud business and solving the types of problems was very interesting to me.”

Greg has remained in the security field because it offers him the ability to continually learn and challenge himself. He explains, “My philosophy is that I always ask myself how can I make things better than when I found it, and it’s always been a mission statement for me my personal brand and character within the security field. Focusing on this as my principal compass helps me strive to build great things for the companies I’ve worked at as well as create a positive impact for the people I have the opportunity to work with.”

Greg believes security should be an enabler and not an inhibitor. He reveals, “Security is not a place of yes or no, it’s meant to be my operating approach in my partnership with the business. Security should help an organization get to where they want to be providing guardrails which allows for business velocity and insight into helping to protect from cyber threat actors.” He continually focuses on that approach in order to set proactive realistic tones between security and the business that lead to trust, collaboration, and partnership. To achieve positive outcomes he ensures to meet regularly with stakeholders to establish two-way dialog between teams.

## FOCUS ON SECURITY AWARENESS

Greg runs the cybersecurity function from an operations and engineering perspective. His duties range from managing internal and external risks to running parts of the security awareness program and everything in between.

According to Greg, a strong security culture is paramount to an organization’s cyber resiliency. He explains, “Training and awareness gets people attuned to what threat actors are doing. The stronger you make the workforce, the stronger you make your organization. I believe in things like security champion programs where people help promote security awareness across the organization. They have their eyes and ears open for things that attackers may be attempting to do. It is important to make sure you have a feedback loop so that information gets back to you and your program, so you can continue to improve over time.”

He believes it takes changing the organization's culture to become more security-focused to help improve security posture. He considers regular and targeted communication as a core way to spread the mission of security, so everyone becomes invested in helping protect the organization and the workforce feels it is their duty to help protect it. Greg also believes in ensuring someone within security should help to market a company's trustworthiness to the lines of business. Building a security-minded culture is not easy and takes thoughtful planning along with strong communication and interpersonal skills. By showcasing how security protects the organization and positively impacts business outcomes, you are able to enable the business on security-related initiatives. Greg says this approach helps result in a stronger overall security posture.

## THREAT ALERTS AND GOOD CYBER HYGIENE

"I always ensure stakeholders and executives are informed on threat actor motives and tactics so they have awareness for what is going on in the world and how it may impact the organization. Security should help shepherd stakeholders and executives so they can make the right decisions and judgement calls with regards to threats. To be impactful, it is all about being able to simplify and not go into the weeds. I leverage current events and simplify the facts by being a good storyteller to keep their attention focused on what's most important," comments Greg. With security constantly in the news, Greg and his team must translate those threats and how they may or may not impact the organization. Not only does security need to address current threats, but they must work hard to stay a step ahead and be proactive for what could possibly come next.

By sharing information on a regular basis, employees stay aware of current risks, and in turn, each individual department is able to make better informed decisions around their specific risk tolerance. Greg says the more impactful information you provide around risks, the better decision outcome can be made. He continues, "As we partner with people across the business and talk to them about the cyber threat landscape and different types of potential attacks, security hygiene basics must be leveraged to create a stronger defense. Just like with fitness, if you are consistent then you will live a long healthy life. Security is the same, if you continue to do the basics with good security hygiene you are setting yourself up for life-time resilience and grit to handle cyber threats. You also need to use innovation and transformation to implement strong security practices that make it transparent to end-users."

## CLOUD AND SECURE ACCESS SERVICE EDGE (SASE)

With cloud security top of mind for many security professionals, Greg says investing time and resources into understanding the technology and business problems helps to implement stronger effective controls in the cloud.

For Greg, key drivers for moving toward a cloud architecture include scale, availability, and standardization in a distributed environment as many organizations move toward a hybrid work environment in the new post-covid world. He says, "You have to now plan for where people are working from (remote, off site, in-office), set up control posturing machines and make sure the computers connecting into the environment meet the standards that the organization establishes. It's important to cover how to control different aspects of cyberattack techniques which could be leveraged by insiders or external bad actors. You also must have the right levels of access, logging, and configuration management to establish cyber resilience in a remote environment."

Since achieving SASE involves networking and security teams working closely together, Greg believes in partnering as soon as possible for major initiatives to make sure teams and stakeholders are aligned around goals and necessary areas of action. He comments, "Getting IT, cloud, and security teams on board up front helps to ensure that the business problems are addressed during the design phase. Rome wasn't built in a day, so you need to set reasonable goals and milestones. I recommend building foundational controls first including resilience, control effectiveness, logging, and service failover capabilities. Then add additional capabilities over time in future phases."

Metrics are also a vital part of any cloud security initiative. Greg says it is important to ensure you create the right metrics and keep track of them as you are delivering the solution. He comments, "The more you can do with regards to demonstrating value the better the outcome. You want to be able to show how the security controls improve experience and the network resilience. You also want to show the isolation and segmentation capabilities to help drive the organization forward and create the level of mobility that might not have been there before. I recommend showing before and after imagery or graphs to help build the business case that you are in a better place now that solutions have been implemented."

### ALWAYS LEARNING

"I try to learn something new each week. As leaders, we need to be continually learning whether it is on a personal, technical, or leadership level. I am always challenging myself to learn something new. The CISO community is also very important. I often have honest conversations with my peers to bounce ideas off and assess risk. Having that support structure in such a high stress environment is important so security can continue to do mature and improve security around the world. The more the community works together, the better we all become."

# CLOUD NATIVE APPLICATION PROTECTION PLATFORMS

## CNAPP'S ROLE IN A HOLISTIC CLOUD STRATEGY

By Roger Vann, Senior Information Security Consultant, K l;ogix

Cloud Native Application Protection Platform (CNAPP) is "an integrated set of security and compliance capabilities designed to help secure and protect cloud-native applications across development and production (Gartner)." The term was coined by Gartner, who recognized the expanding needs that go into securing applications in the cloud. Broadly speaking, CNAPP solutions aim to address workload and configuration security by scanning applications in development and protecting them at runtime.

CNAPP is a culmination of the market shifts from raw virtualization of workloads going back two decades, to automating security of both the workloads and the environments in which those workloads run. The purpose of CNAPP is to unify and orchestrate independent solutions or architectures to enforce application behaviors that conform to the developer's intent.

CNAPP is a combination of "Cloud-Native":

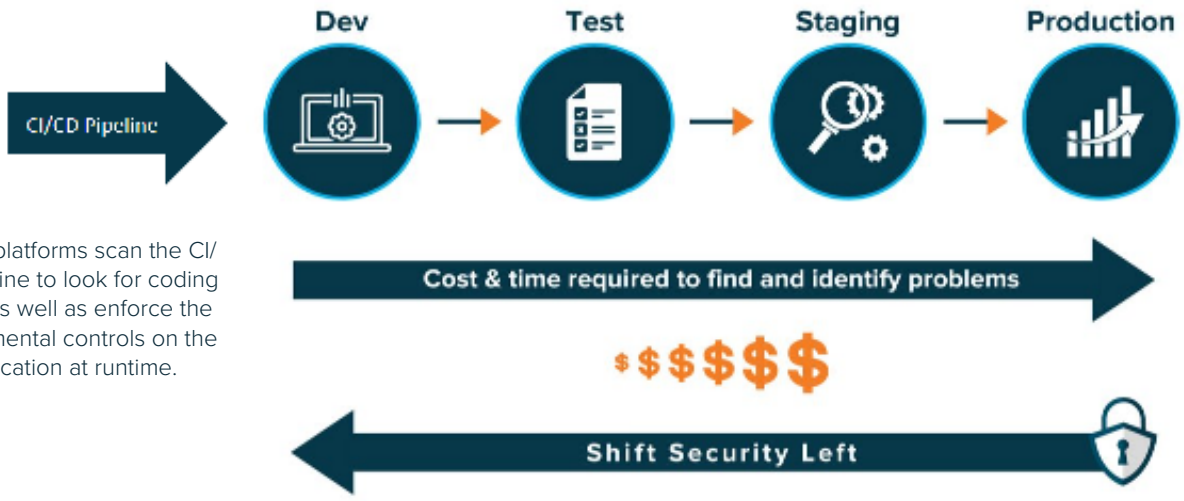
- Security tools (e.g.; code analysis, posture management and workload protections)
- Data sources (logs and telemetry)
- Automated coding practices (Continuous Integration/ Continuous Delivery, aka "CI/CD")

CNAPP serves as a convergence of multiple technologies, combining the capabilities of existing cloud security solutions, primarily Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP), Cloud Infrastructure Entitlement Management (CIEM), Kubernetes Security Posture Management (KSPM), API protection, serverless security (microservices), code repository integration (e.g.; GitHub, BitBucket, etc.) and more.

Cloud-native applications are built on a foundation of containerization and microservices. This architecture enables the CNAPP to protect the application throughout its lifecycle. CNAPPs enforce the developer's intent by enforcing secure coding practices (e.g., ban hard-coded secrets) and integrates those with approved container configurations at application runtime.

The environment in which cloud-native applications run is defined using "Infrastructure as Code" (aka. "IaC" such as Terraform, Ansible, etc). If the runtime configuration of the application should "drift" from that which was approved when the code was promoted to production, a CNAPP can block or report this activity for remediation. Key to this functionality

### CNAPP AND SHIFTING LEFT




CNAPP platforms scan the CI/ CD pipeline to look for coding errors, as well as enforce the environmental controls on the application at runtime.

is a technique known as “IaC scanning”, which is integrated into the CI/CD pipeline.

## CNAPP AND SHIFTING LEFT

Developing cloud-native applications with security baked-in is another way of saying “shift-left” application security. Shifting security left means implementing security measures from the beginning of, and during the development lifecycle, rather than at the end of the cycle. CNAPPs work with the shift-left mentality by integrating secure coding techniques within the CI/CD pipeline. CNAPP platforms scan the CI/CD pipeline to look for coding errors, as well as to enforce the environmental controls on the application at runtime.

The benefit of shifting security left is identifying security issues before they cause damage or become too costly to remediate.

## WHY DOES CNAPP EXIST?

There are two important elements in the term CNAPP that help explain why it exists. The first is “cloud-native.” The shift to the cloud has brought a wide range of new security needs along with it. The rise of dynamic and ephemeral environments within the cloud have increased complexity and created unique and unpredictable interactions. Traditional agent-based security approaches are not able to provide the appropriate coverage required to keep up with ephemeral, containerized, and serverless environments.

The second element is “application protection.” Previously, most cloud security tooling was focused on helping teams understand the security of their infrastructure. However, as Gartner says, “it’s no longer enough to ask, ‘Is my cloud infrastructure secure?’ Security tools must now ask, ‘Are my cloud applications secure?’”

When it comes to cloud applications, organizations need to be holistic in their security thinking. There are many ways to expose applications to risk in the cloud, from unintentional public internet exposure to overly permissive access rights, and more. Organizations should focus on identifying and mitigating the highest priority risks their cloud applications are exposed to, not just collecting a long list of security-related issues that in isolation pose little risk. With individual point solutions, they often narrowly focus on a limited set of security issues and do not integrate well together when it comes to correlating their signals, leading to challenges around prioritizing many low-priority alerts.

## KEY COMPONENTS OF CNAPP

As CNAPP represents a convergence of existing security product categories, let’s briefly review what capabilities fall under the CNAPP umbrella. Everything below represents an existing point solution. CNAPPs bring aspects of these point solutions together to provide full stack visibility across cloud environments and shift the focus from individual security issues to broader, interconnected combinations of issues that pose a critical risk.

### CSPM

CSPM solutions are focused on identifying misconfigurations in cloud resources and tracking compliance to different controls and frameworks. They focus on the cloud control plane, examining cloud infrastructure at the provider level. CNAPPs perform a deeper analysis of configurations and combine them with other inputs to identify and prioritize actual risks.

### CWPP

CWPP is about securing cloud workloads, such as VMs, containers, and serverless functions, regardless of their location. CWPP capabilities go inside the workload, scanning for vulnerabilities, workload configurations, hard-coded secrets, API keys, and more. CNAPPs leverage CWPP capabilities to identify issues in the data plane within the workloads themselves.

### Supporting tooling: CIEM, KSPM, serverless, and more

While CSPM and CWPP capabilities are the primary components of CNAPP, a complete CNAPP solution will bring in elements of other cloud security tooling. Some examples include:

### CIEM

CIEMs deliver infrastructure entitlement management capabilities so organizations can enforce related governance controls. Identity and access governance represent an important risk area that CNAPPs should be able to address. For example, Wiz recently found that 82% of cloud companies unknowingly gave 3rd party providers access to all their cloud data.

### KSPM

KSPMs are a special type of CWPP. Containers such as Kubernetes are essentially workloads that run workloads. KSPMs are essentially CSPMs for Kubernetes. They focus on Kubernetes-related misconfigurations and security needs. For CNAPPs, bringing in a dedicated focus on Kubernetes and container security is important for cloud-native environments.

If you are interested in learning more about CNAPP, K logix has extensive educational workshops. Don’t hesitate to reach out to us.

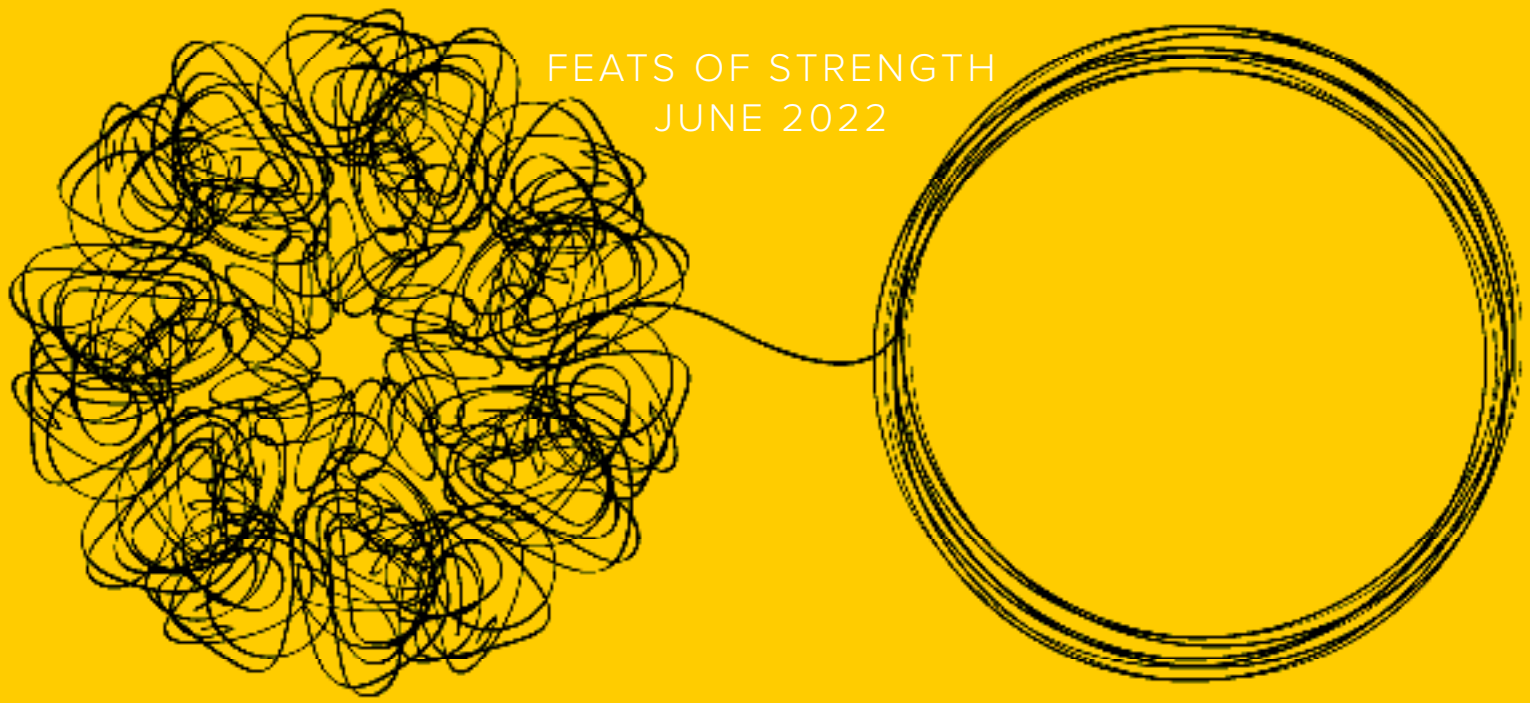
K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM

# HOLISTIC CLOUD SECURITY

FEATS OF STRENGTH
JUNE 2022



K logix