appgate

How Do Generational Differences Impact Enterprise Cybersecurity Teams?

Leveraging multigenerational expertise to close the cybersecurity skills gap

ZERO TRUST NETWORK ACCESS **WHITEPAPER**

TABLE OF CONTENTS:

Introduction

The inspiration to examine the impact of intergenerational differences on enterprise cybersecurity teams was born from our work with a large financial institution. It was in the process of deploying Appgate SDP, an industry-leading Zero Trust Network Access (ZTNA) solution, to simplify secure user access. But, it faced an internal challenge finding the skills to integrate legacy mainframe data into its broader cloud strategy. This, combined with the fact that the pandemic caused an exodus of Baby Boomers—the main knowledge workers for all things mainframe—from the tech workforce, led to questions about the wider impact of generational differences on the industry.

To illuminate answers, Henry Rose Lee, a leading expert and author on intergenerational diversity, was tapped to conduct extensive desk research and in-depth focus groups with IT and security professionals from Baby Boomer and Gen-X groups. This whitepaper examines how differing attitudinal behaviour and skills impact IT and security teams and highlights how Gen-Xers can be the conduit to bridge skills gaps between outgoing Baby Boomers and incoming Millennials to ensure continuity for enterprise cybersecurity strategies.

The Human Element

Generational differences exist in all aspects of social and cultural life with most enterprises having multiple generations represented in their workforces. An age-diverse workforce creates significant benefits for employees and employers, particularly when it comes to overcoming the much-publicized cybersecurity talent shortage as digital transformation continues.

Different generations have acquired distinct technological and cybersecurity skillsets with varying views and knowledge determined by their own experiences. Understanding these differences and harnessing them appropriately will greatly benefit employers and employees when creating their enterprise-wide cybersecurity plan.

Baby Boomers witnessed the growth of enterprise technology and are well-established legacy system gurus. They have worked with these platforms for decades and hold a fundamental role in managing them and integrating old with new. However, according to the 2021 BMC Mainframe Survey, during the pandemic many Baby Boomers took early retirement, leaving organisations with more than half of their data residing on mainframes and a lack of skills to integrate those resources into the cloud era.

Younger generations, Gen-Xers and Millennials, stepping up to the plate, naturally have less life and work experience yet have grown up with rapidly evolving digital technology that demands speed, simplicity and control. Being less familiar with legacy systems, they struggle to integrate traditional technology with security frameworks like Zero Trust that enterprises are embracing to mitigate the rising wave of cyberattacks. It is crucial that organisations find a way to transfer legacy knowledge to incoming teams, so the technology they have invested in to protect the business remains robust and future-proofed.

Baby Boomers (1946-1964)

Believe that hard work delivers a better future. Good social and communication skills.

Early IT adopters, yet tend to see some technology as not relevant and may ignore it if it's not useful.

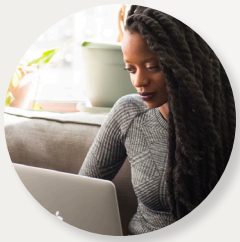
Approximately 33% of UK workforce.

Generation X (1965–1980)

Independent, self-starting and a bridge between older and younger generations. Grew up with email and mobile phones.

Have happily adopted new technologies as digital immigrants.

Approximately 35% of UK workforce.



Millennials (1981–1996)

Interested in freedom, flexibility and work-life balance. More mobile and less settled than older generations.

Digital natives due to their acceptance and use of technology at work and home.

Predicted to make up 40% of the workforce by 2025.

Key Findings

Through examination of intergenerational differences within the workforce and behaviours toward cybersecurity, the research by Henry Rose Lee reveals:

- It is all about people: knowledge and experience make the real difference to effective cybersecurity resiliency, not the latest-generation technology and infrastructure
- Businesses are at risk of creating their own cybersecurity abyss: with Baby Boomers retiring, swathes of experience and knowledge can be lost including the ability to manage and integrate legacy platforms into secure Zero Trust security environments
- Millennials aren't as cyber-savvy as we think: while they may be tech-savvy digital natives, Millennials may lack accountability and a deeper understanding of the back end of security, which can make organisations more susceptible to cyberattacks
- Gen-Xers can be the knowledge conduit: bridging the gap between the generations, Gen-Xers play a pivotal role in distilling and bringing together the experience and expertise of Baby Boomers and Millennials
- Baby Boomers are cybersecurity saviours not dinosaurs: many retiring cybersecurity professionals can stay in key roles or be redeployed as post-retirement consultants to support legacy systems and support the transfer of knowledge to Gen-Xers and Millennials

Legacy technology heroes: Baby Boomers

Baby Boomers, ranging in age from mid-50s to mid-70s, have observed huge changes and evolutions in technology and cybersecurity across decades. They have a broader and more strategic mindset, influenced by their experiences, and a deeper understanding of likely outcomes. This means they are less likely to buy the latest tech fad as soon as it is available, despite often being budget holders or decision-making influencers. Instead, they seek to validate specifications to ensure emerging solutions are the best fit for the business and will, crucially, work with legacy technologies in place.

Baby Boomers bring a multitude of advantages to cybersecurity teams due to their higher emotional intelligence and maturity. Research by Verssimo, Verhaeghen, Goldman, Weinstein and Ullman (2021) demonstrates that many cognitive abilities improve due to life experience. In fact, Baby Boomers have learned key skills that are vital to maximise cybersecurity strategies, such as the ability to think deeply through a challenge, avoid distraction and fully focus when required.

Research from Gallup (2019) also found that Baby Boomers are often overlooked when it comes to career progression and skills development. However, as people today are often able to work into their 70s and even older, Baby Boomers can and should remain in the workforce. Plus, thanks to extensive life and work experience, they possess some of the most valuable skills that businesses need.

There is a well-documented shortage of cybersecurity skills worldwide. The UK Department for Digital, Culture, Media & Sport (DCMS) 2021 annual report on the industry reveals 50% of UK businesses lack the technical, incident response and governance skills in-house to effectively manage their cybersecurity game plan. One challenge reported is a lack of candidates with proficiency beyond technical capabilities that include soft skills such as a willingness to learn, problem solving abilities and commitment—qualities commonly evidenced in the Baby Boomer generation. Yet, the UK's largest investment management company Hargreaves Lansdown reports that, post-pandemic, one in 10 workers are planning to retire early compared to one in 25 workers before the pandemic.

According to research from Darrell Norman Burrell, The Florida Institute of Technology, Melbourne, USA (2019), companies need to broaden their range of candidates to seek smart, motivated and dedicated individuals who work well as part of a team. Addressing the cybersecurity skills shortage requires new approaches to talent management including hiring and retaining employees from the Baby Boomer generation who can bring the value of maturity, considerable work experience and critical thinking.

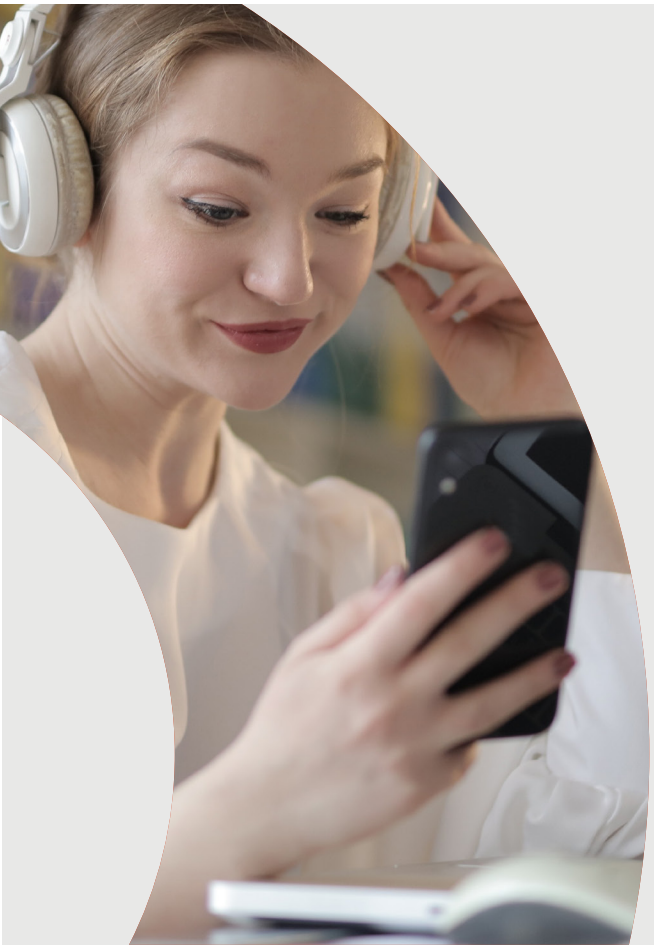
An exodus of Baby Boomers from the IT sector will further exacerbate the loss of skills in mainframe and systems management that are so vital in integrating legacy system data into today's digitally transformed world.

Meeting in the middle: Gen-Xers

Following in the footsteps of Baby Boomers are the Gen-Xers, ranging in age from early-40s to mid-50s. They, too, have been present for rapid technology advancements and are very adept at new IT and cybersecurity system integrations. As the last generation to enter the workforce before the transition from analogue to digital, they are also equipped with valuable cybersecurity and IT skills.

Highly collaborative in nature, Gen-Xers can play a significant role between Baby Boomers and Millennials as a proficiency conduit. Supporting this perspective is 2019 research undertaken by Health Education for England, which highlights that the Generation X workforce is most adept at collaborating with others and most engaged with organisations if they feel they are part of a team.

Gen-Xers are known for their independence, resilience and adaptability within the workplace; however, they would rather have the autonomy to fix a problem or propose a solution versus being told what to do and how to do it. This resistance to micromanagement means that while they tend to be loyal to their profession, they aren't necessarily loyal to employers, potentially deepening the cybersecurity and IT skills chasm for organisations.



Next-generation technology adopters: Millennials

Aged between 25 and 40, Millennials are technologically savvy and are the first generation to grow up with social media and smartphones. They also claim the broadest usage and fastest adoption rates of new technology, which comes with pros and cons. In particular, Millennials lack the deeper life experiences of Gen-Xers and Baby Boomers, which can hamper decision-making in situations that are not clear-cut or quick and easy to deal with, such as responding to cyberthreats.

Emotional intelligence (EQi) also plays a significant role in decision-making, yet research from Six Seconds shows Millennials are deficient in this area. The research reveals that EQi increases with age and suggests that Millennials do not form as strong of relationships or perform as effectively at work as their Baby Boomer counterparts. EQi areas that Millennials score lowest in are vision, collaboration and critical thinking, all vital to implementing sound cybersecurity strategies.

An NTT report on Cyber Security and the Next Generation (2019) highlights differing generational attitudes toward cybersecurity. Under 30s are much more concerned about flexibility and productivity, rather than caution and corporate responsibility. Speed and ability for systems to work in a frictionless manner are top of mind. Driven by the need for a quick resolution and ease of access, 39% of Millennials admit they would pay a ransom. This is nine percentage points higher than for over 30s. Millennials also are more optimistic about the time it takes to recover from a cyberattack, on average assuming recovery will take six days less than the more experienced Gen-Xers or Baby Boomers.

Biscom research indicates that Millennials are twice as likely to prioritise simplicity over security when handling sensitive data. In fact, Millennials are three times more likely to avoid security policies, and 60% admitted they would take the easiest option when handling confidential documents. The younger generation's comfort with technology has sometimes led to a laissez-faire attitude toward sensitive data and a tendency to overshare on social media, making them potentially more vulnerable to cyberthreats in their public and private lives.

How do you nurture and maintain a multigenerational cybersecurity workforce?

All generations bring their own sets of unique skills and values to the industry. The advantages of having a multigenerational workforce have been recognised by many, and the Organisation for Economic Co-operation and Development (OECD) research this year revealed that the inclusion of more older workers boosts productivity by around 11%. They also discovered that 70% of employers are looking to implement or explore the benefits of multigenerational workforce policies to support greater collaboration between older and younger employees.

Most businesses are still slow to take proactive steps to reap the benefits of an age-diverse workforce. Yet, there's every reason to believe that IT and security staff could benefit from this cross-pollination of technical skills and the softer skills of collaboration, problem solving and deep thinking brought by each generation of its current workforce.

Bringing Intergenerational Differences into Focus

The attitudes and behaviours presented by the predominant generations in the workforce are borne from their experiences to date. But, how does this impact cybersecurity teams' ability to share key learnings and ensure critical IT and security systems knowledge is passed from older to younger knowledge workers?

To find out from those on the frontlines, Henry Rose Lee moderated two focus groups comprised of Baby Boomer and Gen-X cybersecurity and IT professionals. They discussed how each generation views their contributions to the industry and the challenges they see ahead for Millennials as they take up the cybersecurity reins.

What value do Baby Boomers and Gen-Xers bring to the cybersecurity table?

The importance of a depth of experience and a robust understanding of the daily cybersecurity challenges facing organisations reigned supreme amongst the focus group participants. Unsurprisingly, half of the Baby Boomer focus group gave themselves the cybersecurity edge and attested they are the most efficient, proactive and knowledgeable protectors of an enterprise's data.

This was due to several factors:

- They "grew up with the transition from mainframe to personal computing" and witnessed the evolution of cybersecurity, so they have deep expertise when it comes to how hackers break into systems and the way organisations have adapted and developed safeguards
- Baby Boomers consider younger generations—even when having an IT and cybersecurity education—to be too trusting and are concerned this puts their organisations at increased risk for possible breaches due to lack of on-the-job experience
- Increased use of remote working means traditional on-site conversations to share ideas and get advice has disappeared, meaning the Gen-Xers and Millennials are not getting the ad-hoc exposure to learn and discuss any challenges with the more experienced Baby Boomers

The in-depth experience and big-picture perspective when merging legacy IT and security systems with new, often cloud-based, solutions is a significant intrinsic Baby Boomer value—one that organisations should carefully consider. Unlike many Millennials and some Gen-Xers, Baby Boomers know how to migrate data smoothly and securely from mainframes and data centres to the cloud while navigating bureaucratic hurdles and diverse business priorities to minimize disruption and protect new workloads. In addition, Baby Boomers believe in the power of intergenerational teams to share ideas and experiences to better serve the business.

Organisations must seek to combine the strategic thinking and legacy tech experience of Baby Boomers with the education and exposure to modern tech solutions held by Gen-Xers and Millennials.

One Baby Boomer commented: "We've seen things that maybe the younger people don't or haven't seen in terms of IT … but equally, younger people are given information during their education about how to safeguard. So, if you can pull those different skill sets together you've got collaboration for mitigating risks."

Gen-Xers similarly voiced that whilst younger generations receive more education on technology and cybersecurity, older generations have more experience. Accepting they may not have the formal education that the Millennials hold, Gen-Xers maintain their value comes from first-hand experience in witnessing cybersecurity shortcuts that led to long-term strategy and cyberthreat repercussions for an enterprise.

Leaning on their predisposition to problem solve and bridge intergenerational skill sets, Gen-Xers seek to affirm their value by bringing new and innovative ways to move business forward. Balancing out this creativity is a solid understanding of the importance of following security procedures and policies to safeguard the business. This is demonstrated by 80% of Gen-X focus group participants believing they adhere more strictly than others to the corporate security guidelines when working remotely during the pandemic.

What happens when Baby Boomers retire?

All focus group participants were asked to discuss potential industry impact when the more mature generation retires. From the Baby Boomer group, 40% were retired and 40% were planning to retire in the next six years. Known for being dedicated to their job roles and supporting business continuity, 80% confirmed they would consider re-entering the industry as paid consultants.

On the other hand, Gen-Xers held varying views. While some considered Baby Boomer retirement as a massive industry loss, others stated that an IT specialist of any age is beneficial to the business and retirees will simply be replaced. Their perspective is that once the Baby Boomers have left the workforce, leaders won't seek candidates with mainframe experience. Instead, they will hire professionals with expertise in AWS, Google Cloud Platform or Microsoft Azure Cloud. Yet, this view omits years of experience acquired by Baby Boomers, including expertise steeped in the legacy systems that future teams will be responsible for integrating with new solutions.

It was acknowledged that mixing older and younger generations within cybersecurity teams and in the workforce balances the digital savviness of youth with the acumen of more mature generations. Organisations would continue to benefit from having a multigenerational workforce and retaining legacy system skills to migrate mainframe data. One suggested solution is for the Baby Boomers, Gen-Xers and Millennials to mentor and reverse mentor each other in the skills they know best and use most effectively.

Attitudes toward cyberattacks

Baby Boomers and Gen-Xers know first-hand the damage of a successful cybersecurity breach. It is their concern over the Millennial approach to cybersecurity that unites them—further emphasising the opportunity for the Gen-Xers to serve as the intergenerational skills transfer conduit.

Focus group Gen-Xers also pointed out that whilst evolved security solutions are in place to mitigate risk, it takes more than advanced technology for Millennials to be solid cybersecurity guards at the gate. According to one participant, "Systems have gotten much better, and people in the business are forced by things like two-factor authentication to be better. That doesn't mean they make good cybersecurity decisions. It's the systems that make them better, but people can still be the weak link."

Whilst Baby Boomers were quick to acknowledge the benefits of age diversity, Gen-Xers were more concerned about younger generations' cybersecurity credentials due to the following workplace observations:

- Lack of accountability if an error occurs and a sometimes misplaced confidence in technology
- Tendency to be less cautious and to look for speedier alternatives to improve workplace productivity
- A sometimes limited understanding of systems and back-end security, making the organisations they work for susceptible to cyberthreats
- A propensity to quickly adopt and implement latest next-generation tech

Who is responsible for securing enterprise assets?

There are three weak points: infrastructure, software and people.

- Cybersecurity is the responsibility and accountability of all generations in the workplace, not just those who work in cybersecurity
- Employees are responsible for how they use the systems and how cyber-aware and cyber-secure they are
- Once infrastructure, software and security controls are sorted, the key cybersecurity weakness is still human error, with 88% of data breach incidents caused by employees' mistakes
- 75% of focus group participants said that organisations should deploy staff training, with doomsday dry-runs and additional policy and guideline manuals, to reduce security hacks and breaches

As history has shown, proficient human decisions are fundamental to all cybersecurity strategies. Baby Boomer and Gen-Xer focus group participants worried that Millennials—due to a tendency to want fast results—might push back against the perceived time it takes to implement stronger security measures such as Zero Trust, choosing instead to seek less secure alternatives that they think might be faster to spin up.

The Baby Boomer group also knows the realities of how long it takes to recover from a cyberattack and the importance of preparation for such events. Concerned that organisations often don't have a cybersecurity incident back-up plan, they said their experience of operating before the internet means they can revert to manual processes if something like a ransomware attack takes out systems. Meanwhile, they noted that younger generations have less experience operating in an offline world, which can add to cybersecurity skills gap concerns.

Navigating the Challenges of Migrating Legacy Systems and Adopting Zero Trust

Out with the old

Making the shift from legacy to modern—and often hybrid—IT infrastructure is no easy task. As a whole, focus group participants recognised the need to minimize the possibility of cyberattacks as digital transformation initiatives change IT ecosystems but reflected on a general lack of readiness. Technology and workload migrations require complex mapping and specific in-house expertise—which isn't always available—to determine how each area of the business will be impacted.

Baby Boomers explained the challenges involved in integrating and securing legacy and cloud data that include layers of bureaucracy and business units managed by different people, including services, network security and legal. In order to reduce complexities and achieve business-wide success, organisations must build a comprehensive plan by consulting each relevant party.

In with the new

Zero Trust security, based on the principle of preventing user and device access to the network until they are verified, delivers greater levels of protection for hybrid infrastructures, scattered workloads and work-from-anywhere workforces versus older, perimeter-based cybersecurity models.

Linked to this, Zero Trust Network Access (ZTNA) is a software technology and risk-based approach rapidly becoming the enterprise standard for secure access control. By applying Zero Trust principles to network security, users are denied access to networks and digital assets by default before they are verified and granted access. By leveraging ZTNA, organisations benefit from greater operational efficiencies without compromising security, convenience and agility.

When asked about Zero Trust security and ZTNA technology, the Baby Boomer focus group expressed concerns around perceived demands for additional overhead, greater bandwidth requirements and further administration.

Respondents also discussed the fine line between better security and unnecessary complications. Conscious that piling on security measures and restricting user access could become arduous, a key concern was that if security interferes with business productivity, workers will get security fatigue and find shortcuts that undermine the intention of Zero Trust.

In addition to delivering a major reduction in successful cyberattacks, ZTNA provides enhanced application management for on-premises and remote teams.

For the Gen-X group, Zero Trust kicks up some different concerns. Focus group participants perceived that modern identity-based network security encourages adversaries to target people, not systems. And to bypass security, cybercriminals must harvest authenticated user credentials, meaning innocent employees could be dragged into the cybersecurity war. They noted that where old criminal methods involved old-fashioned hacking through a firewall, identity and Zero Trust bring people into the equation.

However, whilst there are a few concerns around the Zero Trust approach, participants highlighted well-established benefits supporting the need for Zero Trust adoption within the enterprise. In addition to delivering a major reduction in successful cyberattacks, ZTNA provides enhanced application management for on-premises and remote teams.

It is Appgate's mission to communicate the true value behind Zero Trust in cybersecurity so that businesses feel confident stepping away from legacy systems. Crucially there needs to be a mindset shift, as Zero Trust security is more than just a technology or solution; it is a security methodology or paradigm with people and processes playing an important role in the equation.

Organisations that have adopted ZTNA have seen tangible benefits across their operations in strengthening their security and risk posture by providing enhanced protection for applications and data held in the data centre or in the cloud. Delivering time management and cost savings, ZTNA solutions simultaneously reduce unnecessary complexity, streamline automation and provide all users with greater support and a seamless experience.

The benefits greatly outweigh any deployment challenges, and ZTNA is a valuable technology for all generations steering their businesses through the complex cyberthreat landscape.

Conclusion

The increasing number of Baby Boomers reaching retirement age is an indicator of change for the cybersecurity industry. This study's findings are meant to encourage organisations to consider how to integrate differing skills, attitudes and expectations of multi-generational IT and security teams, while also considering the security implications driven by remote and hybrid workforces.

Developing and maintaining a multi-skilled, generationally-diverse security workforce and adopting Zero Trust-based solutions will help organisations securely integrate legacy and on-premises applications and data, along with cloud and IoT-based workloads. As we move into the post-pandemic world of hybrid workplaces and expanded attack surfaces, the Zero Trust evolution is a necessary shift requiring the unique skill sets of all generations to ensure success.

Additionally, gaining a better understanding of how Zero Trust security principles can better protect against the rising tide of ransomware and other cyberattacks is a vital step in gaining acceptance and participation. In particular, ZTNA solutions make enterprise resources invisible whilst seamlessly updating user access permissions to only the resources they need to do their jobs, ensuring organisations don't have to sacrifice speed and productivity in favour of security.

New approaches and changes inevitably provoke consternation. But as more businesses embark on a Zero Trust security journey using tools such as Appgate SDP, an industry-leading ZTNA solution, it becomes more apparent that migrating legacy, on-premises and multi-cloud apps to a Zero Trust framework doesn't have to be complicated. And by harnessing the skills, experience and understanding of all generations, organisations will strengthen their position against the army of cyber adversaries waiting at the door.

Research Methodology

Appgate commissioned intergenerational expert and author Henry Rose Lee to undertake desk and field research between June and September 2021 to examine the impact of generational differences in attitudes and behaviour on cybersecurity in the workplace. The project involved extensive secondary research, alongside in-depth focus groups with Baby Boomer and Gen-X IT and cybersecurity professionals who had experience in securely integrating legacy systems with cloud and on-premises networks. The study examines how organisations can harness the different experience and behaviours exhibited by different generations to implement effective, organisation-wide cybersecurity strategies such as ZTNA that maximise investments in legacy, cloud and on-premises technologies.

About Henry Rose Lee

Henry Rose Lee is one of very few intergenerational diversity experts helping organisations to improve the contribution and profitable performance of the youngest talent in the workplace today. Author of three books on maximising today's young talent, (Generation Z and Millennials), Henry Rose Lee busts myths and gives practical hacks for attracting, recruiting, engaging and retaining your youngest employees. Henry's expertise comes from 15 years working in business development and sales, where performance and results were essential. This was followed by 17 years as a Human Resources qualified consultant and Master Coach, researching and developing diagnostic tools on human motivation, and generational attitudes and behaviours at work. Henry Rose Lee delivers keynotes, diagnostics, consulting, masterclasses, workshops and coaching to ensure diversity and inclusion across all employee age-groups. Her work enhances communications, increases collaboration and inspires employees of all ages to give of their best, whether working from home or remotely or working in a bricks and mortar, or hybrid setting.

About Appgate

Appgate is the secure access company that provides cybersecurity solutions for people, devices and systems based on the principles of Zero Trust security. Appgate updates IT systems to combat the cyberthreats of today and tomorrow through a set of differentiated cloud and hybrid security products, Appgate enables global enterprises and governments to easily and effectively shield against cyber threats.
Learn more at appgate.com.

appgate