CyGlass

Keeping the Doors Firmly Closed

Proactive ways to defend against increasing threats to public sector cyberspace

Executive Summary

CyGlass

Introduction

The UK is facing a period of uncertainty. As pressures on both domestic and global fronts build, organisations across the public sector are far from immune from the challenges ahead. For leaders, the ever-present need to do more with less – to deliver improved service levels under tightening budgetary constraints – has in many ways been helped by the advent of digital transformation. A long-held ambition of Governments of every persuasion, digitalisation has made significant advances in recent years, both in technological and cultural terms.

Driven in many ways through the necessity of the pandemic response, great gains have already been made in all areas of the public sector. Where it has been embraced, digitalisation has helped square the circle of reducing costs while delivering more and better services to citizen users. Innovation in technologies such as machine learning, robotic process automation (RPA) and cloud computing has moved at a truly rapid pace. Recognising its potential, the Government has encouraged its widespread adoption through a far-reaching Digital, Data and Technology (DDaT) Strategy[1]. There are currently more than 1300 AI companies based in the four nations, with more than 30000 people employed in the industry[2]. Underlining a desire to ensure the UK retains its enviable position as a global AI superpower, the National Strategy for Artificial Intelligence[3] was announced in late 2021. This was followed by the 2021 Comprehensive Spending Review, which made several spending commitments paving the way for numerous ambitious projects across Whitehall and in the wider public sector arena, commitments which have since been reaffirmed.

These advances have, however, brought new challenges of their own. While innovation has ushered in many changes, both for the workforce and the citizens who access public services, new opportunities have been created for those with malicious intent. Demand for online services from a multiplicity of devices grows exponentially. Hybrid and remote working models require constantly expanding numbers of access points, all of which serve to increase the surface area vulnerable to attack. Cyber security has become a constant consideration, the responsibility of everyone. In this white paper we will address this development. We will look at some of the ways malevolent actors might seek to press home their attack, ways to defend and mitigate the effects of such attacks and how to ensure every organisation is kept secure in the uncertain world we inhabit.

"It is vital that cyber security remains a priority for government, industry and the public in building UK resilience to a spectrum of risks."

The Paymaster General[4]

CyGlass

The need for watchfulness

"Of the 777 incidents managed by the National Cyber Security Centre (NCSC) in the year to 2021, 40 per cent were targeted at the public sector."[5]

The world has changed. As we emerge from the pandemic period determined to build back better, old certainties must be reassessed and priorities reconsidered. Where there was once clear definition, today's public sector must be constantly aware of the environment in which it exists, responding and adapting to its changing nature.

Nothing short of a wholesale change in mindset is necessary. Where it was once relatively easy to understand where weak points might lie, and thus to defend accordingly, the area of vulnerability is now much wider. We are under constant threat, both from criminal enterprises and state actors – sophisticated, agile and determined to disrupt our way of life, either for financial gain or strategic advantage.

"So we must all, therefore, consider the likely long-term threat, so that we are as prepared as we possibly can be. And the greatest cyber threat to the UK – one now deemed severe enough to pose a national security threat – is from ransomware attacks."

Chancellor of the Duchy of Lancaster[6]

The statistics are alarming. A Freedom of Information Act[7] request has revealed that 161 local councils and local authorities across the UK suffered 10000 cyber-attacks in the first eight months of 2022. During the same period, some 2.3 million attempted attacks were detected. By far the most common threat came from phishing but Digital Denial of Service (DDoS) attempts were also a cause of considerable concern. Criminal groups have noted the rapid expansion of digitalisation in public service provision and understand that councils cannot afford their systems to be taken offline.

"...With so many attacks happening every day, it only takes one error to cause significant problems."

Tim Devine, Managing Director for Government Housing Education and Public Sector, Arthur J Gallagher & Co.

These numbers evidence the fact that a technological arms race is taking place. Attackers are constantly probing for the weak point in an organisation. As digitalisation continues to expand, so, too, does the attack surface. Security must now be the paramount consideration in implementing any new IT project.

Given the costs that can be incurred, the stakes are high. For a period of three weeks in 2020, Redcar and Cleveland Borough Council were the target of a sophisticated ransomware-based cyber-attack. Essential systems were shut down, 135000 citizens were unable to access online services and staff forced to revert to pencil and paper records. The financial cost was significant. Following the incident, the council was faced with a bill of £8.7 million with the Government contributing £3.68 million towards rebuilding its systems.

Gloucester City Council suffered a cyber-attack in December 2021. Their systems were penetrated by malware which had a severe effect on the council's benefits section and planning portal. The ramifications were still being felt more than nine months after the event and Leader, Councillor Richard Cook, has estimated that the cost of repair will "exceed six figures."

As well as the financial implications of such incidents, organisations must also bear in mind the reputational cost. Evidence suggests that the public is becoming more accepting of digital service provision. In September 2022, NHS England announced that the NHS App had reached the milestone of 30 million downloads[8] – more than half the population of the country – suggesting high levels of trust that personal data is being properly guarded. Winning and retaining such trust is imperative for public sector digitalisation, which requires the acquisition and storage of vast quantities of citizen's data.

The Government has signalled it is taking the problem seriously. In 2022 the first ever National Cyber Strategy[9] was unveiled. Announcing it, the Chancellor of the Duchy of Lancaster cited the "growing trend" of cyber incidents and the importance of maintaining confidence in digital services, saying,

"...the public rightly expects us to do everything we can to prevent these attacks in the first place and to get services quickly back to normal when they do indeed happen."[10]

In recognition of the essential need to act, the Strategy set out the aim of significantly hardening critical government functions and all public service organisations against cyber-attack by 2025, even those which start from a low level of maturity. To assist in meeting this target, an investment of £2.6 billion in cyber and legacy IT was announced.

Pillar 5 of the Strategy further outlined the challenges ahead, and confirmed the approach to be taken in detecting, disrupting and deterring hostile actors.

"The nature of the threat we face is complex. We are concerned about threats in cyberspace (for example to our online activities), threats to the UK and partners through cyberspace (for example to networked UK critical national infrastructure), and threats to the functioning of underpinning international cyber infrastructure. All of these threats can impact the availability of services that people rely on, or the confidentiality or integrity of data and information that passes through those systems."[11]

Much has been learned already. Recent global events have provided vital opportunities to examine how a hostile state might seek to penetrate our security. Speaking at the Billington Cybersecurity Summit in Washington D.C., Lindy Cameron CB OBE, Chief Executive Officer at the UK National Cyber Security Centre said,

"The Ukrainians have demonstrated what you can do if you are well prepared. The message we're doubling down on is, Look what's possible even against quite a sophisticated adversary."[12]

However, it is now imperative that every individual within every department and organisation understands their role in ensuring vigilance. A culture of security must be fostered. Cyber security is no longer simply the domain of large organisations with direct responsibility for Critical National Infrastructure (CNI) or dedicated IT staff. Cyber security has become everyone's responsibility.

"We in NCSC take that responsibility particularly seriously. NCSC was launched in 2017 as the 'team captain' for UK cyber security. As part of GCHQ we have access to the most sophisticated capabilities, helping us in our mission to make the UK the safest place to live and do business online.

But we can't do that alone – every organisation in the UK has its role to play in sharing knowledge, addressing systemic vulnerabilities and providing leadership on key national cyber security issues."

Lindy Cameron, CEO National Cyber Security Centre[13]

The Digital Supply Chain

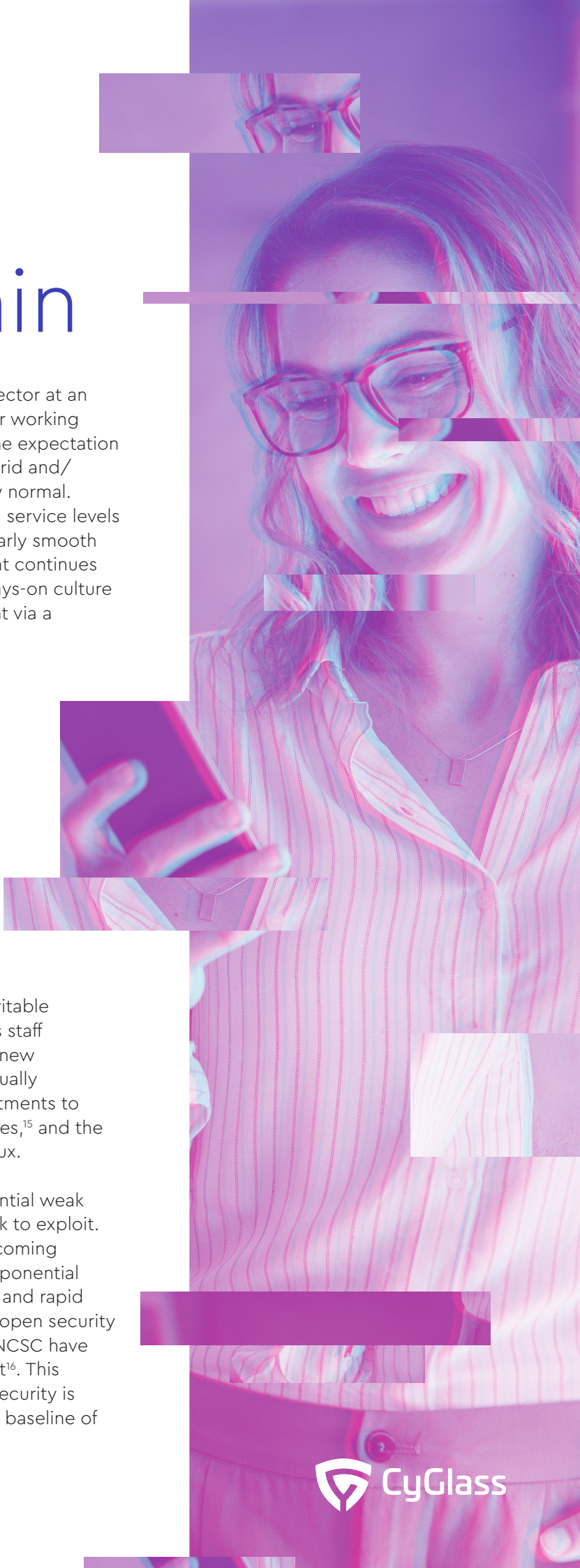
Undeniably, digitalisation is transforming the public sector at an unprecedented scale and pace. It is clear that smarter working methodologies and practices are here to stay, as is the expectation of online provision of services. For the workforce, hybrid and/or remote working models are already defining a new normal. Citizens too, having become accustomed to elevated service levels from the businesses they interact with, expect a similarly smooth interface when accessing public services. Government continues to encourage and promote "digital first" and our always-on culture demands connectivity at all times of the day and night via a seemingly infinite number of devices.

"Such is the speed of progress; digital technology has already grown to touch every aspect of our lives. Democratising threats, but also playing an important part in our future growth, with the potential for huge economic gains."

Chancellor of the Duchy of Lancaster[14]

This complex and fluid chain of connections is an inevitable consequence for any digitally mature organisation. As staff members leave, join or move between departments, new endpoints are created. New suppliers must be continually onboarded, particularly so given Government commitments to spend £1 in every £3 with small and medium enterprises,[15] and the requirements of end users are in a constant state of flux.

Each one of these myriad connections creates a potential weak spot, a point of vulnerability a hostile actor might seek to exploit. For those who would harm us, the environment is becoming increasingly target rich. The recent and continuing exponential growth in data acquisition, smarter working methods and rapid adoption of innovative technologies have created an open security posture. Such is the seriousness of the situation that NCSC have produced a supply chain security guidance document[16]. This sets out twelve principles to help ensure that cyber security is placed at the front and centre of operations, raising a baseline of competence and defining best practice.



CyGlass

Organisations must all understand that these rapid increases in connectivity, while responsible for a great many gains, often present open doors to hostile actors. It is imperative that the entire digital supply chain is protected. Every endpoint, server and hybrid network must be afforded equal consideration – nobody is safe until everybody is safe.

The consequences of supply chain attacks can be devastating. In 2017, the WannaCry cyber-attack exploited a vulnerability in the Microsoft Windows operating system. The ransomware spread quickly. Although not directly targeted, the NHS suffered severe effects. At least 80 NHS Trusts along with 603 primary care and other health service organisations were affected[17]. The attack infiltrated the NHS N3 broadband network, which at the time connected every NHS site. Patient records were locked down and more than 19000 appointments were cancelled across the UK. The week-long attack was estimated to have cost the service £92 million in lost output and remedial work to restore systems.

NHS services were further impacted by a supply chain attack in 2022. IT company Advanced Software Ltd was penetrated by an as yet unknown attacker in what is believed to be a financially motivated ransomware attack. The company supplies software and services essential to the running of NHS 111, patient check-ins, medical notes and certain care home applications. In the immediate aftermath of the incident there were widespread outages across the NHS. In all. Seven systems were taken offline by the attack, which was still having adverse effects more than two months later.

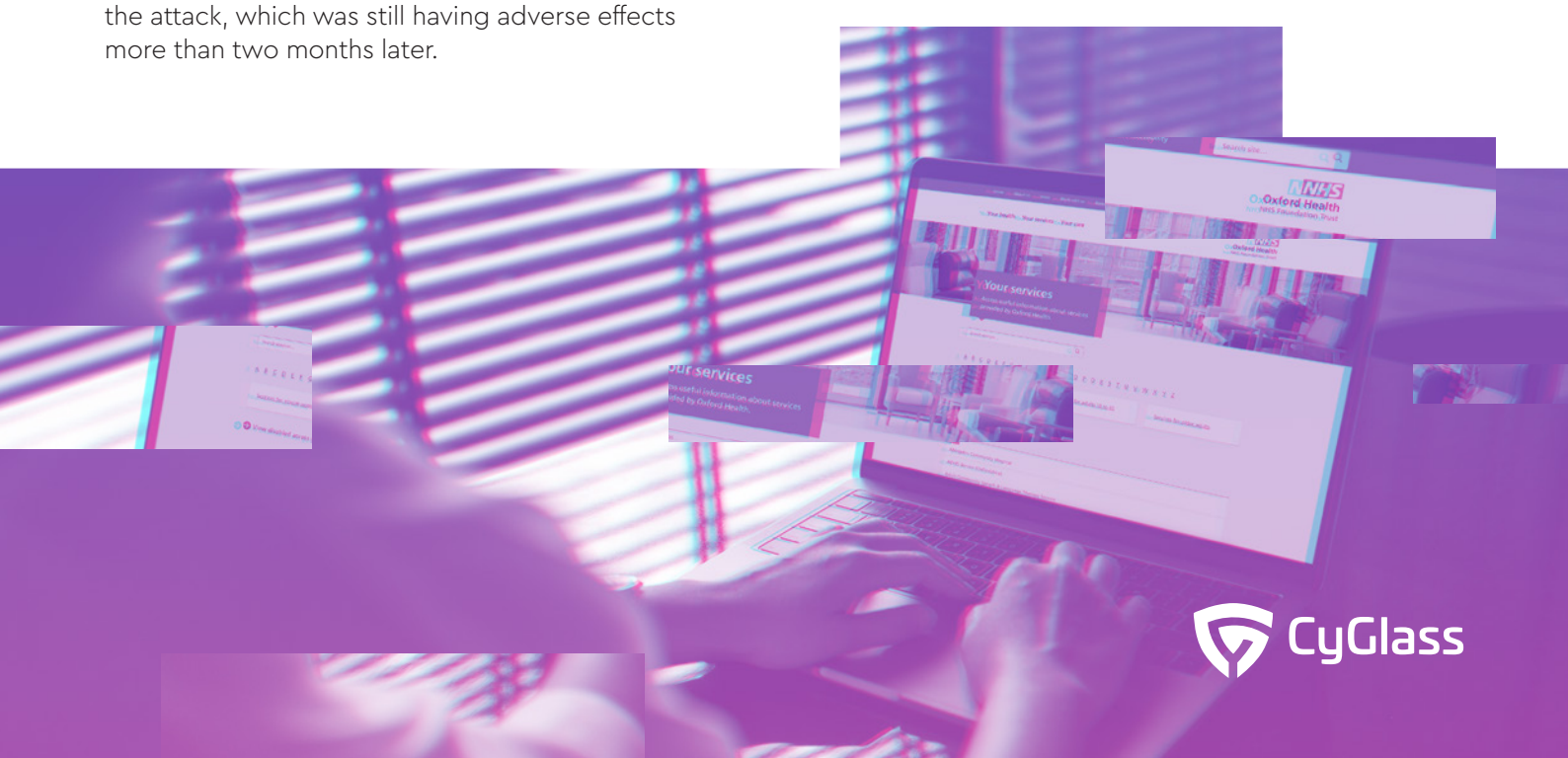
Some of the effects were summed up by Dr Nick Broughton, Chief Executive at Oxford NHS Foundation Trust. Speaking at the Buckinghamshire, Oxfordshire and Berkshire West Integrated Care Board, he said,

"One shouldn't underestimate the impact this has had on our organisation… it is compromising our ability to deliver the quality of care that we would like to."

"We're very conscious of the potential impact on patients and we're monitoring that very closely."[18]

Advanced, the NHS and NCSC are investigating the event and working to restore systems. Repairing the damage will take several months and incur significant costs, despite the backups that were already in place[19].

These incidents illustrate the damage that can be done. Not only can organisations suffer financial and reputational harm, there are very real physical risks to the safety of the public.



The Solution

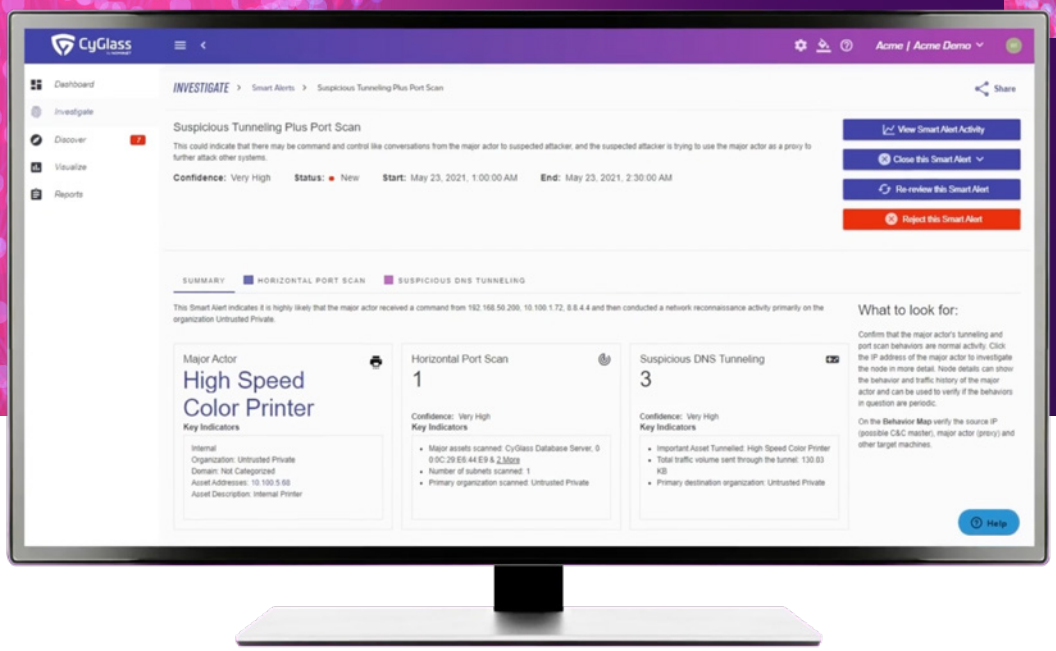
The risk is real and the threat growing, the potential for harm significant. However, in the uncertain economic times in which we find ourselves, fiscal pressures are an ever-present reality.

Historically, cyber security has relied on the need for on-premise solutions. For a network to be effectively defended, it has always been necessary to implement physical hardware at every single point of access. Given the multiplicity of endpoints involved, this would be virtually impossible, both financially and physically.

For this reason, cyber security has often been low on the list of priorities for many organisations. The need for protection, however, has never been more acute. Once again, leaders and teams must try to find a way to square the circle. Any solution must be able to demonstrate that is it not only capable, agile and scalable to meet continual changes in demand, it must also be cost-effective from the start. The answer, as with so many other of the technological innovations that are transforming the way the public sector operates, may be found by looking to the cloud.

Today, a unique solution, CyGlass Open Cloud XDR (Extended Defence and Response) provides a rapidly deployable cloud-based platform providing robust protection across network traffic, cloud services, user and machine identities, wherever and whenever it is needed. Effectively democratising cyber security, CyGlass runs 100% in the cloud eliminating the need for additional hardware or specialist operational staff, bringing a powerful, enterprise-level solution for organisations across the entire public sector spectrum.

CyGlass



Unlike traditional, on-premise NDR (Network Defence and Response) and SIEM solutions, CyGlass can be quickly and easily scaled up or down as required, providing a robust and responsive defence capability across all remote locations at a fraction of the cost of legacy systems.

For cost-conscious organisations already familiar with the Cloud model, CyGlass enables the journey to digital maturity to continue. Systems and data are protected across the entire network, cloud and O365 environment, maintaining the confidence essential to user acceptance of digitalisation.

CyGlass

CyGlass

As pioneers in the field, CyGlass are already partnering with organisations throughout the UK public sector including one of the largest City councils.

CyGlass is one of the first cyber technology providers to deliver a 100 per cent cloud-native solution for network, cloud, SaaS, O365 and IoT defence against cyber-attack, eliminating the need and complexity of specialised appliances and on-premise hardware. Leveraging the AWS platform, CyGlass enables an organisation to deliver critical cyber defence capability in minutes and hours instead of months, at a significantly lower TCO than the previous generation of appliance-based solutions.

The company's unique technology was developed from work initially funded by DARPA (Defense Advanced Research Project Agency) in the United States, which was undergoing research into tackling anomalies that impact fighter aircraft operations for the US Department of Defense. CyGlass uses this unique ability to apply advanced AI models to massive amounts of data and find in that data the critical threats that are important. This would simply be impossible for a human to undertake. However, implementing this capability, leveraging the scale, cost effectiveness and ease of deployment of the AWS cloud compute platform brings this ground-breaking capability to even the smallest organisation.

CyGlass was awarded the prestigious 2021 Cloud Security Product of the Year[20] by Computing Magazine and was a CSO50 Award winner for its "Protecting Citizen Data" project[21]. At the SC Awards Europe 2021, the CyGlass extended NDaaS solution was named as Best SME Security Solution[22].

As one of the new generation of entirely cloud-native cyber security platforms on the market, CyGlass uses the latest innovations in Artificial Intelligence and Machine Learning. Billions of transactions are constantly monitored to detect anomalies. The technology learns normal behaviour to create a baseline of the organisation's network and cloud usage patterns continually to learning and adapting on an ongoing basis.

By always understanding what is normal for an organisation, the CyGlass solution will detect unknown and unpredictable threats, protecting against zero-days, ransomware and threats from inside and outside the organisation's network, cloud, SaaS, IoT and O365 infrastructure. The AI is used to deliver smart alerts, highlighting only the critical threats and drastically reducing false positives and automating remediation actions when desired. The AI and ML capability drastically reduces the load on incumbent IT and security teams.

CyGlass

In addition to the threat, defence and response capability, CyGlass provides accurate, correlated, risk-based dashboards and reports in a form that requires minimal technical knowledge, enabling information to be quickly shared and understood across teams prior to action. These reports eliminate huge amounts of manual work required to fulfil security-based reporting for cyber insurance and supply chain audits, board level or other parties that require demonstrable evidence of an organisations on-going security posture, enabling a continuous compliance to be demonstrated to any interested party. CyGlass customers have also used this capability to gain ISO 27001, Cyber Essentials and Essentials plus accreditation.

CyGlass has recognised the need to provide clear and accurate intelligence to inform human decision-making at multiple levels. By choosing CyGlass as a cyber security partner, organisations can rest assured that critically important decisions will be human, rather than algorithm.

Case Study: Birmingham City Council

As the second largest local authority in the UK, Birmingham City Council represents more than a million citizens and has a staff of more than 12000. When the city was chosen to host the 2022 Commonwealth Games, its IT team faced a monumental task. As Birmingham continued its recovery from the pandemic, athletes from around the world would be welcomed to compete across multiple venues in the full glare of the international media, all against a backdrop of rising global tensions. Clearly, there was a high risk of cyber-attack, which needed to be carefully managed in a complex behind-the-scenes operation.

Having recently brought its IT capabilities in-house, the council was determined to set a benchmark for local authorities throughout the land. Following an extensive RFP and due diligence exercise, it was found that the CyGlass solution offered the world class protection required with, crucially, a significant cost saving over their competitors.

As with traditional NDR, CyGlass uses a combination of machine learning, advanced analytics, rule-based matching and threat intelligence to detect and report anomalous activity. The only true 100 per cent cloud native solution available, the platform provides configurable and easily understood reporting via an intuitive UI. Events can be monitored, investigated and reported in real time for an immediate and effective response.

With full-time 24/7 protection, the council could monitor the network continually, able to predict, visualise and react to any potential threat. The ability to see risks across the network was new for the council. Vulnerabilities were detected, tagged, prioritised and tracked according to their severity.

Having successfully delivered the Games, the council also achieved its secondary aim of providing a security benchmark for other authorities to follow. They have demonstrated how enterprise-level network security can be quickly deployed at a scale appropriate to organisations of all sizes, providing the mission-critical network security for the digitalisation that is transforming the UK public sector.

Birmingham City Council

CyGlass

References

1. **Digital, data and technology strategy: 2021 to 2024**
   www.gov.uk/government/publications/digital-data-and-technology-strategy-2021-to-2024

2. **New UK initiative to shape global standards for Artificial Intelligence**
   www.gov.uk/government/news/new-uk-initiative-to-shape-global-standards-for-artificial-intelligence

3. **National AI Strategy**
   www.gov.uk/government/publications/national-ai-strategy

4. **NCSC defends UK from more than 700 cyber attacks while supporting national pandemic response**
   www.ncsc.gov.uk/news/ncsc-defends-uk-700-cyber-attack-national-pandemic

5. **Record number of cyber incidents mitigated as NCSC protects vaccine rollout**
   www.ncsc.gov.uk/news/record-number-mitigated-incidents#:~:text=The%20NCSC%2C%20which%20is%20a,the%20health%20sector%20and%20vaccines

6. **Chancellor of the Duchy of Lancaster speech at Cyber UK**
   www.gov.uk/government/speeches/chancellor-of-the-duchy-of-lancaster-speech-at-cyber-uk

7. **UK councils hit by 10,000 cyber-attacks every day so far in 2022**
   www.ajg.com/uk/news-and-insights/2022/august/uk-councils-hit-by-10000-cyber-attacks/

8 **NHS app hits 30 million downloads in England**
www.bbc.co.uk/news/technology-63048021

9 **National Cyber Strategy 2022**
www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

10 **Building a cyber-resilient public sector**
www.gov.uk/government/speeches/building-a-cyber-resilient-public-sector

11 **Pillar 5: Countering Threats**
www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#pillar-5-countering-threats

12 **International cooperation is key to fighting threat actors and cybercrime**
www.csoonline.com/article/3673748/international-cooperation-is-key-to-fighting-threat-actors-and-cybercrime.html

13 **CYBERUK 2022: Welcome from Lindy Cameron**
www.ncsc.gov.uk/speech/cyberuk-2022-lindy-cameron-welcome-speech

14 **Chancellor of the Duchy of Lancaster speech at Cyber UK**
www.gov.uk/government/speeches/chancellor-of-the-duchy-of-lancaster-speech-at-cyber-uk

15 **Big opportunities for small firms: government set to spend £1 in every £3 with small businesses**
www.gov.uk/government/news/big-opportunities-for-small-firms-government-set-to-spend-1-in-every-3-with-small-businesses

16 **Supply chain security guidance**
www.ncsc.gov.uk/collection/supply-chain-security

17 **Investigation: WannaCry cyber attack and the NHS**
www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

18 **Oxford Health: Cyber attack continues to hit NHS trust's services**
www.bbc.co.uk/news/uk-england-oxfordshire-63046401

19 **Care home software won't be fully restored until 2023 despite backups**
thestack.technology/staffplan-rebuild-advanced-ransomware/

20 **Congratulations to all our 2021 winners!**
event.computing.co.uk/cloudexcellenceawards2022/en/page/2021-winners

21 **CSO50 and Computing Cloud Excellence Awards Honor CyGlass Customer Waverley Borough Council for AI-based Network Defense-as-a-Service**
www.investegate.co.uk/cyglass/gnw/cso50-and-computing-cloud-excellence-awards-honor-cyglass-customer-waverley-borough-council-for-ai-based-network-defense-as-a-service/20210729130000H8549/

22 **Results 2021**
www.scawardseurope.com/Result

CyGlass | GOV NEWS DIRECT

About Us

CyGlass is a leading provider of cloud and network-centric threat detection and response solutions that help organizations see risks, stop threats, and prove compliance. Our unique 100% cloud-native, AI-driven Network Defense as a Service (NDaaS) platform delivers enterprise-class cyber defense to mid-sized and small organizations at an affordable cost and without hardware or software.

GovNewsDirect

This paper was built in partnership with GovNewsDirect. GovNewsDirect specialise in facilitating innovative and engaging partnerships between the private and public sector.