CASE STUDY

CyGlass by NOMINET

Waverley BOROUGH COUNCIL

WAVERLEY BOROUGH COUNCIL:

Protecting the sensitive data of 126,000 citizens

LOCATED IN THE SOUTH OF ENGLAND WAVERLEY BOROUGH COUNCIL SUPPORTS OVER 123,000 CITIZENS. WITH ASSETS OF OVER 553 MILLION GBP AND AN ANNUAL INCOME OF 73 MILLION GBP, THE WAVERLEY BOROUGH COUNCIL EMPLOYS 450 STAFF, MANAGES 4,800 "COUNCIL HOUSES," AND MANAGES A FULL TIME PENSION FUND.

PROTECTING THE PERSONAL DATA AND INFORMATION OF THE CITIZENS WHO LIVE IN THE BOROUGH IS ONE OF THE COUNCILS TOP PRIORITIES.

CHALLENGE

2020 was a brutal year for cyber attacks and ransomware as cyber criminals expanded their focus to include government organizations and local authorities. The objectives are well known, blackmailing victims with the threat of public leakage of exfiltrated data and paralysing critical systems and infrastructure for weeks on end.

In October, Hackney Borough Council became a victim of a cyber attack and the UK central government communicated to all local authorities, warning that they review their security posture immediately and take steps ensure that they are effective.

Waverley Borough Council took these warnings seriously and working with trusted partner Click26, reviewed their security systems and policies. This review found that Waverley had a solid layered cyber security defense program; good firewall and endpoint security and well-defined cybersecurity awareness training. But the review did find one area where defenses needed improvement, Waverley lacked visibility into their network assets and associated risks. This visibility gap left the council's IT infrastructure and digital assets vulnerable to ransomware, unauthorized web and DNS activities, lateral movement, and data exfiltration. Improving network visibility and defense would add an additional layer of protection to Waverley's already strong defensive architecture. But Waverley Borough Council had to solve this network security challenge with limited budget, and no ability to add headcount to an already very busy IT Team.

REQUIREMENTS

- Understand their network and define where sensitive data was located.
- Correlate and authorize security policies that protect their sensitive data and align to their security framework.
- Automatically learn "normal" network activity and surface any potential threats.
- Automate prioritized alerting of suspicious behaviour without the need for additional resource in the team.
- Improve their ability to mitigate the threat of ransomware attack.
- Continually monitor and measure how existing security tools and policies are performing.

> *"The first step was implementing CyGlass within our network – this could not have been easier. CyGlass is fully automated with interactive scripts and being a fully hosted solution, is non-intrusive and of no risk to our data. We achieved initial traffic flow in 45 minutes. It took just a few days to learn our network, shining a light on many areas that were not easily visible. This helped us highlight and prioritize remediation work much more effectively with limited resources in the team."*
>
> HOWARD DENHART, SERVICE DESK SUPERVISOR

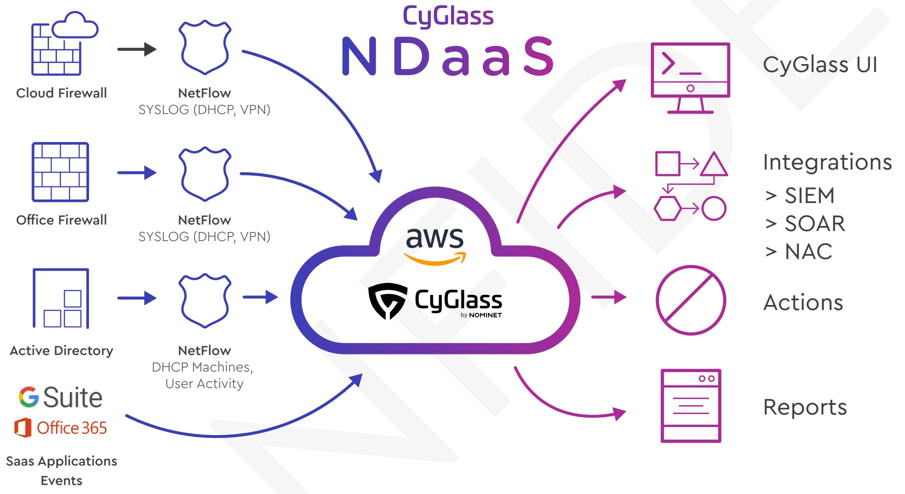
SOLUTION

Click26 turned to Nominet's cyber security division, and its cloud based, AI driven Network Defence as a Service (NDaaS) solution.

NDaaS was a perfect fit for Waverley Borough Council. It met all of the project objectives including visibility of assets and risk on the network, network based threat detection, continual monitoring, and automated detection and response, but most importantly, it required no new hardware and no new headcount.

ACHIEVEMENTS

- ✓ Accurately mapped all network resources and all identified "unknown" systems.
- ✓ Identified, categorized and labelled sensitive assets on the network.
- ✓ Enabled a continual monitoring process that watches network traffic, IT systems and endpoint systems for risks and threats.
- ✓ Deployed security policies that expanded the Council's security framework to cover ransomware attacks.
- ✓ Risky network behaviours – including those indicative of ransomware attacks – are automatically identified and alerts are sent to the IT team 24X7.
- ✓ AI is successfully used to prioritize alerts and focus the small IT team on the threats that pose the greatest risk to sensitive data.
- ✓ Produce consistent, easily digested executive reports demonstrating improved security posture and effectiveness of their technology investments.



> *"CyGlass allowed us to efficiently manage our important alerts. CyGlass has given us a 24/7 pair of eyes, helping to ensure that we continually improve our security posture against ever emerging threats."*
>
> **HOWARD DENHART,**
> **SERVICE DESK SUPERVISOR**

SECURES HYBRID CLOUD

- Visibility across network and cloud, identify rogue assets and abnormal, risky activities
- Monitors users on premise, at home, VPN, AD Azure, O365
- Protects SaaS apps like Salesforce.com, Dropbox

STOP CYBER ATTACKS

- Detects anomalies caused by Ransomware, Insider Threat and other advanced threats
- Blocks user and network access automatically
- Investigate, remediate, and recover

OPERATIONALLY EFFICIENT

- Easy to install – no additional hardware, software or people
- Use existing hardware infrastructure
- Customizable reports
- Monthly per/user pricing