CASE STUDY

UK CITY COUNCIL

Protecting the sensitive data of over 1 million citizens

CyGlass by NOMINET

UK'S LARGEST LOCAL COUNCIL DEPLOYS AN ENTERPRISE SCALE SAAS NDR

UNITED KINGDOM CITY COUNCILS USES A LEADERSHIP INITIATIVE TO SET CYBERSECURITY PROTECTION IN PLACE AHEAD OF THE COMMONWEALTH GAMES WITH AN AI-BASED NETWORK DETECTION AND RESPONSE DEPLOYMENT THAT WILL SERVE AS AN EXAMPLE TO OTHER CITIES AND COUNTIES ACROSS THE UK.

CHALLENGE

Next to London, this local government council is the largest in the UK, representing over one million people. That, alone, makes them a key target for ransomware and other malicious cyberattacks. Alongside the ubiquitous challenges of managing remote workers during the pandemic, the Council is hosting the 2022 Commonwealth Games, putting it even more in the crosshairs as a high-profile target for cybercriminals.

The Council's IT team has already built and deployed a cyber defense "best practices" framework to ensure a robust and systematic security posture that protects against most types of cyber threats. As part of this security framework, the Council sought "class-leading" cyber security protection for its network that would enable it to respond to anomalous activities and cut off an attacker's ability to disrupt/damage services. It was determined that the Council would seek proposals to deploy an AI-driven network threat monitoring and detection tool deployed as a software as a service (SaaS).

THE NETWORK EXPANDS

Like most large organizations, the Council's network is ever-changing, currently spanning multiple data centers and cloud applications, over 12,000 employees, 13,500 devices, and tens of thousands of partner and service provider users in Microsoft Azure. As part of a comprehensive IT transformation around hybrid cloud and digitalization, the cybersecurity team had implemented "Security by Design" and "Security Operations" strategies. Security by Design aims to deliver solutions to protect

REQUIREMENTS

- Identifying all network assets and creating micro segmentation trust zones.
- Monitoring over 30K service provider Azure accounts.
- Monitoring network and Azure environments 24X7.
- Integrating EDR alerts to correlate with Network Threats for Rapid Remediation.
- Improving ransomware defense and minimizing ransomware threat surfaces.
- Eliminating alert fatigue and focusing threat detection and response on high-risk events.
- Deploy a 100% cloud-native SaaS solution

""Upon completion of an extensive RFP process, we found the CyGlass NDaaS platform stood alone in ticking all the requirement boxes for our project, while delivering equal if not better world-class AI at a fraction of the cost of the competition. That was not even the best part, rapid time to value was – we deployed across 130K IP network in a day! NDaaS has delivered on every promise and given us complete visibility into the risks and threats across our network, Azure and M365 environments."

VP of Cyber Defense, UK City Council

THE NETWORK EXPANDS

the organization, its employees, and its citizens. "Security Operations" ensures defense against malicious activity, data breaches, and destruction of critical digital and provides capabilities to monitor and recover from cyber threats.

Network detection and response technology implemented as SaaS is designed to quickly and efficiently analyze the massive amounts of network traffic created by large organizations like the Council. SaaS NDR collects data, using AI to baseline and correlate the actions of network traffic, devices, and user accounts, then compares them against threat intelligence and applies control policies based on threat type and risk level. SaaS NDR allows the Council to discover, detect, and respond to cybersecurity threats while eliminating hardware and software costs and minimizing time/staffing needed to manage legacy NDR tools.

TAKING A LEADERSHIP ROLE IN CYBER DEFENSE

Recently, the Council decided to take IT capabilities in-house, which meant any new security products had to operate within current staffing and operations frameworks. The Council also wanted to set new benchmarks and standards for all county councils across the UK to adopt as best practices. This meant that even though it is one of the UK's largest Council organizations, it wanted to adopt an approach to network defense that would provide superior protection.

According to the Council's Cyber Security Strategy 2020-2024, "We are building secure, sustainable, and innovating capabilities and processes. We aim to become an example to follow amongst the public sector and go-to council, for colleagues while influencing and improving the (our) brand in public services."

THE SOLUTION

The Council undertook an extensive RFP and due diligence process that ultimately selected AI-drive Network Defense as a Service (NDaaS), an innovative solution offered by CyGlass. Functionally, CyGlass stood alone in ticking all the boxes while delivering equal if not better world-class AI at a fraction of the cost of the competition.

Like traditional NDR, CyGlass NDaaS uses a combination of machine learning, advanced analytics, rule-based matching, and threat intelligence to detect anomalous and suspicious activities across cloud and on-premise networks. As a SaaS solution, CyGlass deploys as a cloud-native platform and does not require on-premise hardware, which was critical to meeting the Council's operational framework requirements.

NDaaS aggregates the Council's network and cloud activities, performing threat analysis and correlation and applying threat intelligence to identify related risks and indicators of compromise. The results are delivered via "high-risk" smart alerts, configurable reporting, and an intuitive UI that includes event investigation and immediate remediation.

For the Council, seeing risks across the network and cloud was something new. CyGlass enables managers to see the range and types of assets on the network and identify vulnerabilities that could allow ransomware, such as unsecured port traffic, network traffic to restricted locations, disruptions in scheduled backup activity, or unusual user/admin activity. The team can tag each asset, and as threats and vulnerabilities are detected, CyGlass automatically assigns risk scores to collections of assets so the Council can track prioritize actions based on the severity of the event.

BEYOND VISIBILITY, RESPONDING TO CYBERATTACKS

With NDaaS, the Council can not only see but stop cyberattacks. Its entire network is continually monitored. Smart alerts are generated when correlated anomalies, threat intelligence, or control violations exceed risk thresholds determining an immediate threat. Machine learning algorithms analyze massive amounts of data and deliver near real-time results, identifying and enabling remediation of cyberattacks. The cyber team receives a short, prioritized list of risks and threats, including man-in-the-middle attacks, unauthorized web and DNS activities, masqueraders (tunneling), credential compromise, rogue behaviors, insider threats, lateral movement, and data exfiltration activities. With 24x7 monitoring across all critical networks and cloud-based services, the Council can protect the delivery of information and services to all of its constituents.

EASY DEPLOYMENT IN A LAYERED, INTEGRATED FRAMEWORK

The Council reports that CyGlass NDaaS required no additional customization to be deployed. All configurations were accomplished through point and click interfaces. There is no hardware to procure, install, configure, and maintain. The system tools and dashboards are intuitive and can be rapidly mastered to keep training and downtime to a minimum.

As part of its "class-leading" cyber security framework, the Council is implementing a core set of cyber security technologies. Therefore, the NDaaS solution had to integrate and interoperate with components in the Council's framework, including; Active Directory Cisco routers and switches,

The future of the Council's cybersecurity framework is extended threat detection and response (XDR). The framework will integrate threat detection and direct remediation across the three critical pillars of coverage; network, cloud, and endpoint. Finally, correlating the outputs of all three with threat intelligence feeds to identify indicators of compromise (IOCs). CyGlass NDaaS delivers the network and cloud pillars and includes the required threat intel feeds.

CyGlass integrates AD, Cisco network hardware and Checkpoint firewall logs and data flows, with Sentinel One delivering the advanced endpoint protection. CyGlass NDaaS is fully deployed, and Sentinel One's deployment is underway. The next step is the integration of Sentinel One's EDR threat data and alerts with NDaaS to create a truly integrated threat detection and response framework, which is scheduled for completion in early 2022.

TO THE GAMES AND BEYOND

In the lead-up to and throughout the Commonwealth Games, the Council must manage various technologies required to successfully stage a massive live event. Having a well thought out and tested cybersecurity framework to protect the services provided by the Council is mission-critical to ensure that all participants, viewers, and residents gain the best outcome from the Council's hosting of the Games.

With CyGlass NDaaS, the Council believes it has much-needed network visibility across locations and cloud assets, network blind spots, and rogue devices, including the many IoT devices that will be deployed to support the games. The Council also believes that continuous threat monitoring and risk-based scoring utilizing CyGlass AI and smart alerts will deliver timely, prioritized, actionable threat intelligence to keep the team ahead of any cyberattacks.

Although there are many NDR products and several new SaaS NDRs, CyGlass is currently the only cybersecurity vendor that offers a 100% cloud-native, affordable, single platform solution that is easy to operate and covers both on-premise network and cloud environments. Additionally, the Council believes its CyGlass deployment shows how enterprise-class AI and network security technologies can now be accessible to organizations of all sizes with similar functional requirements. The Council's SaaS AI-driven network defense solution is helping its cybersecurity team meet its goal to become the go-to council to follow amongst its colleagues in the public sector and beyond.

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
- Detects rogue devices and IOT risks and threats

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
- Affordable monthly per/user pricing