Enterprise Class Cybersecurity for Medium and Small Organizations

Challenges

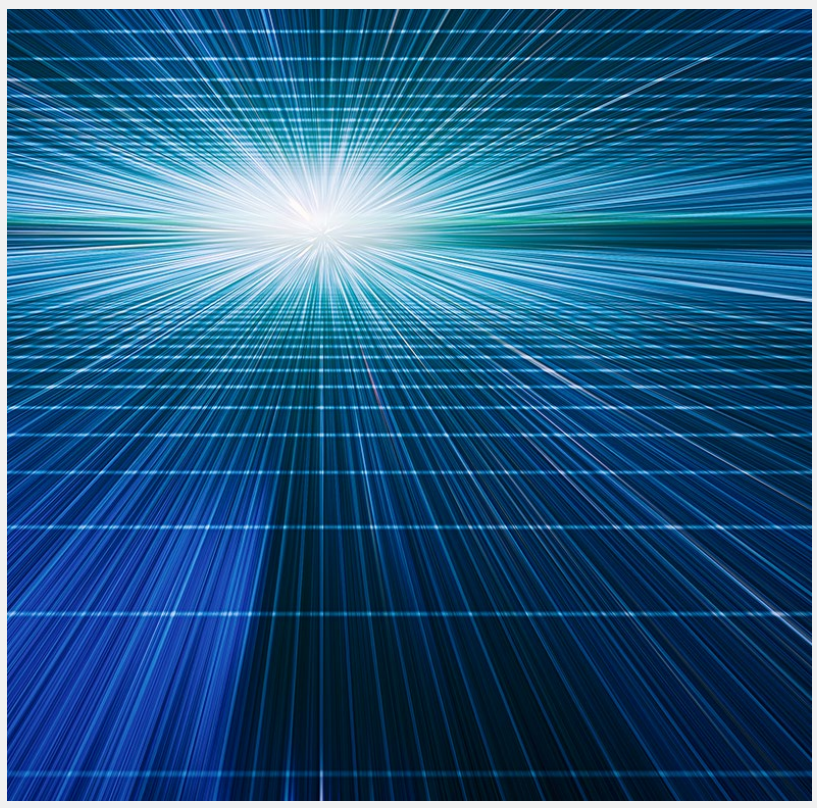
Resource Constrained Teams are Blind to Cloud, Network and Endpoint Threats

To defend an organization from cyberattacks, IT teams must monitor and correlate network, cloud, and endpoint traffic. Traditionally, this has required multiple expensive software and hardware tools and a large group of cybersecurity professionals to run them. This approach is untenable for small and medium-sized organizations, which cannot afford to hire expensive staff or purchase and deploy multiple tools. Resource-constrained teams need visibility to the risks and threats across their entire network and the ability to take action to stop them immediately. They require a solution delivered through simple-to-deploy and operate cloud-native service, including automated compliance controls and reporting.

The CyGlass Solution

Cost effective Enterprise Class Hybrid Network & Cloud Defense

CyGlass Hybrid Network Security is a cost-effective 360-degree risk and threat visibility and remediation solution that runs in the Cloud. CyGlass is explicitly designed for resource-constrained IT teams. The CyGlass platform utilizes Artificial Intelligence (AI) to monitor and correlate threats across user, network, endpoint, and cloud behaviors wherever they emerge: AWS, Microsoft365, Azure, Active Directory, VPNs, firewalls, or network devices. Rapidly deployed without hardware and easy to operate, CyGlass reduces the massive volume of enterprise traffic into easy-to-understand risk-based alerts, investigative views, remediation actions, and threat and compliance reports.



Benefits

CyGlass Hybrid Network Security enables IT and security managers to easily and affordably see risk, stop threats, and prove compliance.

Eliminate Blind Spots

24X7 visibility to cloud, directory, and network systems, including Internet of Things (IoT) devices, surface vulnerabilities, policy failures, and system risks.

Detect Hidden Attacks

AI-based detection combined with cross-event correlation quickly identifies suspicious behavior, not seen by EDR or other tools while automated remediation contain attacks.

Prove Continuous Compliance

With Security Operations (SecOps) scoreboards, threat and risk scoring, and automated compliance reports, CyGlass enables teams to prove compliance 24X7.

CyGlass
a WatchGuard brand

CyGlass on AWS

The AWS platform is core to CyGlass' cybersecurity offering: from the platform's ability to process vast amounts of data, powering our data enrichment and AI models, to its extensibility, enabling our data feeds, enrichment, and correlation processes, to its flexibility which allows us to modify and improve our user experience and automated reporting. Most importantly, by offering a 100% cloud-native solution, CyGlass eliminates the need to deploy and upgrade hardware that costs hundreds of thousands and delays deploys by months. The CyGlass platform is a global offering with customers across Africa, Asia, S. America, N America, Europe, and the UK.

Crown Agents Bank

Case Study: Crown Agents Bank

Challenges

The bank has a small IT and security team, yet cybersecurity was and is critical with over 16 locations worldwide and operations that include sensitive customer and financial data. Challenges: 100% cloud deployment with an aggressive rollout schedule. Easy to operate for a small team, Unified correlation of threats included in compliance reporting.

Solution

CyGlass, with its AI-driven analytics and continuous learning, deployed rapidly and integrated seamlessly with other Crown Agent tools. Within a few hours, CyGlass had surfaced anomalous behavior, correlating threats, automating remediation activities, and improving overall defense posture. Compliance reporting was game-changing, eliminating over 40 hours of manual work in the first month alone.

Results

CyGlass helps Crown Agents Bank understand and reduce its network and cloud risks and protects against cyberattacks. Crown Agents bank is now more resilient and compliant with its many governing regulatory laws, including GDPR and ISO-2700-1. The CyGlass project was completed ahead of time and on budget and continues to expand across Crown Agents' growing hybrid environment

Features

Reduce costs and TCO for mid and small organizations

CyGlass, with its cloud-native architecture, connects to the organizations existing firewalls, routers, directories, data centers, and cloud environment. Deployment times from 30 minutes to a few days significantly increase solution time to value. Our customers achieve total cost of ownership (TCO) savings of 60% or better over legacy NDR or SIEM tools and operate our solution on less than a single FTE. CyGlass automated continuous compliance reporting saves thousands in manual report customization and configuration.

Enable Rapid Threat Detection Globally, 24X7

The SME market has traditionally used only policy-based firewalls to protect its networks, which are ineffective in stopping cyberattacks. Using CyGlass, delivered on the AWS platform, any organization can deploy enterprise-class threat detection and response for network and cloud attacks. CyGlass AI running on AWS meets the operational detection needs of tens of thousands of resource-constrained organizations around the globe.

Visit CyGlass on AWS Marketplace to purchase or start a Free Trial today.

Get started with CyGlass

aws PARTNER

- Qualified Software Partner
- Public Sector Partner
- Marketplace Seller