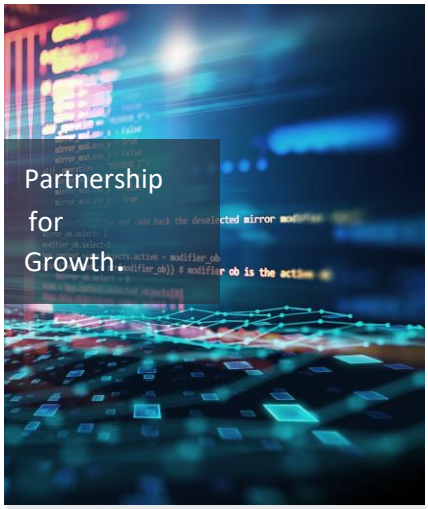
FORESIDE

Cybersecurity Solutions

INVESTMENT ADVISORS AND BROKER-DEALERS OF ALL SIZES ARE A COMMON TARGET FOR THREAT ACTORS FOR OBVIOUS REASONS – THEY POSSESS HIGHLY SENSITIVE CLIENT INFORMATION. IT IS ESSENTIAL THAT ALL INVESTMENT ADVISORS AND BROKER-DEALERS TAKE A PROACTIVE, DEFENSIVE STANCE WHEN IT COMES TO CYBERSECURITY COMPLIANCE.



Foreside's solutions include*:

Cybersecurity Packaged Solutions

Gain 24/7 monitoring, detection, and response to threats

CyberPRO: 24/7 monitoring, detection, and response to cyber threats on endpoints

CyberPLUS: beyond endpoints, this package includes vulnerability scans, SIEM capabilities, and a client portal

Cybersecurity Consulting

Get expert advice and guidance on your strategic cybersecurity initiatives

Penetration Testing

Test your systems and network identify security vulnerabilities

Incident Response Retainer

Prepare for the inevitable with ready-to-deploy experts

**all solutions delivered through our partner, BlueVoyant. For more information on BlueVoyant, please visit https://www.bluevoyant.com/*

Financial firms must innovate or risk becoming obsolete.

At Foreside, we pair comprehensive and customized advice with best-in-class technology to help firms in the investment management space continue to innovate, improve and grow.

We tap state-of-the-art technology to help firms drive operational efficiency and flourish in today's regulatory environment. Foreside's suite of services and platform-based model automate and simplify compliance and distribution for firms, and are designed to scale as clients grow. With Foreside as a partner, firms can dedicate time and effort to portfolio management, client service, sales, and other value-adding work.

Interested in learning more?

www.foreside.com busdev@foreside.com +1.866.251.6920

Cybersecurity Packaged Solutions

Managed Detection Response	CyberPRO	CyberPLUS
24/7 monitoring of endpoints by expert cyber threat analysts	•	•
Cloud-based threat detection platform and technology	•	•
Analyst -led investigations and response to security events	•	•
Live detection of malicious hacker tradecraft and techniques, including lateral spread and file-less attacks	•	•
Active response to detected threats, such as terminating rogue software and isolating compromised devices	•	•
Bundled with Next Generation Antivirus (NGAV) to detect, block, and contain malware, ransomware, zero-days, non-malware and file-less attacks automatically on endpoints	•	•
Automation and orchestration that continuously enhances detections to known threats and improves response times.	•	•

Integrated SIEM (Security Information + Event Management) capabilities:	CyberPRO	CyberPLUS
Extends monitoring and analysis beyond the endpoints		•
Collects and correlates log data from multiple sources, including endpoint, networks, user activity, and other third-party security solutions, providing visibility into risks and threats across multi-cloud and hybrid environments		•
Monitors network and security devices, tracks users, and scans applications		•
Provides real-time security event analysis across your monitored security infrastructure 24/7		•
Monitors the health of installed endpoint agent communications and log sources to ensure they are always working properly		•
Stores collected log data for 30 days for security event analysis		•
Retains collected data in archive storage for one year, or as uniquely specified		•

Vulnerability Scanning	CyberPRO	CyberPLUS
Automated, recurring scanning of your IT environment to identify vulnerabilities		•
Enhances your monitoring service by informing security investigations and response actions with possible root cause and ability to see lateral movement across your environment		•

WaveLength™ Client Portal Experience	CyberPRO	CyberPLUS
Access to our cloud-based client portal where you see an easy-to-understand representation of your security program		•
Ability to interact directly with BlueVoyant's Security Operations Center analysts		•
Full event visibility and access to at-a-glance insights and compliance reports		•

Incident Response Plan Template	CyberPRO	CyberPLUS
Helps streamline the response your team makes to classify events based on overall impact to your organization.		•

Cybersecurity Additional Services

PENETRATION TESTING

Using a three-phase approach, BlueVoyant helps test your systems and network to find and verify security vulnerabilities that could be exploited by a threat actor. All discoveries are documented in a report that will specifically identify deficiencies and recommend improvements.

Includes:

- *Penetration testing for up to 20 IPs*
- *Detailed report of findings with priorities vulnerability and remediation recommendations*
- *Meets regulators recommendations for insider threat monitoring*

CYBERSECURITY CONSULTING

Cybersecurity Consulting provides a bank of hours available for use to address your cybersecurity initiatives.

Hours may be used for security awareness training, development and management of security policies, and other cyber-related intelligence.

Includes:

- *15 hours (max: 10 hours/week)*
- *Immediate access to cybersecurity experts to get technical and strategic advice across a broad range of cybersecurity topics*
- *Security policy templates*

INCIDENT REPONSE RETAINER

The first 72 hours following the discovery of a data breach are critical. The decisions made carry legal, regulatory, investigatory, and public relations repercussions. During this short time period, every decision is critical, and even the most prepared organizations can quickly become overwhelmed.

From forensic collection to the witness stand, BlueVoyant will provide you the answers you need, paired with a superior investigative perspective.

Includes:

- *Retainer agreement tailored to your specific needs*
- *Pre-negotiated terms and conditions to reduce response time*
- *Pre-arranged, rapid response SLA's to minimize breach impact*
- *Meetings regulators recommendations for incident response preparedness**

**https://www.sec.gov/files/OCIE-Cybersecurity-and-Resiliency-Observations-2020-508.pdf*