Solution Brief

Azure Digital Forensics Incident Response (ADFIR) Retainer

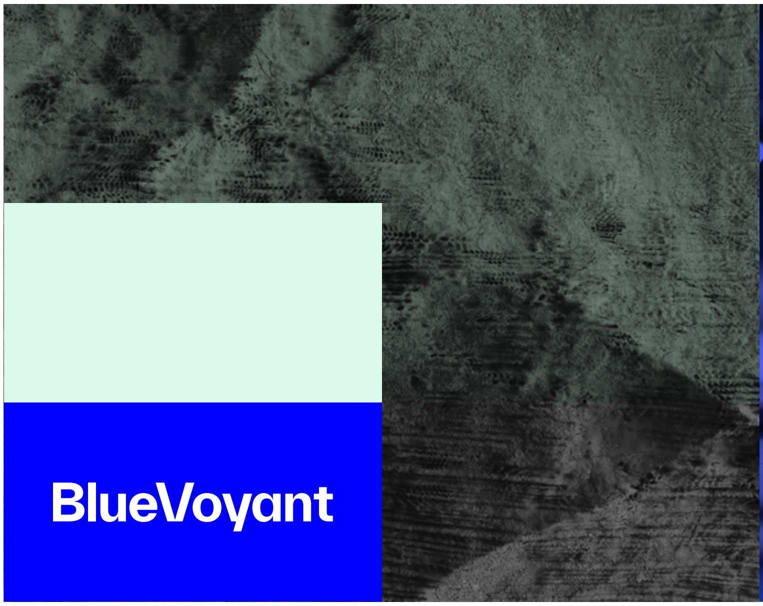
Always-on expert security and investigative team providing forensics and incident response to complement BlueVoyant MDR (Managed Detection and Response) for Microsoft.

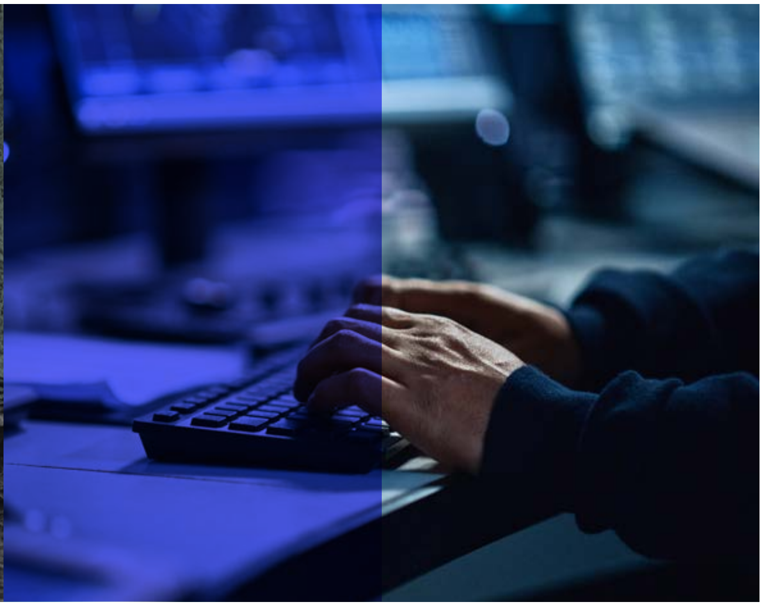
Investigate and manage intelligent and fast-moving threats that occur beyond MDR security workflows

BlueVoyant MDR for Microsoft secures organizations 24×7 across their entire Microsoft estate. We leverage and optimize Microsoft SIEM and XDR technology to deliver the highest security posture possible.

Although MDR provides comprehensive security coverage, many businesses require additional cloud-native incident response, deep digital forensics, or legal testimony support that falls outside the scope and capabilities of MDR

To support our clients and provide complete integrated security services leveraging Microsoft's larger cloud ecosystem, we offer the BlueVoyant Azure Digital Forensic Incident Response (ADFIR) Retainer.





Augment MDR with BlueVoyant's ADFIR Retainer

Kubernetes and SQL database forensics need different tools than endpoint-based forensics. While Defender for Cloud integrated with Sentinel can provide some level of threat monitoring, there is more than just detections needed to thwart bad actors.

Next-generation threats know when they are being hunted, mutate into variants, and transition quickly between apps, servers, networks, and clouds. You need a provider who can follow them where they go and stop them in their tracks.

Microsoft expertise is at the core of both of our services – MDR and ADFIR, but within cybersecurity, they conduct different jobs and need different parts of the Microsoft ecosystem to do their work.

One way to understand how MDR and ADFIR complement each other is to compare them to law enforcement. MDR is similar to the police department. Like the police, MDR manages the vast majority of threats and keeps the environment secure 24×7. ADFIR is similar to a SWAT team or intelligence agency. Like those teams and agencies, ADFIR investigates and manages incidents that are beyond the jurisdiction and capabilities of MDR.

Common ADFIR use cases include:

- Business credential or email compromise
- Compromise assessments and forensics
- eDiscovery/eDisclosure
- Employee offboarding
- Extortion or blackmail
- Government and law enforcement notification
- Data exfiltration and intellectual property theft
- Pre- and post-mergers, acquisitions, and integrations
- Phishing investigations
- Ransomware investigations
- Workplace investigations and insider threats

Incident activities managed by ADFIR include:

- High threat volumes continue to appear in an environment and are eradicated by MDR, but the source is unknown and beyond the reach of MDR sensors and tools.
- An anonymous disgruntled employee is exfiltrating data that appeared on the dark web. You need to discover who, where, how, and for how long the breach has been active.
- A malware threat has been halted by BlueVoyant MDR, but may have mutated and shifted beyond the reach of MDR security services and must be contained.
- Network Time Protocol (NTP) is not working, timestamps are changing erratically, and you can't find the cause. You suspect someone is tampering with timestamps and using this tactic to make tracking their malicious exploits difficult, if not impossible.
- Regulatory compliance requires that a recent incident be reported, which triggered an audit. You'll need to prepare a full incident report, including chain of custody for all artifacts and other digital evidence.

When forensics are required or incidents occur beyond MDR boundaries, ADFIR can help.

ADFIR Retainer vs. Per-Incident Emergency Third-Party Contractor

If you need assistance to track down a threat beyond MDR or conduct a forensics investigation, one option is to engage a one-time, third-party service. But that could take days or even weeks to organize.

- A SOW may need to be created and approved
- Funding and POs need to be processed
- A large portion of time is required for knowledge transfer
- Security clearances and access must be validated and granted
- New or existing agents and tools may need to be installed and shared
- A task team and response plan must be created if one does not exist
- Real-time communication and collaboration must be established

There is also the risk that the third party is not equipped or experienced in working with and optimizing Microsoft Azure security, forensics, and response tools.

If too much time is lost or expertise is lacking, a sophisticated threat will mutate, move, and hide, or worse, exfiltrate data and hold your systems and data hostage.

Immediate response

With BlueVoyant's ADFIR Retainer, our security experts go straight to work investigating, hunting, and halting threats. Our Microsoft MDR Security Operations Center (SOC) team and digital forensics experts act as an escalation path to getting you the resolution you need based on the threat at hand. Moreover, with a retainer everything that would normally take days or weeks to process and implement such as paperwork, access, and tools are either already in place or easy to implement quickly.

Extensive knowledge transfer isn't needed because incident response (IR) teams already have knowledge of your security environment, infrastructure, and the assets you need to protect.

Leveraging the power of Azure

With the ADFIR Retainer, you keep all evidence data in Azure. BlueVoyant's investigators process evidence from your Azure environment in custom-designed Azure forensic labs while maintaining proper chain of custody. With rapid onboarding and scalability by design, scope and associated artifacts can be quickly identified and submitted for a deep-dive forensic analysis while avoiding moving your sensitive evidence data to external third-party platforms.

From forensic collections, root cause analysis, and all the way to the witness stand, we have paired expertise with a superior investigative model that doesn't compromise your data privacy.

Reduce cyber insurance costs

Demonstrating to insurers that you have digital forensics and incident response capabilities will help you:

- Reduce rate increases
- Remove coverage denial or restricted coverage concerns
- Meet coverage security requirements

Moreover, BlueVoyant's incident response retainer may be credited toward your retention or deductible.

Beyond traditional IR retainers

Added benefits of using ADFIR Retainers include:

- Gain access to a team of Azure digital forensics investigators armed with the experience and tools to get you answers without losing chain of custody.
- Our ADFIR team of seasoned threat hunters and forensic investigators have decades of experience in crisis management, forensic investigations, eDiscovery, and cyber incident response. Their experience includes both public law enforcement and the private sector.
- Our directors will personally handle your case and are highly experienced "Incident Commanders" comfortable with guiding your C-Suite through post-breach forensics and legal challenges.
- Augment your internal response staff during periods of high demand, such as forensic root cause analysis, log review, or O365/Azure auditing.
- Perform human resources investigations, insider threat evaluations, and assess severity alerts.
- Annual domain-wide third-party breach report and quarterly threat briefings help you remain vigilant of changing attack vectors.
- Trusted by more than 20 leading cyber insurance companies to perform incident response and forensic investigative services for their insured clients.

Services included with BlueVoyant's Azure Digital Forensic Incident Response (ADFIR) Retainer

Understand the latest attack vectors, realistic data recovery strategies, as well as long-term potential litigation considerations.	Recommend security configuration changes to mitigate risk of further compromises.
Respond to incidents outside of normal MDR workflows.	Pre-negotiated terms and conditions to reduce response time to an incident.
Incident cyber forensic collection, detailed analysis, expert witness, and other litigation considerations, and overall crisis management.	Pre-arranged, rapid response SLAs to minimize breach impact.
Predefined chain of command, processes, pre-authorization with client's third-party suppliers and service providers, communication methods, intervention scope, and monitoring technologies and security perimeter.	Quarterly threat briefings
Root cause investigation of initial compromise and identification of resources and identities accessed by the threat actor.	Annual domain-wide third-party breach report
Environmental audit and threat hunt for persistence methods in Azure and hybrid on-premises environments.	Retainer agreements tailored to your specific needs
Azure log and resource artifact investigation to determine actions taken by the threat actor.	Augmentation to internal response staff during periods of high demand, including forensic root cause analysis, log review, and O365/Azure auditing.
Evidence collection to determine if it was accessed, viewed or exfiltrated.	Perform resource investigations, insider threats evaluation, and identify severity of alerts.
Establish a chain of custody for all evidence collected.	Region-specific benefits: – For EMEA clients, we will perform a high-level Incident Response Gap Analysis, such as a review of the incident response plan, policy, and playbook, as part of the onboarding process. – For U.S. clients, we offer the ability to rollover up to 50% of unused hours into a retainer renewal.

Ready to get started? Learn more.

Notes
Additional Azure licenses may be required. BlueVoyant's ADFIR requires Azure services and licenses depending on customer requirements.

Incident response services are available in most but not all countries. Please contact your BlueVoyant representative to ensure that your country is supported.

BlueVoyant

If you experience an incident, contact us directly at **incident@bluevoyant.com**.