Advanced Threat Defense with Crystal Eye:

A Unified Approach to Cybersecurity & Zero Trust

Red Piranha

Executive Summary

Cyber threat actors are getting smarter, and many attacks can go unnoticed for months, putting businesses at risk. According to Red Piranha's 2025 Threat Intelligence & Ransomware Report, Ransomware incidents have skyrocketed by an alarming 74.42% in just two years. Red Piranha's Crystal Eye Unified Security Platform is engineered to combat this reality by drastically reducing threat dwell time. What often takes the average business 277 days to identify and contain can be reduced to mere minutes with Crystal Eye.

This whitepaper introduces Crystal Eye's holistic cybersecurity solution, detailing some of its key capabilities in

- **Threat Detection, Investigation, and Response (TDIR)**
- **Network Detection and Response (NDR)**
- **Secure remote access via WireGuard VPN integrated with Microsoft Entra ID SSO**
- **Declarative A**uthorization **Service (DAS) for fine-grained Zero Trust access control.**
- **Managed Detection and Response (MDR) as a plug-and-play SOC-as-a-Service**
- **Passive Encryption Control for OT and Critical Infrastructure asset protection**

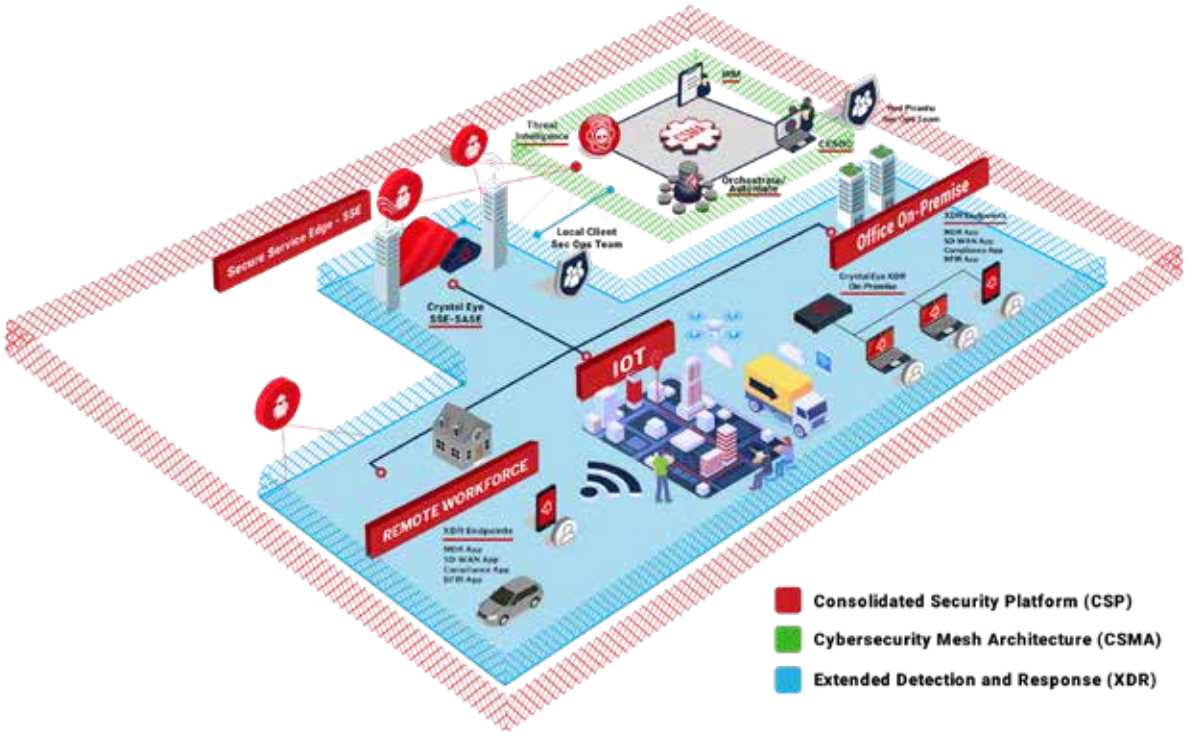
These components work in concert to provide enterprise-grade protection in a unified, easy-to-manage platform.

Unlike fragmented, multi-vendor security stacks that increase complexity and create blind spots, Crystal Eye delivers full-spectrum protection through centralised management, correlated telemetry, and automated, policy-driven response workflows.

A key differentiator is Red Piranha's Augmented MDR-as-a-Service, which provides 24×7 detection and response capabilities, backed by expert analysts and driven by machine-speed automation. Organizations can deploy Crystal Eye rapidly and gain operational SOC capabilities without needing internal teams or third-party integration efforts, significantly reducing time-to-value and operational overhead.

Together, these components form a defense-in-depth ecosystem that empowers organizations to:

- Detect and respond to threats in real time
- Enforce Zero Trust access principles across users, services, and APIs
- Secure remote connectivity without compromising performance or visibility
- Automate investigation and containment workflows across network, endpoint, and cloud



Crystal Eye combines multiple security functions. From next-generation firewall and intrusion prevention to endpoint and cloud monitoring into a single pane of glass. This unified approach helps eliminate security blind spots caused by siloed tools and enables automated, coordinated responses to threats across your entire environment. The platform's advanced TDIR capabilities leverage high-fidelity detection engines and threat intelligence to spot both known malware and elusive advanced persistent threats (APTs) in real-time.

Its NDR module gives deep network visibility (capturing lateral "east-west" traffic within the network) to uncover hidden attackers, boasting up to ten times more visibility into threats than traditional firewalls in its class.

At the same time, Crystal Eye's integrated WireGuard VPN provides lightning-fast, encrypted connectivity for remote users up to 6× faster than legacy VPNs with seamless single sign-on (SSO) through Microsoft Entra ID for strong authentication. Finally, the platform's Declarative Authorization Service enables organizations to enforce Zero Trust principles, ensuring that every access to sensitive applications or APIs is tightly controlled and need-based, without adding administrative burden.

Modern Cybersecurity Challenges

Organizations today operate in a threat environment that is more challenging than ever. Cyber adversaries from organised crime rings to nation-state APT groups are employing stealthy, advanced techniques to breach defenses.

Ransomware and targeted attacks have surged, often bypassing traditional perimeter security. APTs may infiltrate networks and remain undetected for months by using legitimate credentials or "living off the land" tactics, blending into normal activity. The rise of remote work and cloud services has expanded the attack surface beyond the corporate firewall, rendering legacy security architectures less effective.

At the same time, security teams struggle with operational complexity and resource constraints. Many enterprises have accumulated a patchwork of point solutions such as separate firewalls, intrusion detection systems, endpoint antivirus, SIEMs, etc. This do not always interoperate smoothly.

This fragmented toolset creates data silos and blind spots, where critical alerts can be missed amidst the noise. Managing multiple consoles and integrating data from disparate systems taxes already-stretched IT staff. Smaller businesses (SMBs) often lack the specialised personnel and 24×7 coverage needed to effectively monitor and respond to threats across all these tools.

People, process, and technology gaps make it difficult to mount a robust defense. The cybersecurity skills shortage is well documented. Finding and retaining experienced analysts to run an in-house Security Operations Center (SOC) is costly and challenging.

Meanwhile, compliance requirements (GDPR, PCI DSS, ISO standards, etc.) are growing more stringent, demanding better visibility into security events and faster incident response. In many cases, businesses are also pursuing a "Zero Trust" strategy (never assume implicit trust for any user or device) to counter sophisticated breaches, but implementing Zero Trust requires new levels of granular control and verification across the IT environment.

In practical terms, modern CISOs and IT managers face questions such as: How can we detect a breach faster, before attackers do serious damage? How do we investigate and contain incidents with agility, even after hours? Can we simplify our security architecture so that it's both more effective and easier to manage? How do we secure a rapidly growing remote workforce without sacrificing user productivity? And importantly, how do we enforce least-privilege access to sensitive systems to limit what an attacker can do if they do break in?

These challenges call for a more unified and intelligent approach to cybersecurity. Rather than relying on a fragmented array of point products, forward-thinking organizations are moving toward integrated platforms that combine multiple security functions and share information in real time.

By unifying threat detection across network, endpoint, and cloud; automating investigation workflows; and enforcing strict access controls, such platforms can dramatically improve an organization's security posture. This is exactly the ethos behind Red Piranha's Crystal Eye Unified Security Platform. In the next section, we introduce Crystal Eye and how it is designed to tackle these modern challenges head-on.

As mentioned earlier, point solutions often address only one aspect of cybersecurity, leaving gaps in an organization's defense.

For example:

- **A standalone access control tool may enforce policies but lacks visibility into network-level anomalies.**
- **An independent threat detection system might flag suspicious activities but cannot dynamically adjust access controls to prevent further compromise.**
- **A network monitoring tool might detect unusual traffic patterns but lacks the contextual understanding of user or application-level activities.**

By integrating DAS, TDIR, NDR and Wireguard, Red Piranha overcomes these limitations, creating a cohesive defense mechanism where each component enhances the others.

This integration:

- **Closes Gaps**: Provides comprehensive visibility from endpoints to the network core, eliminating blind spots.
- **Improves Efficiency**: Reduces operational complexity with unified management, centralised reporting, and fewer false positives.
- **Enhances Proactivity**: Combines real-time intelligence from TDIR with automated responses from DAS and continuous network monitoring by NDR.

Red Piranha's Crystal Eye Unified Security Platform

Crystal Eye is Red Piranha's flagship unified security platform, built to deliver comprehensive protection through a single, consolidated system. In essence, Crystal Eye functions as a multi-layered security nerve center for your organization. It combines the capabilities of a next-generation firewall, intrusion detection and prevention, endpoint protection, secure gateways, threat intelligence feeds, and more into one integrated platform.

This unified approach addresses the complex challenge by avoiding the need to configure and monitor a dozen different security products. Instead, Crystal Eye correlates data and events across your entire environment (network, endpoints, and cloud) and enables automatic or one-click responses, all through a single pane of glass.

At its core, Crystal Eye provides a defense-in-depth strategy in one solution. It serves as a next-generation firewall at the network perimeter, inspecting traffic with advanced threat detection engines and enforcing policy. Simultaneously, it aggregates security telemetry from internal network segments (via NDR sensors), from endpoints (via an EDR agent or log collectors), and even from cloud infrastructure or SaaS applications.

By consolidating Cloud, Network, and Endpoint Detection with Extended Response capabilities, Crystal Eye ensures that an attack noticed on one vector (say, a suspicious process on an endpoint) can be correlated with activity on another (like that endpoint communicating with a known malicious server) in real time. This complete visibility means security operators can identify multi-stage attacks that would evade isolated tools.

Key Characteristics:

Threat Detection and Investigation Response (TDIR)

TDIR provides real-time detection and mitigation capabilities that integrate seamlessly with other security layers:

- **Advanced Threat Identification**: Employs behavioural analytics and signature-based detection for early identification of malicious activities.
- **Dynamic Incident Management**: Automates the containment of threats by orchestrating actions across DAS and NDR, such as quarantining endpoints or locking compromised accounts.
- **Forensic Capabilities**: Ensures complete auditability with detailed event logging, aiding in compliance and post-incident reviews.

Network Detection and Response (NDR)

NDR enhances network visibility and protection through:

- **Behavioural Analysis and Anomaly Detection**: Utilises machine learning models to establish baselines and detect deviations that could indicate malicious behaviour.
- **Integration with DAS and TDIR**: Leverages access logs and threat intelligence to provide a correlated, multi-dimensional view of security events.
- **Proactive Defense Mechanisms**: Automatically blocks malicious traffic while dynamically updating DAS policies to mitigate insider threats or prevent lateral movement.

Declarative Authorization Service (DAS)

DAS enforces a fine-grained, policy-driven access control model that dynamically adjusts based on user roles, attributes, and real-time threat intelligence. Key technical advantages include:

- Declarative Policy Enforcement: Implements policy-as-code principles, enabling automated and precise access decisions aligned with zero-trust frameworks.
- Centralised Management: Manages access control policies across hybrid and multi-cloud environments from a single pane of glass, reducing configuration drift and ensuring consistency.
- Integration with Threat Intelligence: Responds dynamically to TDIR's insights by revoking or escalating access permissions, mitigating risk in real time.

Crystal Eye's WireGuard VPN delivers high-speed, secure, and flexible remote access. With up to 6× faster performance than legacy VPNs, it leverages UDP-based, kernel-level integration to reduce latency. Security is enhanced through ChaCha20 encryption and Curve25519 key exchange, making it resistant to cryptographic attacks. Additionally, organizations can choose between split-tunnel mode (routing only corporate traffic through the VPN) or full-tunnel mode (encrypting all traffic), offering deployment flexibility based on security needs.

Microsoft Entra ID SSO Integration

- **Seamless Authentication**: Users log in with Azure AD credentials, eliminating separate VPN passwords.
- **MFA & Conditional Access**: Enforces Microsoft 365 multi-factor authentication and security policies.
- **Automatic Access Control**: Revokes VPN access when an Azure AD account is disabled, preventing orphaned accounts.
- **Effortless Management**: Centralised identity-based access control simplifies administration.
- **ZTNA Compliance**: Every connection is authenticated and end-to-end encrypted.
- **Real-Time Threat Detection**: Crystal Eye NDR & TDIR actively monitor VPN traffic for anomalies.
- **Incident Correlation**: VPN logs are integrated with security events, improving SOC visibility.

Seamless Integration of Security Controls

Crystal Eye includes a rich suite of security controls out-of-the-box firewall, intrusion detection/prevention (IDS/IPS), secure web gateway, email security, data loss prevention, vulnerability scanning, and more all integrated.

These components share intelligence automatically. For example, if the IDS detects a new malware signature on the network, that information can feed into firewall rules or endpoint responses immediately, without manual intervention. This eliminates the integration gaps found in a multi-vendor setup, creating a continuous security fabric with no blind spots.

- **Single-Vendor Simplicity**: By consolidating capabilities, Crystal Eye significantly reduces the operational overhead on IT teams. There's one vendor to engage with for support and updates, and one intuitive management console to learn. This ease-of-use is by design. Red Piranha has aimed Crystal Eye to be "extreme security that is both easy to use and affordable" for organizations including MSPs and SMEs. Routine tasks like applying security updates, viewing reports, or adding a new site into the secure network fabric are streamlined through centralised management.

- **Scalable Deployment Options**: Recognising diverse infrastructure needs, Crystal Eye can be deployed as a physical appliance, virtual machine, or cloud service. For example, enterprises can install Crystal Eye appliances on-premises at their main offices or data centers (available in form factors from a small desktop appliance up to rack-mounted servers. These on-prem devices can work in tandem with Crystal Eye Secure Service Edge (SSE), a cloud-delivered SASE option, to extend protection to branch offices and mobile users. This flexible architecture allows organizations to protect assets wherever they reside on-site, in cloud, or at the network edge – under a unified policy framework.

Crystal Eye provides a unified shield for the modern enterprise. It is engineered to reduce risk, detection time, and complexity all at once. By leveraging integrated threat intelligence, automation, and a comprehensive suite of controls, it helps businesses stay ahead of hackers and meet compliance requirements with ease. The following sections will unpack specific pillars of Crystal Eye's functionality: TDIR for security operations, NDR for network threat visibility, WireGuard VPN for secure connectivity, and DAS for Zero Trust enforcement.

Crystal Eye TDIR and Its Role in Security Operations

Security teams face significant challenges with fragmented tools, overwhelming alert fatigue, and delayed responses, allowing sophisticated threats like multi-stage attacks to evade detection and escalate. According to Gartner, Threat Detection, Investigation, and Response (TDIR) is a foundational pillar of modern cybersecurity, driven by the escalating sophistication of adversaries leveraging EDR bypass techniques, fileless attacks, and zero-day exploits.

Red Piranha's Crystal Eye TDIR solution addresses these pain points by integrating advanced threat detection using machine learning, behavioural analytics, and real-time threat intelligence to identify subtle attack patterns others miss.

It encapsulates the end-to-end workflow of modern security operations, from spotting signs of an intrusion to digging into the details and taking action to mitigate the threat. Red Piranha's Crystal Eye platform elevates TDIR to a new level by combining advanced technology with efficient processes ("playbooks") in a single system. The goal is to empower security teams (even small ones) to quickly and efficiently identify, assess, and respond to all threats, known or unknown.

At the Threat Detection stage, Crystal Eye employs best-in-class detection engines across multiple domains. This includes signature-based detection (with an enormous library of constantly updated IDS/IPS rules – over 70,000), anomaly and behaviour-based detection using machine learning, and integrated threat intelligence feeds for spotting known bad IPs or domains.

The platform monitors network traffic, endpoint activity, user behaviour, and more, looking for the faint traces of malicious activity that others might miss. For instance, Crystal Eye can detect signs of an attacker's "kill chain" – from the initial compromise (e.g., a phishing payload or exploit) to persistence mechanisms (like suspicious registry changes on endpoints) and lateral movement (such as unusual use of administrative protocols internally). These detection capabilities are continuously refined by Red Piranha's security research team, meaning customers benefit from up-to-date knowledge of the latest threats.

Once an alert is raised, the Investigation phase kicks in. Traditionally, analysts would need to pivot between different tools (firewall logs, server logs, EDR console, etc.) to investigate an incident, often losing time.

Crystal Eye's TDIR unifies this process: all relevant data is available in one console, with intuitive dashboards and drilldowns for forensic analysis. The platform automatically correlates related events to paint a full picture.

For example, if malware is detected on one host, Crystal Eye can show which other systems that host communicated with, what files were changed, and if any unauthorised access to resources was attempted – all within the same interface. This correlation is powered by the platform's advanced analytics and lateral movement detection capabilities, which connect the dots between network events and endpoint events that share common indicators.

Crystal Eye also enriches alerts with context from its threat intelligence (e.g., "this IP is associated with a known APT group command-and-control server") to prioritise and guide the investigation.

During investigation, analysts can leverage built-in tools such as full packet capture analysis (PCAP) for deep network forensics or utilise the integrated Digital Forensics and Incident Response (DFIR) module if a deeper endpoint investigation or memory analysis is needed.

The platform's design supports human-machine teaming, meaning it augments human analysts with AI-driven suggestions (for example, highlighting an unusual pattern that merits attention) while also allowing experts to apply their intuition and expertise. This significantly improves incident triage and reduces alert fatigue, as the system helps filter out false positives and highlight the most critical threats.

Finally, Response is where Crystal Eye also shines as a solution. Once a threat is confirmed, the platform can automatically or manually execute a range of response actions. These include network containment (e.g., isolating a compromised device or blocking an attacker's IP across the firewall), endpoint containment (like killing a malicious process or quarantining a file via the EDR component), and even user account actions (disabling a breached account via integration with directory services).

Automated playbooks can be configured so that, for instance, if ransomware is detected on one machine, Crystal Eye's SOAR (Security Orchestration, Automation and Response) logic will immediately cut off that machine from the network and initiate a backup restore, all before the security team even steps in. This dramatically reduces response time and damage.

Crucially, Crystal Eye's TDIR approach is risk-based and context-driven. It helps security teams prioritise the most dangerous threats first, reducing the dwell time of attackers. By focusing on high-fidelity alerts (through correlation and context) and enabling swift containment, TDIR minimises the "opportunity window" for attackers to achieve their objectives.

From a security operations perspective, deploying Crystal Eye with TDIR means you're effectively getting an augmented SOC capability. Many organizations pair the platform with Red Piranha's 24×7 monitoring service (CESOC) or their own MSSP, wherein expert analysts watch the alerts around the clock.

But even for internal teams, TDIR in Crystal Eye offers "force multiplication": fewer analysts can successfully manage more threats thanks to automation and integration. In short, TDIR is the brains of Crystal Eye's operation, orchestrating detection and response across all other components. Next, we'll zoom in on one of those critical components Network Detection and Response (NDR) which feeds richly into the TDIR process by revealing what's happening on the network in real time.

How Crystal Eye NDR Enhances Network Visibility and Threat Mitigation?

Networks are the common thread that connects all digital assets in an organization and increasingly, they are the highways attackers use to move between systems or exfiltrate data. Network Detection and Response (NDR) is all about shining a light on this traffic and intervening when malicious activity is detected. Crystal Eye's NDR module is a powerful tool that gives security teams unprecedented visibility into network communications and the ability to detect and disrupt threats in transit before they cause harm.

Traditional network security often relied on perimeter defenses (like firewalls) that inspect traffic entering or leaving the corporate network. However, modern threats easily bypass the perimeter through stolen credentials, VPN access, or malware that an employee inadvertently brought inside and then operate laterally within the network (east-west traffic) where traditional firewalls might not inspect closely.

Traditional Endpoint Detection and Response (EDR) solutions primarily focus on individual devices within a network. While they play a vital role in identifying and mitigating threats at the endpoint level, they often struggle against advanced attack techniques. For example, the Red Piranha threat intelligence team has identified suspected SAIGA Threat Actors who exploited Australian Legal Sector with EDR Bypass. Another example is of the AvNeutralizer, developed by the notorious FIN7 hacking group, as a prime example of how threat actors are advancing their techniques to bypass traditional defenses, particularly Endpoint Detection and Response (EDR).

Red Piranha's Network Detection and Response (NDR) solution provides a more robust and comprehensive security approach by monitoring the entire network infrastructure. Unlike EDR, which is limited to endpoint-specific threats, NDR offers visibility across all network traffic, including east-west communications between internal systems. Powered by Crystal Eye, this solution establishes a baseline of normal network behaviour, allowing it to detect even the subtlest deviations that could signal a potential threat. especially those that evade traditional endpoint defenses.

Crystal Eye NDR addresses this gap by monitoring all network traffic, including internal traffic among devices, in real time. By deploying Crystal Eye sensors or appliances at strategic points (such as core switches or cloud VPCs), organizations gain a full picture of which devices are talking to whom, on which protocols, at what times.

Key Capabilities of Crystal Eye NDR:

- **Advanced Threat Detection in Network Traffic**: Crystal Eye NDR uses a combination of signature-based detection (leveraging IDS rules for known threats like malware command-and-control signatures) and anomaly detection. The anomaly detection employs machine learning and User/Entity Behaviour Analytics (UEBA) to establish a baseline of "normal" network behaviour and then flag deviations. For example, if a device suddenly starts communicating with an IP in a foreign country that it's never contacted before, or if there's a spike in data transfers at 3 AM, NDR will alert on those anomalies. This helps catch stealthy attackers who might be using novel techniques that don't match known signatures, the system sees that something strange is happening even if it isn't a known malware pattern.

- **East-West Traffic Monitoring**: Unlike many tools that focus only on north-south traffic (in/out of the network), Crystal Eye NDR is explicitly designed to monitor lateral movements. This means even if an attacker slips past the endpoint protection, their attempts to probe other servers or move laterally will be picked up. Living-off-the-land attacks, where hackers use legitimate tools like PowerShell or WMI over the network, are notoriously hard to spot, but NDR can identify unusual uses of these protocols or unusual access patterns that suggest malicious intent. This was the case in the Volt Typhoon example, where NDR was crucial in identifying abnormal internal activities that endpoints alone did not catch.
- **Integrated Threat Intelligence (CTI)**: The NDR doesn't operate in isolation. It's fed by contextual threat intelligence feeds. Crystal Eye correlates network observations with known threat indicators (malicious IP addresses, domains associated with phishing, threat actor TTPs, etc.) from Red Piranha's threat intel database. This means if a device in your network reaches out to a server that's known to be a malware drop site, you get an immediate alert with context ("contact with blacklisted IP X associated with malware family Y"). Such integration greatly speeds up analysis, because the security team understands why a certain traffic flow is dangerous. The platform's threat intel is continuously updated (Red Piranha is a top contributor to the global Cyber Threat Alliance), ensuring protection even against emerging threats.
- **Encrypted Traffic Analysis**: As encryption becomes ubiquitous (even malware uses HTTPS these days), seeing into that traffic is vital. Crystal Eye's NDR supports encrypted traffic inspection and analysis. Through techniques like SSL/TLS inspection (on the Crystal Eye appliance acting as a proxy) or analysing packet metadata patterns, the platform can detect threats that try to hide in encrypted channels. For instance, a sudden spike in encrypted traffic from an internal database server to an external host might indicate data exfiltration. NDR can flag this for investigation while decrypting when necessary to confirm the contents. Having this capability provides greater protection across multiple attack vectors, even when attackers use encryption as a shield.
- **Automated Network Response**: True to the "response" in NDR, Crystal Eye isn't just passively monitoring. It can actively intervene when a threat is confirmed. This might include instructing the Crystal Eye firewall to block certain connections or quarantining a suspicious device by cutting off its network connectivity. The NDR can work hand-in-hand with the platform's orchestration engine. For example, if malware is detected spreading over the network, NDR can trigger a response to isolate affected systems and halt the spread within seconds. Automated containment drastically reduces the potential blast radius of an attack.
- **Deep Packet Capture and Forensics**: For incidents that require deeper analysis, Crystal Eye NDR can capture full packet data. Security analysts can retrieve PCAP files around an event to thoroughly inspect the network exchanges (useful for complex malware or data exfiltration cases). The platform also maintains a long-term data lake of network metadata with by default 18+ months storage. This archival is incredibly useful for forensic investigations or compliance audits, as analysts can retroactively trace an attacker's actions or verify that no unknown communications occurred during a given period.
- **High Protocol Coverage and Customization**: Out-of-the-box, Crystal Eye NDR can parse over 3,200 network protocols far beyond just web or email traffic. This includes industrial control system protocols (SCADA), IoT traffic, and other niche protocols. For any proprietary protocols unique to your environment, the platform supports custom parser development. This means no matter what unique systems or devices you have on your network, Crystal Eye can be configured to monitor them. Such broad coverage ensures attackers can't simply hide by using a non-standard port or protocol.

All these capabilities translate to practical security outcomes. With Crystal Eye NDR deployed, organizations typically see a dramatic increase in threat visibility. More visibility means earlier detection of attacks, which means you can stop attacks before they escalate.

It's worth noting that Crystal Eye NDR is designed to be deployed with minimal disruption. It can be set up in a span port (passive listening) mode or inline. Many choose to start with out-of-band monitoring (so it won't impact traffic flow) and then move to inline blocking mode for active response once comfortable. The platform's in-line deployment is achieved without major network redesign, and the single-platform approach also means lower total cost of ownership to achieve world-class detection. In fact, by avoiding multiple separate NDR, SIEM, and SOAR tools, Crystal Eye offers significantly reduced complexity and cost for what you get.

In short, the NDR module of Crystal Eye acts as the eyes on your network's "dark corners," catching threats that other controls might overlook and giving you the chance to destroy threats in transit. It feeds invaluable data into the broader TDIR process, ensuring that whether a threat originates inside or outside your network, you have the actionable intelligence to respond. Next, we'll shift focus to securing the network entry point for many threats – remote access – and how Red Piranha leverages WireGuard VPN integrated with Entra ID SSO to lock that down with speed and simplicity.

Securing Remote Access with WireGuard and Microsoft Entra ID SSO

Remote access has become a lifeline for modern businesses enabling employees, contractors, and distributed teams to connect to corporate resources from anywhere. However, it's also a prime target for attackers, who exploit VPN vulnerabilities or steal credentials to slip into networks undetected.

Traditional VPN solutions (like IPsec or older SSL-VPNs) are increasingly showing their age in this regard. They can be slow, complex to manage, and sometimes rely on outdated cryptographic standards. Red Piranha's Crystal Eye addresses this by integrating a state-of-the-art VPN solution – WireGuard – and pairing it with Microsoft Entra ID Single Sign-On (SSO) for robust, seamless user authentication. The result is secure remote access that aligns with Zero Trust principles (verify every user, every time) while dramatically improving performance and user experience.

Why Legacy VPNs Fall Short?

Many legacy VPNs were designed in an era of lower bandwidth needs and have grown into bulky systems with large codebases. This complexity not only introduces more potential vulnerabilities (a larger attack surface) but also hampers performance. It's not uncommon for old VPNs to become network bottlenecks, adding latency and slowing down cloud applications. Configuration and maintenance are another pain point: setting up IPsec tunnels or managing certificates and pre-shared keys can be notoriously error-prone and time-consuming.

Furthermore, not all legacy VPNs integrate easily with modern identity platforms or multi-factor authentication, leading to separate credentials that users must manage (and attackers might phish for).

These issues have real security implications: a misconfigured VPN or an unpatched VPN server can open the door for breaches, and slow VPN performance might lead users to seek unsanctioned workarounds.

Crystal Eye WireGuard – A Modern, High-Performance VPN

WireGuard is a relatively new VPN protocol that has rapidly gained praise in the security community for its simplicity, speed, and strong cryptography. It consists of only a few thousand lines of code (compared to hundreds of thousands in IPsec/OpenVPN), which means fewer bugs and vulnerabilities, plus faster execution.

Crystal Eye's built-in WireGuard VPN leverages this minimalist design to deliver significant performance gains – up to 6× faster throughput than legacy VPNs. This is achieved through efficient use of UDP and kernel-level integration, minimising overhead and latency. In practical terms, remote users will notice smoother connectivity: large file transfers, voice/video calls, and cloud application access all work with minimal lag, even compared to direct connections.

Despite its light weight, WireGuard doesn't skimp on security. It uses cutting-edge cryptographic algorithms by default (such as ChaCha20 for encryption and Curve25519 for key exchange) that are considered extremely secure and also optimized for performance. This means the VPN tunnel is highly resistant to cryptographic attacks and is future-proof against most emerging threats. The protocol also has built-in resistance to common VPN attacks like replay attacks, and it supports strong peer authentication. In Crystal Eye's implementation, WireGuard can be configured in either split-tunnel mode (only corporate traffic goes through VPN, internet bound traffic goes out locally) or full-tunnel mode (all traffic encrypted through VPN) depending on security requirements.

Integration with Microsoft Entra ID SSO

Perhaps one of the most compelling features is how Crystal Eye ties WireGuard into Microsoft Entra ID (formerly Azure Active Directory) for authentication. Instead of static VPN credentials or separate user databases, users can log in to the VPN using their existing company Azure AD accounts. This SSO approach provides multiple benefits:

- By leveraging Azure AD, you can enforce Multi-Factor Authentication (MFA) and conditional access policies on VPN logins just like any other corporate login.
- Users authenticate with the familiar corporate login page – if they're already signed into Microsoft 365, the VPN connection can even be nearly transparent. There's no separate VPN password to remember, and access can be granted or revoked centrally. When an employee leaves the organization, disabling their account in Entra ID automatically revokes their VPN access, closing a common gap where orphaned VPN accounts might otherwise linger.
- For IT administrators, integrating with Entra ID means no duplication of user directories or manual sync processes. Crystal Eye fetches the necessary user and group info from your Azure tenant allowing you to easily assign VPN permissions. The Declarative Authorization Service (DAS) can even leverage these groups to enforce which users are allowed to reach which services (more on DAS in the next section). Overall, managing access for hundreds or thousands of users becomes much more efficient with centralised identities.

Bringing WireGuard and Entra ID together, Crystal Eye effectively delivers a Zero Trust Network Access (ZTNA) solution. Trust no connection until the user's identity is verified (via SSO/MFA) and the device is known.

Every remote session is encrypted end-to-end with strong protocols. And because it's all part of the Crystal Eye platform, NDR and TDIR are watching the VPN traffic too suspicious activities by a VPN user (say an authenticated user trying to access unauthorised systems) can be detected and stopped in real time, which is synergy we discuss in the next section. Moreover, by integrating remote access into the broader security platform, the company's SOC team can correlate VPN access events with other security events. For example, if a certain VPN user account triggers an IDS alert on the network, Crystal Eye's TDIR can tie those together in an incident report ("User X's VPN session was active when a threat was detected on subnet Y"). This is far more insightful than separate systems would be.

To summarise, Crystal Eye WireGuard with Entra ID SSO delivers secure, high-performance remote connectivity. It exemplifies how embracing newer technology can resolve the old trade-off between security and usability.

Organizations get the best of both worlds: up to 6× faster VPN connections alongside strengthened authentication and simpler management. In the next section, we will explore the Declarative Authorization Service (DAS), which complements this by controlling what users (remote or local) can do once they are connected implementing fine-grained Zero Trust policies within the network.

Implementing Zero Trust with Declarative Authorization Service (DAS)

Even after authenticating users and securing the network channels, a core Zero Trust principle remains: "Never trust, always verify, enforce least privilege." This means that within your network and applications, every request for access should be evaluated against strict policies – does this user need to access this resource at this time?

In hybrid and dynamic environments, traditional access control mechanisms have failed to keep pace with the evolving threat landscape. Organizations still rely heavily on static firewall rules, hardcoded ACLs, and coarse-grained IAM policies that lack the precision and agility needed to enforce Zero Trust principles.

The Problem: Static Access Controls Don't Work Anymore

Security teams are often forced to choose between usability and security:

- Granting broad access to ensure workflows aren't disrupted.
- Manually managing ACLs across different environments (cloud, on-prem, internal apps).
- Lacking real-time visibility into who is accessing what, when, and why.

This opens the door to:

- **Excessive privilege sprawl**, making lateral movement easier for attackers.
- **Policy drift and misconfigurations**, especially in multi-cloud setups.
- **Delayed response**, where revoking access in a live attack scenario takes too long.

Red Piranha's Crystal Eye platform includes a feature called Declarative Authorization Service (DAS) to meet this need. DAS provides a centralised, fine-grained access control system that allows organizations to define and enforce who (or what service) is allowed to access specific applications or data, and under what conditions. It's a powerful tool for reducing internal attack surface and preventing unauthorised lateral movement, even if an attacker somehow slips inside the network.

Red Piranha built DAS to solve the problem of dynamic, fine-grained access enforcement in modern Zero Trust architectures. DAS centralises access control decisions and allows organizations to declare precise, real-time policies like:

- "Only the HR team can access the payroll API during business hours."
- "Block any access to financial systems from users flagged as high-risk by threat intel."
- "Quarantine service-to-service communications if anomalous behaviour is detected."

These policies are enforced instantly, across all environments, using policy-as-code powered by OPA (Open Policy Agent) and integrated deeply.

As cloud environments become more dynamic and distributed, enforcing consistent and context-aware access control across services, APIs, and identities is critical. Red Piranha's Declarative Authorization Service (DAS) is engineered to serve as a foundational component of modern Cloud Access Security Broker (CASB) and Cloud-Native Application Protection Platform (CNAPP) architectures, as recognised by Gartner.

By applying policy-as-code principles and leveraging integrations with identity providers, DAS enables fine-grained, real-time authorization across cloud-native and hybrid workloads. It aligns with CNAPP objectives by delivering centralised policy enforcement, runtime protection, and least-privilege access control across multi-cloud and on-prem environments all from a single platform.

DAS not only protects cloud applications and APIs but also closes the enforcement gap between detection and access management by integrating tightly with Crystal Eye's TDIR and NDR engines. This allows security teams to shift from reactive defense to proactive, context-driven Zero Trust enforcement, ensuring compliance and threat resilience at scale.
Key Features of Crystal Eye's DAS:

- **Fine-Grained Policy Definitions**: Unlike coarse network firewall rules that might just allow or block traffic by IP or port, DAS works at the application level. It allows administrators to specify policies in detail as a particular REST API endpoint on a service and which identities or roles can invoke it. For example, you could say "Only the HR application server (identity verified) can send POST requests to the payroll database API, and no one else," or "Marketing team members can access the analytics dashboard service, but only read-only." These policies cover internal services that are critical. So even if an attacker breaches a server, they cannot automatically access everything else, because DAS is enforcing boundaries at each service.
- **Integration with Identity Providers**: DAS doesn't work in isolation; it pulls in identity context from external sources. Crystal Eye's implementation integrates seamlessly with Azure AD (Entra ID) tenants. This means it can import your internal users and groups and use them in policy rules. It also can identify client applications or services. So, policies can be tied to user roles or group membership (e.g., only users in the "Finance" AD group can access the finance app) and even to specific devices or service identities. By leveraging the existing identity infrastructure, it ensures the policies align with your organizational structure and are easier to maintain as people join/leave or change roles.
- **Scalable and Automated Enforcement**: The term "Declarative" indicates that you declare what the policy is, and the system figures out how to enforce it. Under the hood, Crystal Eye's DAS uses proven open-source components like OPA (Open Policy Agent) as the policy decision engine and Traefik as a reverse proxy to intercept and check requests. Policies are stored and managed centrally and enforced in a distributed manner without needing constant manual intervention. This scalable architecture means you can have thousands of policies, and the system will evaluate them in milliseconds for each access request. It's far more efficient than manually configuring ACLs on each service or maintaining static allow-lists.

- **Simplified Policy Management**: Despite doing a complex job, DAS offers a simpler and more intuitive way to define authorization policies compared to traditional methods. Through Crystal Eye's GUI, an admin can add a "tenant" (link to their Azure AD), define "applications" (the services or servers to protect, including details like their hostnames/IPs and ports), and then define "resources" which are essentially the specific endpoints or functionalities to guard. Once these building blocks are in place, creating a policy is as straightforward as selecting the resource and assigning which identities or groups are allowed (or explicitly denied) to access it. In technical terms, it's crafting OPA policies without having to write code – the system generates the necessary rules and handles the enforcement. This means even smaller IT teams can set up quite granular controls without needing a PhD in security policy languages.
- **Real-Time Enforcement and Monitoring**: When DAS is active, any access that violates a policy is immediately blocked. For instance, if malware on an internal host tries to call a protected API that it's not allowed to, DAS will deny that request – effectively containing the malicious action. These events are logged and can be seen in Crystal Eye's dashboards, so the security team gets visibility into attempted violations (which could indicate an attack in progress or an insider threat). Over time, these logs also help refine policies or identify if legitimate access was inadvertently constrained (allowing quick adjustments). By reducing the need for manual overrides and constant supervision, DAS reduces the need for manual intervention in access control. It's a "configure and let it run" approach, with administrators intervening only to update policies when business needs change.

Zero Trust in Action: To illustrate the impact of DAS, consider an example: A company has a legacy internal tool that only certain departments should use, but it's hosted on the general corporate network. Without DAS, an attacker who compromises any user's PC might be able to reach that tool (especially if it lacks proper authentication itself) and potentially extract data or use it as a pivot.

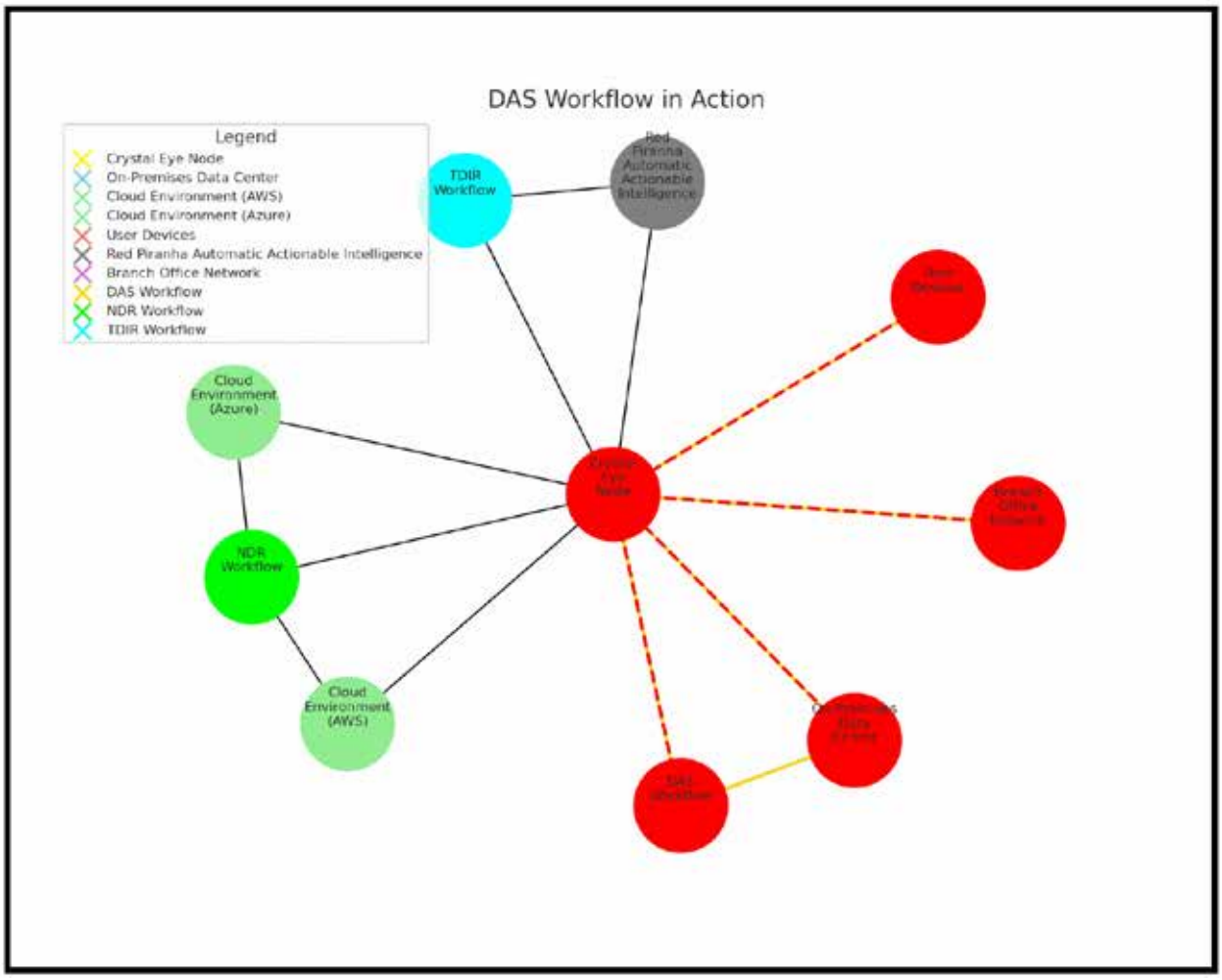
With DAS, even if that attacker gets onto the network, they will find that access to the sensitive tool is blocked at the service level for that user or machine. Another scenario is that if an employee in one department inadvertently tries to access a database from a tool they shouldn't; DAS would enforce the least privilege and block it, preventing accidents or curiosity from becoming security incidents. Essentially, DAS acts as an internal Zero Trust policy guard, segmenting not just networks but applications and data on a very granular level.

Moreover, implementing DAS can assist with compliance requirements that mandate principle of least privilege and role-based access control. Auditors and frameworks (like NIST Zero Trust framework) increasingly expect to see such controls. Crystal Eye's DAS gives organizations a ready-made way to demonstrate that they have these fine-grained controls in place, and that they are automated and consistent across the board.

In short, Declarative Authorization Service is Crystal Eye's answer to Zero Trust access management. It offers a much simpler and more intuitive way to declare "who can do what" in your digital environment. By operating on a scalable, automated framework, DAS significantly reduces the manual effort traditionally associated with maintaining dozens of ACLs or firewall rules.

When combined with strong identity integration and network controls, it ensures that even if attackers breach one layer of defense, they cannot freely move or access sensitive assets. Next, we will discuss how all these technologies – TDIR, NDR, WireGuard+SSO, and DAS – synergise to create a holistic security approach and what that means for an organization's overall defense strategy.

Synergy Between These Technologies for a Complete Security Approach



- **Threat Detection** – Crystal Eye WireGuard ensures that remote access traffic is continuously monitored by TDIR, which identifies unusual user behaviour indicative of credential compromise. If an attacker attempts to access the network using stolen credentials via the VPN, WireGuard logs and activity patterns provide critical telemetry for early detection.
- **Automated Response** – If a compromised user is detected, DAS instantly revokes VPN access, preventing lateral movement within the network. Simultaneously, NDR actively monitors and blocks any suspicious traffic from the WireGuard tunnel, ensuring that potential threats originating from compromised endpoints are neutralized before causing damage.
- **Correlated Insights** – Crystal Eye WireGuard integrates seamlessly with DAS, TDIR, and NDR, providing essential VPN access logs that contribute to comprehensive incident reports. By correlating user authentication events with security alerts, security teams gain deeper visibility into how a threat actor may be exploiting remote access.
- **Ongoing Protection** – Updated security policies are automatically pushed across the system, ensuring that any vulnerabilities exploited through remote access are mitigated proactively. If WireGuard sessions are involved in an attack, new rules can be enforced dynamically, restricting access until risk levels are reassessed.

Red Piranha's integrated approach enables:

- **Real-Time Action**: TDIR triggers immediate DAS policy updates and NDR responses to contain threats before they propagate.
- **Cross-Layer Intelligence**: Shared insights between DAS, TDIR, and NDR, Wireguard enhance detection accuracy and minimise false positives.

End-to-End Visibility

Integration ensures that:

- User, application, and network activities are monitored cohesively.
- Threat patterns are identified and correlated across all security layers, enabling advanced threat hunting and analysis.

Dynamic and Adaptive Security

By combining these solutions, Red Piranha provides:

- Real-Time Policy Adjustments: DAS adapts to evolving threats as detected by TDIR and NDR.
- Proactive Containment: Automated actions prevent threats from escalating or spreading laterally.

Cost and Operational Efficiency

The unified platform eliminates the need for multiple disparate tools, reducing:

- Licensing costs.
- Training requirements.
- Operational overhead through centralised management and automated workflows.

Unique Value Proposition of Red Piranha

Red Piranha delivers several unique advantages to the cybersecurity market:

- **Comprehensive Zero-Trust Architecture**: DAS ensures granular policy enforcement aligned with zero-trust principles, while TDIR and NDR provide continuous validation of user and network behaviours.
- **Performance at Scale**: Designed for high-performance environments, Red Piranha's platform supports thousands of concurrent access evaluations and network events without latency.
- **Seamless Multi-Cloud Integration**: Ensures consistent security across AWS, Azure, Google Cloud, and on-premise environments, making it ideal for hybrid infrastructures.
- **Enhanced Threat Intelligence**: Centralised threat intelligence repository feeds into all components, enabling proactive defense against emerging vulnerabilities and exploits.

With Crystal Eye, all security functions share the same ecosystem, ensuring seamless data correlation and automation. For example, if a user logs in via WireGuard VPN with Entra ID SSO and then attempts unauthorised access to a finance server, Crystal Eye instantly detects the anomaly using NDR, blocks the request via DAS, and triggers a real-time TDIR alert for investigation. This level of integration enables context-aware security enforcement, ensuring that every access request, network event, and user activity is continuously verified, logged, and responded to automatically.

Beyond integration, Crystal Eye simplifies security operations through a unified management console, reducing complexity for both internal SOC teams and MDR providers. Organizations gain end-to-end Zero Trust enforcement, where VPN authentication, network traffic monitoring, and access control dynamically adapt to threats.

The platform's proactive threat hunting, automated exposure management, and real-time threat intelligence updates ensure early detection and rapid response to cyber threats. By consolidating firewall, IDS/IPS, network visibility, endpoint security, and policy-based access control into one scalable solution, Crystal Eye enhances security while reducing deployment costs. Whether securing remote workforces, IoT environments, or hybrid cloud infrastructures, its adaptive, multi-layered security model proactively mitigates risk, making it a powerful, future-ready cybersecurity solution for enterprises and SMBs alike.

Managed Detection and Response (MDR) as a Plug-and-Play Extension of Crystal Eye

As modern threat actors increase the speed, automation, and sophistication of their attacks, organizations must be able to detect, investigate, and respond at machine speed. Yet most businesses, especially SMBs and resource-constrained enterprises lack the internal capacity for continuous security operations. Red Piranha's Managed Detection and Response (MDR) service was built to address this operational gap by providing a plug-and-play, full-spectrum SOC-as-a-Service, directly integrated with the Crystal Eye Unified Security Platform.

Solving the Operational Challenge with Human-Machine Teaming

Security teams today face a critical scale issue. Many report receiving 10,000 to 15,000 security alerts per day, overwhelming their ability to determine what's real and what's noise. As adversaries automate their intrusion attempts, traditional SOC models struggle to match their pace. Red Piranha's MDR service combines machine-speed automation with expert analyst oversight a Human-Machine Teaming model that offloads noise while focusing human expertise where it matters most.

Through this approach, Crystal Eye not only detects anomalies and high-risk behaviours in real-time but also automates triage and prioritisation, enabling analysts to focus on incidents that require decision-making, intervention, or escalation.

Scope of MDR Services

Red Piranha's MDR offering encompasses:

- **24×7 Threat Monitoring and Detection**
  Continuous telemetry ingestion from Crystal Eye's TDIR, NDR, and endpoint agents ensures full-spectrum visibility across the network, cloud, and endpoints.
- **Incident Response and Containment**
  The SOC team can initiate immediate containment actions including isolating endpoints, revoking credentials, or blocking lateral movement based on predefined rules or analyst validation.
- **Digital Forensics and Investigation (DFIR)**
  Organizations can initiate full forensic investigations, leveraging packet captures, log correlation, and threat intelligence to trace root causes and attack progression.

- **Threat Hunting**
  Beyond alerts, the MDR team proactively searches for signs of stealthy or novel threats such as living-off-the-land techniques, lateral movement, or beaconing activity that may evade automated detection.
- **Automated Threat Intelligence and Correlation**
  Integrated threat intelligence from Red Piranha's global research team powers automated decision-making, enabling faster identification of known IOCs and suspicious behaviours.
- **Security Orchestration and Automated Response (SOAR)**
  Crystal Eye's built-in SOAR capabilities allow for scripted, scalable responses based on MDR findings ensuring consistent, rapid mitigation across environments.

How MDR Differs from Traditional MSSP Services?

While traditional MSSPs provide basic monitoring often limited to firewalls or external traffic, Red Piranha's MDR provides deep, correlated visibility across the full environment. It extends beyond perimeter monitoring to include:

- **East-west traffic inspection**
- **Cloud service integration**
- **Identity-aware access tracking**
- **Behavioural baselining and anomaly detection**
- **Integration with endpoint and application layer telemetry**

This allows for early identification of multi-stage threats, including insider threats and advanced persistent threats (APTs), which often go undetected in siloed or reactive security models.

Seamless Integration and Deployment

Red Piranha's MDR is designed to be operational within hours, not weeks. As a native extension of the Crystal Eye platform, it requires no additional integration, licenses, or third-party tools. Key features of this plug-and-play model include:

- **Predefined deployment workflows** that adapt to on-prem, hybrid, or cloud environments
- **No extra licensing or configuration overhead** for SOAR, SIEM, or threat hunting
- **Inline or out-of-band NDR deployment**, depending on risk appetite and architecture
- **Use-case-driven tuning** of detection rules and response actions to fit organizational risk profiles

Outcomes: Faster Detection, Targeted Response, Lower Risk

According to industry research, the average time to detect and contain a breach is **277 days**. With Red Piranha's MDR service, detection and containment can often be achieved within **minutes** of compromise dramatically reducing the attack surface and potential impact.

Key measurable benefits include:

- **Reduced dwell time and blast radius**
- **Improved signal-to-noise ratio** through automated alert triage
- **On-demand incident response** without requiring internal escalation chains
- **Improved compliance posture** through real-time logging, reporting, and forensic readiness

Quality Assurance and Compliance

Red Piranha operates its MDR service through **ISO/IEC 27001-certified SOCs**, staffed by highly trained analysts with real-time access to the full Crystal Eye telemetry stack. This assures clients that their security operations are managed under a globally recognized standard for information security management.

In summary, Red Piranha's MDR-as-a-Service transforms Crystal Eye from a security platform into a fully augmented security operations capability. Organizations gain the detection power of an XDR platform, the response speed of SOAR, and the strategic oversight of a 24/7 SOC without the complexity or cost of building it themselves.

Conclusion

Red Piranha's Crystal Eye Unified Security Platform represents a paradigm shift in how organizations can protect themselves against modern cyber threats. By fusing Threat Detection, Investigation, and Response (TDIR) with advanced Network Detection and Response (NDR), secure remote connectivity through WireGuard + Entra ID SSO, and fine-grained access control via Declarative Authorization Service (DAS), and MDR Crystal Eye delivers a comprehensive, integrated defense that is greater than the sum of its parts. This single-platform approach not only counters today's sophisticated attacks from APTs stealthily operating within networks to opportunistic ransomware blasts but does so in a way that simplifies management and reduces costs.