Security is more complex than ever

Securing your business against cyber threats demands time, effort, and expertise.

Yet spotting and stopping suspicious activity before it can affect you takes knowledge and experience that not everyone has access to.

In response, businesses layer new security tools and technology in an effort to protect their data and assets across their network, cloud services, and endpoints.

Security toolsets are more complex than ever, leading to information overload and alert fatigue.

What if there was a better way?

You need an always-on solution that keeps you safe from cyber threats. You need actionable information that helps you improve and enhance your security—without taking time out of your busy day.

You need a continuous view of potential cyber risks and malicious activity, backed by expertise, to prevent cyber threats and eliminate security vulnerabilities easily.

Your hands-free cyber security solution.

MDR, XDR, SIEM, SOC... it's all under the hood. From threat detection to analysis and response, Pro4ia has you covered.

Built from the ground-up to detect and respond to abnormal behavior on endpoints, cloud services, and networks, Pro4ia's holistic cyber security solution delivers visibility into the threats and risks facing your business—giving you the advantages of automated cyber security, backed by human intelligence.

No matter the size of your team or where they work, Pro4ia extends across your entire IT infrastructure. We pinpoint the cyber threats and vulnerabilities targeting your business and deliver the information you need to respond—all from one user-friendly platform.

Real-time active response

Pro4ia is always prepared to respond to suspicious activity across your IT environment, such as:

- Execution of anomalous processes
- Inappropriate access between processes
- Attempts to load user and/or kernel mode modules
- Abnormal file system access
- Suspicious network traffic
- Anomalous registry access
- And much more

When the system spots something that doesn't look right, Pro4ia gets to work immediately, identifying the threat and taking appropriate action to keep you safe. Pro4ia's service automatically blocks major threats like ransomware and advanced persistent threats (APTs), all while keeping you informed about what's going on.

What's more, because the system was designed to work seamlessly across your endpoints, network, and cloud services, Pro4ia understands what activity in one part of your environment means for the system as a whole.

Using active response profiles lets you further tailor Pro4ia to meet your needs, giving you unmatched insight and control over your protection.

Intelligent alerting.
Guided remediation.
Expert counsel.

The findings from Pro4ia's advanced threat detection and analysis are transformed into actionable insights that help you quickly and proactively understand the response needed to secure your business.

We deliver analyst-verified threat data as simple, prioritized, actionable reporting that helps you understand your threats as Actions, Recommendations, and Observations (AROs). Our proprietary approach removes noise to show you the alerts that matter with the context needed to resolve them.

Say goodbye to a volume of threat alerts that take hours to investigate. No security event logs to sort through. No more time spent gathering data across your network from multiple tools.

Actions

When immediate action is needed for an active or imminent threat that could compromise your network or devices, we will flag this as a required Action.

Recommendations

If a suggested change is needed to your network configuration, software, or technology to address specific vulnerabilities or possible threats, we will indicate this as a Recommendation.

Observations

Specific conditions or events in your network may be early indicators of malicious activity that could impact your cyber security. We report this as an Observation.

Need help? We've got your back.

Like a professional security concierge service, gain the peace of mind that comes from a dedicated team of experienced cyber pros and analysts providing expert support, counsel, and recommendations. From technical support to advice on security strategy, we're at your side to help you continually protect your business.

Cyber security made simple with all-in-one threat detection, analysis, and response.

1.	**24/7 Network traffic analysis**	Secure your network by analyzing all network traffic, including known and unknown devices, Internet of Things (IoT) devices, and mobile devices. Identify and respond to threats and potential vulnerabilities to your network.
2.	**Complete endpoint threat detection & response**	Protect all your endpoints—including servers, desktops, and laptops—and identify anomalous behavior to actively block known and emerging malware and attack techniques.
3.	**Active malware and APT protection**	Automatically identify and block malware, ransomware, and advanced persistent threats (APTs) using policies and technology informed by leading cyber expertise.

4.	**Cloud layer detection and response**	Use our cloud-native monitoring sensor to protect your company domain and cloud-based programs and applications, including Microsoft 365, Google Workspace, Amazon Web Services, Azure, Dropbox, Box, Okta, Salesforce, and more.
5.	**Fortify your network perimeter**	Rely on our DNS firewall to ensure safe web browsing and Internet access by blocking connections to malicious websites.
6.	**Mitigate vulnerabilities and risks**	Identify important changes and activity across your IT environment that indicate risks—including misconfigured cloud services and unpatched software—and receive detailed steps to resolve issues and improve your security.
7.	**Access advanced analytic engine**	Benefit from machine learning and analytic capabilities that provide continuous analysis of user and service data to identify and address threats. The result is real-time visibility to detect, monitor, measure, manage, and reduce attackable points from end to end.
8.	**Gain expert threat hunting**	Obtain better insight and security recommendations thanks to our expert threat hunters who dive deep into network and data to identify new, emerging, or otherwise undetected vulnerabilities and threats.
9.	**Experience active response**	Automatically block malware, isolate devices, or take further action to protect your business. Pro4ia takes appropriate action on your behalf and based on your risk tolerance, always backed by human analysis.
10.	**Look behind the scenes with Dashboard**	Take a closer look at how we analyze data from your network, endpoint, and cloud layers to keep you secure. The Pro4ia Dashboard lets you access all information about your security posture in an easy-to-use and easy-to-view format.

11.	**Minimize your impact with Incident Readiness**	Put the right preparation in place now to minimize the impact of a future security incident. Through our Incident Response (IR) Readiness Package, we identify improvements and the best practices and processes needed to prepare for potential incidents. We help you set the stage early on to respond quickly with less recovery costs and downtime.
12.	**Prioritize security efforts**	Implement security controls, user policies, and education efforts through targeted insights and guidance from our intelligent Actions, Recommendations, and Observations (AROs) alerts and reporting.
13.	**Flag suspicious email activity for expert review**	Protect email communications with our Suspicious Email Analysis Service, enabling users to quickly forward any suspect emails to our cyber experts for fast analysis.
14.	**Access integration functionality**	Use Pro4ia APIs and SDKs to easily integrate Pro4ia with other systems and provide monitoring and AROs alerting from one platform, including Simple RESTful API integration with the primary Pro4ia platform, advanced Python SDK and API to work with Pro4ia sensors, and integrations and add-ons for third-party products.
15.	**Align with cyber security frameworks**	Experience advanced vulnerability discovery and reporting based on industry best practice frameworks, including the NIST Cyber Security Framework, ISO 27001, Canadian Centre for Cyber Security Baseline Controls (CCSC BC), Payment Card Industry Data Security Standard (PCI DSS), and Australia's ACSC Essential Eight Mitigation Measures.
16.	**Rely on easy set-up, state-of-the-art appliances**	Choose from a range of Pro4ia appliances to complete your Pro4ia deployment and ensure sophisticated cyber security monitoring, detection, and analysis for your specific IT environment.
17.	**Access round-the-clock security expertise**	Get help every step of the way. Our expert cyber analysts are available for your security questions, providing the advice you need.
18.	**Phishing Simulation, End User Training Education**	Engaging and interactive micro-training lessons emailed weekly combined with phishing awareness through the delivery of simulated phishing emails to employees. Help to educate users on how to spot phishing emails, a common device for infiltrating business computers and networks.