Secure Your Digital World Today to Protect Your Tomorrow

With a proven record for protecting customers from threats, InfoGuard uses the advanced capabilities of Palo Alto Networks Cortex® platform to protect their customers with comprehensive SOC services, even as the threat landscape and your IT environment evolve.

Why Does This Matter?

Providing cybersecurity and protecting the business is getting more challenging. All organisations face an evolving and expanding threat landscape. A proliferation of devices, increasing digitisation, adoption of cloud, remote work, and a more distributed IT environment leads to more security blind spots, a wider attack surface, and increasing complexity.

The increasing volume of threats and security risks means many go unrecognised. Where threats and alerts are reported, limited security resources are overwhelmed, meaning remediation doesn't occur fast enough—increasing the risk of damage. The rise of AI-led threats means the time between an attack and significant damage occurring is reducing, and the ease at which attacks can be orchestrated and conducted at scale increases.

- By 2026, organisations prioritising their security investments based on a continuous threat exposure management program will realise a two-thirds reduction in breaches.[1]
- Through 2025, generative AI will cause a spike in the cybersecurity resources required to secure it, causing more than a 15% incremental spend on application and data security.[2]

A multipoint-solution approach to security, looking at firewalls, malware protection, or network protection individually, is no longer effective. A more holistic approach is needed that considers IT, processes, and people, to secure the business today and combat the threats of tomorrow.

The Solution: Cybersecurity and Cyber Defence Services from InfoGuard, Supported by Palo Alto Networks Cortex Platform

Quickly adopt critical security capabilities and address any security risks. Then add layers of security, intelligence, and automation over time to keep pace with changes in regulation, emerging AI-enabled threats, and business transformation.

InfoGuard is an independent, leading cybersecurity expert that helps organisations in Switzerland, Austria, and Germany keep their systems and data secure for over 20 years. Providing a 360-degree security service, InfoGuard and its more than 240 security experts across four locations offer the highest level of security around the clock, professionalism, and reliability for their clients, with no substantial business impact by Managed Detection and Response (MDR) customers to date.

InfoGuard's leadership understands that helping customers quickly attain a robust security posture—with all core capabilities in place and critical security vulnerabilities addressed—is a vital first step. Then they can help customers evolve their security environment in readiness for future change. To this end, InfoGuard provides an extensive range of security services including:

- MDR
- Incident response and forensics
- Proactive threat hunting
- Managed SOC or comanaged SOC
- Managed security and network services
- Cybersecurity and network solutions
- Security consulting services
- Penetration testing

[1] Richard Addiscott, et al., *Top Trends in Cybersecurity for 2024*, Gartner, January 2, 2024.

[2] Ibid.

InfoGuard has been partnering with Palo Alto Networks since 2012, offering its firewall products and Cortex platform as an on-premises security solution, managed security service, and MDR service. InfoGuard's choice of Palo Alto Networks technology is down to three factors.

First, Palo Alto Networks constant innovation and continuous improvement ensure that customers get the best cybersecurity capabilities. Second, Palo Alto Networks platform approach enables InfoGuard to quickly offer customers the critical security services they need today, while providing next-generation MDR capabilities and seamlessly adding new services as part of a customer's longer-term security roadmap. Lastly, Palo Alto Networks solutions are designed with a security-first mentality. They process all traffic, and all their security capabilities are "switched on" as standard without any impact on performance. This reduces the risk of customers assuming that they're protected when a feature isn't active, leaving them vulnerable.

The Palo Alto Networks Cortex® platform is a best-in-class solution that offers end-to-end security in a single, AI-enabled platform. It uniquely provides ML-enabled automation, AI-powered SOC, extended detection and response, and cross platform visibility in one.

What This Means for Our Joint Customers

You get visibility and clarity of your security weaknesses and quickly establish a robust, total security posture that addresses your vulnerabilities. InfoGuard has hundreds of security experts who will act as your trusted security advisor and partner. They'll work through InfoGuards' proven, standardised frameworks to assess your security capabilities across all cybersecurity pillars, ensuring a fast and comprehensive analysis. For larger, more complex environments, these are supplemented with a more tailored approach. However, in all cases, we establish a "baseline" of security capability that identifies any gaps or security risks and closes them during the security journey, ultimately protecting the customer from organised crime.

InfoGuard knows how to establish a foundational or "basic" level of security, ensuring that your business is safe from ransomware attacks. This is built on MDR—services in standard packages that can be quickly implemented, ensuring a comprehensive security posture, while gaining comprehensive 24/7 protection, detection, and response.

Once your security posture is effective, InfoGuard consultants will jointly follow your security journey, taking a pragmatic, logical approach based on your maturity and your business plans to advise on your next steps. You'll get a clear understanding of how to evolve your security and what second lines of defence to adopt so you can maintain your posture as the environment or threat landscape changes.

InfoGuard can support organisations already experiencing a breach. Its Computer Security Incident Response Team (CSIRT) and APT Response Service will swing into action on request, leveraging Cortex's capabilities to quickly identify the threat actors and bring the situation under control. With this, they can assist in bringing the incident to a close fast and get systems back up and running. Due to the strong protection of Cortex XDR®, we can successfully implement the setup on the compromised infrastructure.

Customer benefits include:

- **24/7 protection against cyberattacks** through a more holistic, effective, and cost-effective security approach with data and insight from the entire estate in a single view. Total visibility of your cloud, network, solutions, and applications' security posture with data from across your whole estate ensures no visibility gap.
- **Address issues based on priority or risk** and shrink your attack surface to protect it better.
- **A clear plan to reduce your security burden** while improving security, compliance, and reducing risk.
- **Reduce the risk** of security becoming a roadblock to innovation.

You get the security skills and capabilities that you need, while augmenting and empowering your own IT resources. InfoGuard has the expertise and resources to manage your security environment whether fully taking over your SecOps or supporting with shared responsibility in comanaged SOC environments. The wide range of offerings and consultancy offered by. InfoGuard can provide you with tailored and managed security services for specific aspects of your environment. These include managed security governance, engineering capabilities and on-site professional services, CISO advisory services, or CISO-as-a-service offering. Whatever the requirement, you'll get access to the skills and people with the experience to ensure you get secure, stay secure, and can evolve and enhance your security stance.

Did you know?

4/10 More than 4 in 10 (organisations) think that MDR service providers can simply do a better job than in-house resources can. One-third report immature security programs, also lacking the tools and systems needed.[3]

42% of businesses report significantly fewer successful attacks as a benefit of working with a managed security service provider.[4]

100% Palo Alto Networks Cortex XDR was the only solution to provide 100% protection without missing critical protection steps, as well as achieving 100% visibility and 100% analytic coverage (detections) with zero configuration changes and zero delay detections.[5]

Your team at InfoGuard will help you quickly and effectively scale up from MDR—reducing your exposure to threats and ransomware—to begin penetration testing, tabletop exercises of crisis readiness, and examination of specific use cases. They'll work with you to map your security journey based on business plans, industry-specific requirements, determine what legacy systems are in place, and other considerations. This ensures that security is built in rather than an afterthought. In addition, compliance experts can help you align your plans with known regulatory changes and ensure readiness in advance.

Empowered by the powerful AI-enabled automation and extensive monitoring capabilities of Cortex, expert technicians can focus on adding value and reducing your TCO, while providing your teams with access to vital insights and controls. They can leverage data from across your entire IT estate—including cloud, network, devices, and applications—giving them and you a full understanding of security dependencies and implications when considering transformation investments or other IT environment changes.

InfoGuard teams have achieved all the required Palo Alto Networks NextWave Cortex Specialisations: XMDR Specialisation, Threat Response Proficiency, and Cortex XSOAR Specialisation, on top of their years of experience working with Palo Alto Networks technologies.

Customer benefits include:

- 24/7 MDR with more than 80 experts.
- 12+ years of SOC and MDR experience and expertise.
- A flexible suite of services means you can outsource specific security functions, your entire security environment, or establish a comanaged SOC environment.
- Remove overhead and resourcing limitations.
- Enhance your security capabilities without having to hire more resources.
- Increase confidence in your cybersecurity.
- More detailed, in-depth, and intensive investigations with better outcomes and fewer resources used.
- Empower staff with the insight that they need and reduce their admin load, enabling focus on higher-value work.

[3] Dave Gruber, *What Security Teams Want from MDR Providers*, ESG, September 2022.

[4] Ibid.

[5] *2023 MITRE Engenuity ATTACK® Evaluations*, MITRE Engenuity, last accessed July 23, 2024.

You get the intelligent, adaptive capabilities you need to stay ahead of AI-driven attacks and future threats. As your IT environment gets more complex, AI becomes more ubiquitous and continued adoption of cloud, new attack vectors, and security vulnerabilities are being exposed. Today, bad actors require little technical skill to create AI-enabled attacks and these attacks are starting to compromise identities rather than systems. This shift demands a new security approach, evolution of governance policies, and greater visibility in the cloud. Fully automated attacks are now becoming common, requiring a totally different level of detection and response. Based on InfoGuard's experience, such attacks can cause severe damage within seconds of a compromise.

Did you know?

38%	of organisations lowered their security operating costs by working with a managed security service provider.[6]
50%	saw improved security personnel skills learnt by working with a managed security service provider.[7]

This means continuous improvement and adaptation of your security environment and SecOps over time to keep pace. Assume that any attack may be partially successful and begin to adopt layers of defence, working together effectively to create a more robust protective shield. AI-enabled solutions are the keys to responding at speed, closing down attacks as they begin, and ensuring vulnerability patching happens much faster.

InfoGuard has been working with AI for many years. With Palo Alto Networks and other AI-enabled solutions, its teams have become very efficient at improving detection and defence capabilities. InfoGuard has also reduced the time limits established in their service-level agreements inline with this shortening of response windows. They'll reduce these again at no extra cost to the customer to ensure they're keeping pace and can keep customers protected.

With the Palo Alto Networks Cortex platform, experts at InfoGuard can create out-of-the-box rules for detecting behavioural threats and use its AI-powered capabilities to better detect attacks across endpoint, network, IoT/OT, cloud, and identity. These capabilities can also help you calculate attack risks and automatically respond to attacks based on your needs, policies, and processes. InfoGuard experts can create AI-enabled profiles and identities and define analytics across cloud, network, endpoint, and identities to enable targeted, effective automation of security policies. These are automatically kept up to date by Cortex's capabilities to ensure they remain accurate as your profiles, users, applications, and threats all change. You get next-generation security capabilities today and keep ahead of future threats.

Customer benefits include:

- AI expertise and capabilities that match the evolution in AI-enabled threats.
- Future-proofing your security posture and environment, getting ahead of new threats and changes in regulation.
- Adopting one comprehensive security ecosystem enabling consolidation of tools, improvements in performance, and seamless adoption of new capabilities over time.
- Closing the loop on threats by leveraging the solution synergies across the Cortex ecosystem, with products that work in concert to monitor the threat landscape and provide the most robust detection, response, and investigation capabilities.

Did you know?

Palo Alto Networks has been positioned as a Leader in the 2023 *Gartner® Magic Quadrant™ for Endpoint Protection Platforms (EPP)* report.

[6] *What Security Teams Want from MDR Providers*, September 2022.

[7] Ibid..

What our customers say

Siegfried AG, a global life sciences company with production sites in Switzerland, the United States, Malta, China, Germany, France, and Spain, relies on rapid, professional support from experts who are available round the clock with the resources and experience of similar situations.

> **“You need one thing above all in order to deal successfully with cyberattacks—rapid, professional support from experts who are available round the clock with the resources and experience of similar situations. This is precisely the service that InfoGuard provided us with, right when we needed it. The excellent interaction of expert staff, efficiently organised processes and the right technologies is what helped us the most. This is exactly the kind of service you need to be up and running again as soon as possible.”**
>
> – Dr. Christian Neubaur, CIO, Siegfried AG

> **“Cortex XDR was a very important piece of the puzzle for my team and me as head of the crisis management team, to successfully drive forward and carry out the reconstruction of the compromised infrastructure.”**
>
> – Ernesto Hartmann, Chief Cyber Defence Officer, InfoGuard AG

About InfoGuard

InfoGuard has been protecting customers in Germany, Austria, and Switzerland for over 20 years. Over 240 security experts across four locations ensure comprehensive protection around the clock for more than 700 companies. Years of experience, a broad portfolio of solutions, recognised certifications, and highly qualified employees are the cornerstones of our business, offering the top level of security, professionalism, and reliability. As an independent company, we are able to react quickly and flexibly to changes in clients’ needs.

InfoGuard has met stringent criteria to be accredited:

- ISO 27001 (Information Security Management)
- ISAE 3000 Type 2 (SOC 2 compliance)
- ISO 14001 (Environmental Management)

About Palo Alto Networks

Palo Alto Networks is recognised by industry analysts and its thousands of customers as a global cybersecurity leader. With best-of-breed platforms, world-class threat intelligence, and expertise, Palo Alto Networks technologies are helping businesses everywhere protect themselves in a fast-changing landscape full of new vulnerabilities and emerging and evolving threats. Working hand in hand with our accredited MSSP partners, our customers get the targeted services, knowledgeable expertise, and integration support to create the cybersecurity defences they need now and tomorrow.

Palo Alto Networks is helping protect:

- 10 out of 10 of the Fortune Top 10
- 8 of the 10 largest U.S. banks
- 9 of the 10 largest utilities worldwide

3000 Tannery Way
Santa Clara, CA 95054

Main: **+1.408.753.4000**
Sales: **+1.866.320.4788**
Support: **+1.866.898.9087**

www.paloaltonetworks.com

parent_wp_secure-your-digital-world-today_080524