SeqOps Partner Program Whitepaper

Empowering Your Cybersecurity Strategy for Growth and Success

1. Overview of SeqOps Platform

(Image)

SeqOps stands as a formidable cybersecurity partner, committed to empowering businesses to navigate the intricate threat landscape with resilience and confidence. Our platform is designed to seamlessly integrate into your existing infrastructure, enhancing your security offerings and operational efficiency through advanced threat detection, automated vulnerability management, and comprehensive reporting tools.

Harness the strength of the SeqOps platform to unlock new revenue streams, master security expertise, and deliver proactive security measures to your clients. With access to specialized training, comprehensive support, and an expert network, partnering with SeqOps means advancing your security services and achieving remarkable growth.

2. Our Services

SeqOps offers a suite of cybersecurity solutions tailored to help businesses of all sizes tackle the challenges of an ever-evolving threat landscape. Our holistic approach to cybersecurity helps clients secure their digital assets and mitigate risks effectively.

Server Security

Securing servers from data leaks and unauthorized access is crucial for maintaining data privacy, accuracy, and availability. SeqOps implements robust security measures covering network, physical, and operating system security to guarantee reliability and data integrity.

Cloud Security

As cloud computing gains wider adoption, securing cloud environments like GCP, AWS, and Azure is vital. SeqOps provides comprehensive solutions for managing data, securing networks, and encrypting data to block unauthorized access and prevent data breaches, ensuring compliance with industry regulations.

AWS Security

Our customized security solutions for Amazon Web Services (AWS) leverage advanced threat detection, encryption, and access controls to secure assets and applications hosted on AWS.

GCP Security

SeqOps protects Google Cloud Platform (GCP) assets with unique security protocols, including network security, identity and access management, and data encryption, helping organizations scale operations securely with optimized control and visibility.

Azure Security

Protecting your Azure environment is crucial, and SeqOps makes it seamless. Our platform offers comprehensive Azure Security solutions designed to safeguard your data, applications, and infrastructure. We provide advanced threat detection, continuous monitoring, and automated vulnerability management tailored specifically for Azure.

Office 365 Security

We secure Microsoft 365 suite environments by implementing data loss prevention, email security, and threat detection controls, safeguarding collaboration tools, email communications, and documents.

Penetration Testing

SeqOps conducts simulated cyber attacks to identify vulnerabilities in applications, networks, and systems, enabling preemptive risk mitigation. Our penetration tests uncover security weaknesses, allowing organizations to address them before malicious actors exploit them.

Load Testing

Assessing the performance and scalability of systems under different conditions and loads ensures seamless user experiences. SeqOps identifies performance bottlenecks, improves resource allocation, and validates application performance to prevent user dissatisfaction and downtime risk.

Security Review & Audit

Conducting comprehensive reviews and audits of security policies, controls, and measures is essential for improving cybersecurity posture and boosting resilience. Our assessment efforts identify risks, gaps, and areas for improvement, ensuring compliance with industry regulations.

Managed Detection & Response (MDR)

Proactively monitoring systems and networks for security threats allows for real-time incident detection and response. SeqOps' MDR solutions leverage advanced threat detection capabilities, automated response systems, and expert security analysts to ensure quick and formidable incident responses.

3. Our Tools and Strategies

Unpatched vulnerabilities pose a significant cybersecurity threat, with many cyberattacks exploiting these weaknesses. Recent data highlights that approximately 82% of cyberattacks against U.S. organizations targeted patchable external vulnerabilities. Financial repercussions of these attacks were substantial, with affected organizations experiencing costs 54% higher than incidents stemming from human error (source: SC Media). Up to 60% of data breaches can be attributed to poor cyber hygiene, particularly neglecting to patch vulnerabilities (source: Automox Operations).

SeqOps offers a range of strategies and tools to fortify the security of cloud and server environments:

Automated Scanning Tools: Systematically examine systems for known vulnerabilities, covering infrastructure as code in cloud environments, server configurations, and operational systems.

Continuous Monitoring: Enable real-time detection of anomalies and signs of vulnerabilities or ongoing attacks, ensuring prompt threat identification and response.

Threat Intelligence Feeds: Integration of threat intelligence feeds provides the latest information on vulnerabilities and exploits, facilitating prioritized scanning and remediation efforts.

Penetration Testing: Regular penetration tests simulate real-world attack scenarios to identify vulnerabilities that may evade detection by automated tools.

Configuration Management: Maintain proper configuration management to ensure compliance with best security practices, minimizing potential attack surfaces from misconfigurations.

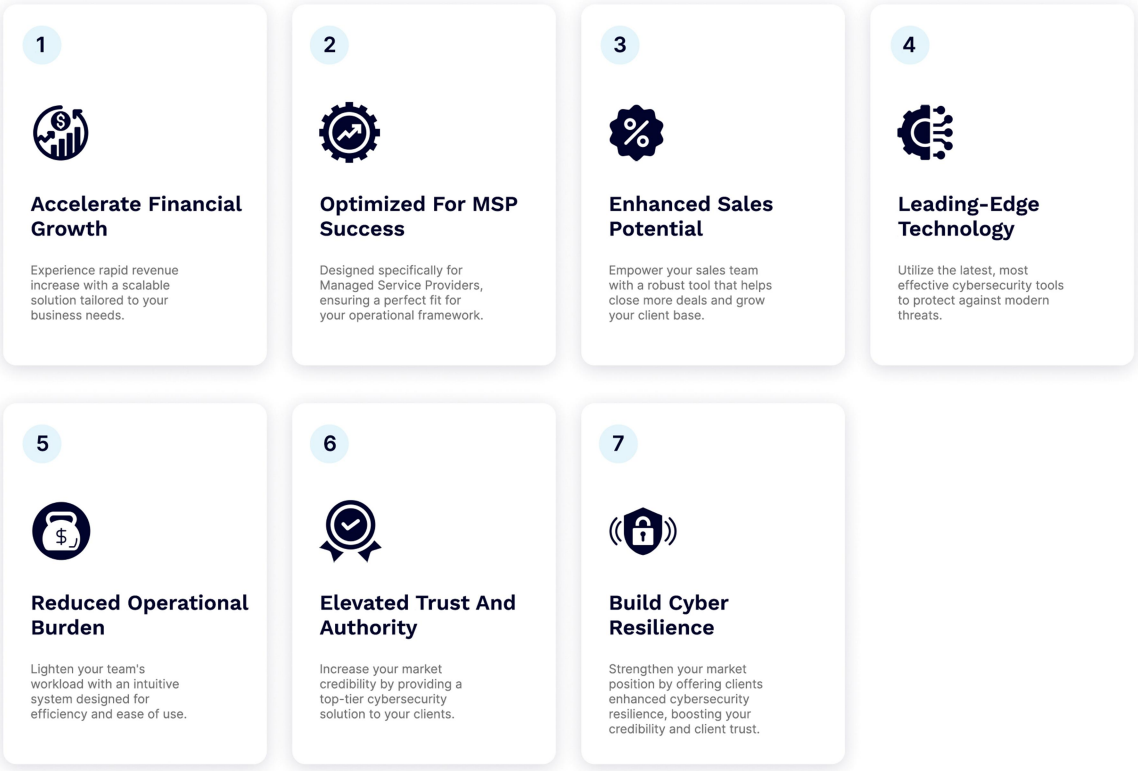
Compliance Auditing: Regular audits ensure alignment of cloud and server environments with industry standards and regulations.

Employee Training and Awareness: Comprehensive security training for staff members reduces the risk of vulnerabilities arising from human error.

Patching Strategy: Develop and implement a robust patch management strategy, facilitating timely updates to servers and cloud systems.

4. Operational Efficiency

Discover the key advantages of joining the SeqOps Partner Program, including revenue growth opportunities, access to advanced security solutions, and the ability to differentiate your services in the market. Our program streamlines your operations and enhances service delivery, driving greater efficiency and customer satisfaction.



Why Partner with SeqOps?

Scalable Security Solutions

SeqOps empowers you to effortlessly expand your security offerings in alignment with your business growth. Our scalable solutions meet the dynamic security needs of your clients, ensuring robust protection that grows with them. This flexibility helps you respond quickly to market demands and emerging threats, securing client trust and satisfaction.

Enhance Revenue Potential

Maximize your profitability through our clear and transparent pricing structures, designed to significantly enhance your revenue potential. By partnering with SeqOps, you gain access to a model that supports your business growth at every stage, ensuring accurate cost and profit predictions.

Superior Customer Protection

Offer superior protection to your customers with SeqOps' advanced and user-friendly security solutions. Our technology ensures top-tier defense mechanisms, reducing client risks and enhancing trust in your services.

Dedicated Partner Support

Enjoy the full support of our dedicated team, committed to your business's growth and success. SeqOps provides extensive personalized assistance, from technical support to strategic business advice, ensuring you have all necessary resources to navigate the complex cybersecurity market confidently.

Build Trust and Authority With Clients

SeqOps not only equips you with cutting-edge security solutions but also enhances your reputation and authority with both existing and new clients. By onboarding your customers to the SeqOps platform, you can immediately identify and demonstrate existing weaknesses and vulnerabilities in their systems. Our continuous monitoring and real-time threat detection provide ongoing insights, essential for maintaining robust security.

This transparency fosters a deeper mutual understanding between you and your clients, facilitating informed discussions about the necessity of managed services providers (MSPs) for effective patching and remediation. Instead of overselling, you can clearly illustrate the immediate need for action, making the decision for patching and fixes straightforward and compelling.

This proactive approach not only strengthens client relationships but also opens new revenue streams. Existing customers will appreciate the added value of continuous monitoring and threat mitigation, leading to increased trust and loyalty. Simultaneously, showcasing your advanced capabilities to potential clients can attract new business opportunities, positioning your services as indispensable in the ever-evolving cybersecurity landscape.

5. Case Study-Opsio

Opsio has successfully integrated SeqOps Services into their Security as a Service offering, capitalizing on the advantages of a dedicated security partner for their customers. This strategic move has resulted in a notable increase in Opsio AB's revenue streams, elevating their monthly recurring revenue by over 15% on 3-year contracts over the past year.

Andreas Johansson, CEO of Opsio, expressed his enthusiasm, stating, "SeqOps' service and platform isn't just a tool; it's the key that unlocked a world of revenue opportunities for our partnership. Together, we've fortified not only our clients' digital defenses but also the foundation of trust they have in us. With SeqOps, our bond has grown stronger, just like the security it provides."

Erik Hedlund, CEO of SeqOps, also highlighted the success of their collaboration, "Our partnership with Opsio has been incredibly successful and mutually beneficial. SeqOps' service and platform have provided Opsio with the tools necessary to unlock significant revenue opportunities and enhance their clients' digital security. Together, we've not only fortified the digital defenses of numerous organizations but also strengthened the trust and collaboration between our teams. The success we've achieved with Opsio is a testament to the power of strategic partnerships and the robust security solutions we provide."

6. Implementation and Support

(Image)

SeqOps partners gain insights into the support and resources available, including training programs, marketing support, and technical assistance. Our dedicated team is committed to ensuring smooth implementation and ongoing success, providing you with the tools and knowledge needed to excel.

7. Frequently Asked Questions

What happens after I submit an inquiry to become a partner?

After you submit an inquiry to become a partner with SeqOps, our team will review your application and promptly get in touch to discuss the next steps. We will provide detailed information about the partnership process, outline the benefits and responsibilities, and answer any questions you may have.

Once I become a partner, what should I do next?

After becoming a partner, set up an introductory meeting with your SeqOps partnership manager to outline specific goals and strategies tailored to your business. This ensures you are well-prepared to leverage the partnership fully, benefiting both your business and your clients.

What additional support do we receive?

The support you receive is tailored to your subscription level, including dedicated sales resources, technical expertise, co-branded marketing campaigns, and ongoing customer success support. Higher tiers offer more personalized assistance to help maximize the value of our solutions.

Does SeqOps offer white labeling?

SeqOps does not currently offer white labeling services. However, we provide robust cybersecurity solutions and dedicated support to help you achieve your security goals. For specific needs or customization requests, please let us know, and we will do our best to accommodate them.

How do I invite customers to SeqOps?

Partners can send invitation emails directly from the platform. Customers onboard themselves and are connected exclusively to the partner who invited them.

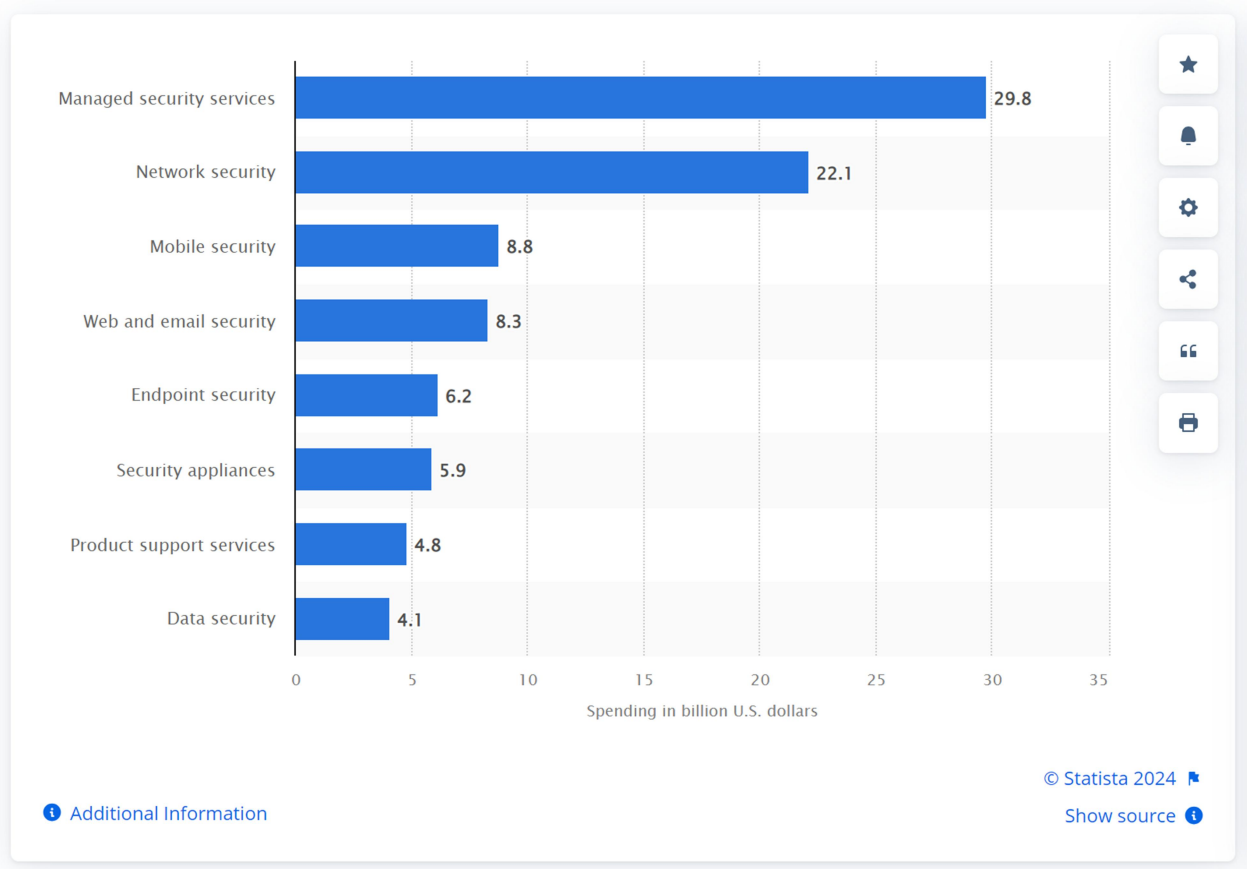
What is the benefit of becoming a SeqOps Partner?

Becoming a SeqOps Partner offers numerous benefits, including access to advanced cybersecurity solutions and dedicated support to enhance your service offerings. You receive tailored resources such as sales and marketing assistance, technical expertise, and ongoing customer success support, enabling you to provide top-tier security services to your clients and grow your business.

8. Market Trends and Insights

Small and medium-sized businesses (SMBs) face significant cybersecurity threats that are often overlooked. Unlike large enterprises with ample resources to invest in robust cybersecurity measures, SMBs often lack the budget, expertise, and personnel necessary to protect themselves adequately from cyberattacks. This vulnerability makes SMBs prime targets for malicious hackers.

In 2025, SMBs are projected to spend $29.8 billion on managed security services, with overall cybersecurity spending expected to reach $90 billion, up from $57 billion in 2020. The regions anticipated to have the highest spending are North America, the Asia Pacific, and Western Europe (Statista).



Gartner has highlighted several key trends to watch in the coming years:

Through 2026: 75% of organizations will exclude unmanaged, legacy, and cyber-physical systems from their zero trust strategies. Zero trust involves granting users and endpoints only the access needed for their roles, with continuous monitoring. However, this approach is challenging to apply to unmanaged devices, legacy applications, and CPS designed for specific tasks in environments focused on safety and reliability.

By 2027: Two-thirds of global 100 organizations will extend directors and officers (D&O) insurance to cybersecurity leaders due to personal legal exposure. New regulations, like the SEC's cybersecurity disclosure and reporting rules, increase personal liability for cybersecurity leaders. Gartner advises updating the roles and responsibilities of the CISO and exploring D&O insurance to mitigate personal liability and professional risk.

By 2028: Enterprise spending on combating malinformation will exceed $500 billion, consuming 50% of marketing and cybersecurity budgets. Advanced technologies enable bad actors to create and spread highly effective, mass-customized malinformation. Gartner recommends that CISOs define responsibilities for anti-malinformation programs and invest in tools and techniques to counteract these threats.

Erik Hedlund, CEO of SeqOps, emphasizes the critical role of partnerships in enhancing cybersecurity for SMBs: "In today's complex cyber landscape, SMBs cannot afford to tackle cybersecurity alone. Our partnerships are essential in providing the expertise and resources necessary to defend against evolving threats. By collaborating, we not only strengthen individual defenses but also build a more resilient cybersecurity ecosystem for all."

9. **Join Us Today!**

Improve your cybersecurity offerings, optimise your operational efficiency, and unlock new revenue streams by joining the SeqOps Partner Program. Enjoy access to specialized training, comprehensive support, and an expert network dedicated to your success. Partner with SeqOps to advance your security services and achieve remarkable growth.

Contact us today to learn more about the SeqOps Partner Program and how we can help you transform your cybersecurity strategy.

References

Gartner Unveils Top Eight Cybersecurity Predictions for 2024. SYDNEY, Australia, March 18, 2024. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2024-03-18-gartner-unveils-top-eight-cybersecurity-predictions-for-2024

Borgeaud, Alexandra. Global SMB cyber security spending forecast 2025, by category. Published by Statista, March 31, 2023. Retrieved from https://www.statista.com/statistics/1245710/cyber-security-spending-category-forecast-smb/