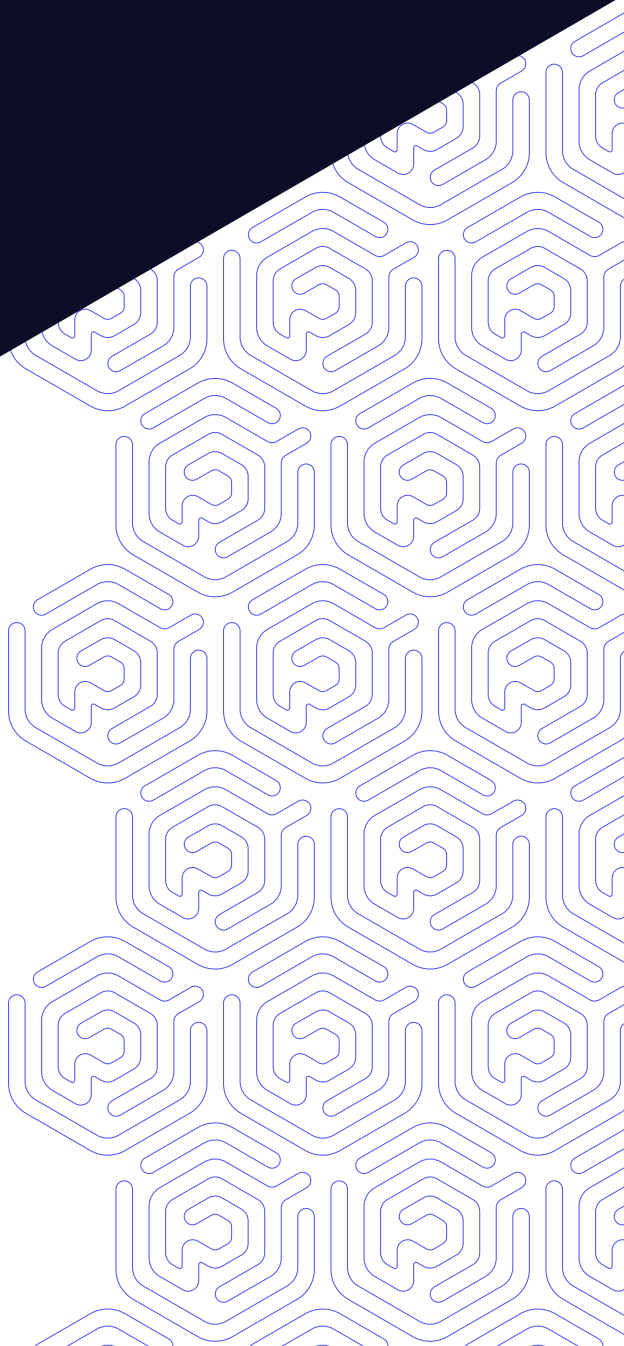
WHITE PAPER

The Case for Offensive Security

The Hand Which Strikes Also Blocks



praetorian

A Prevention First Strategy

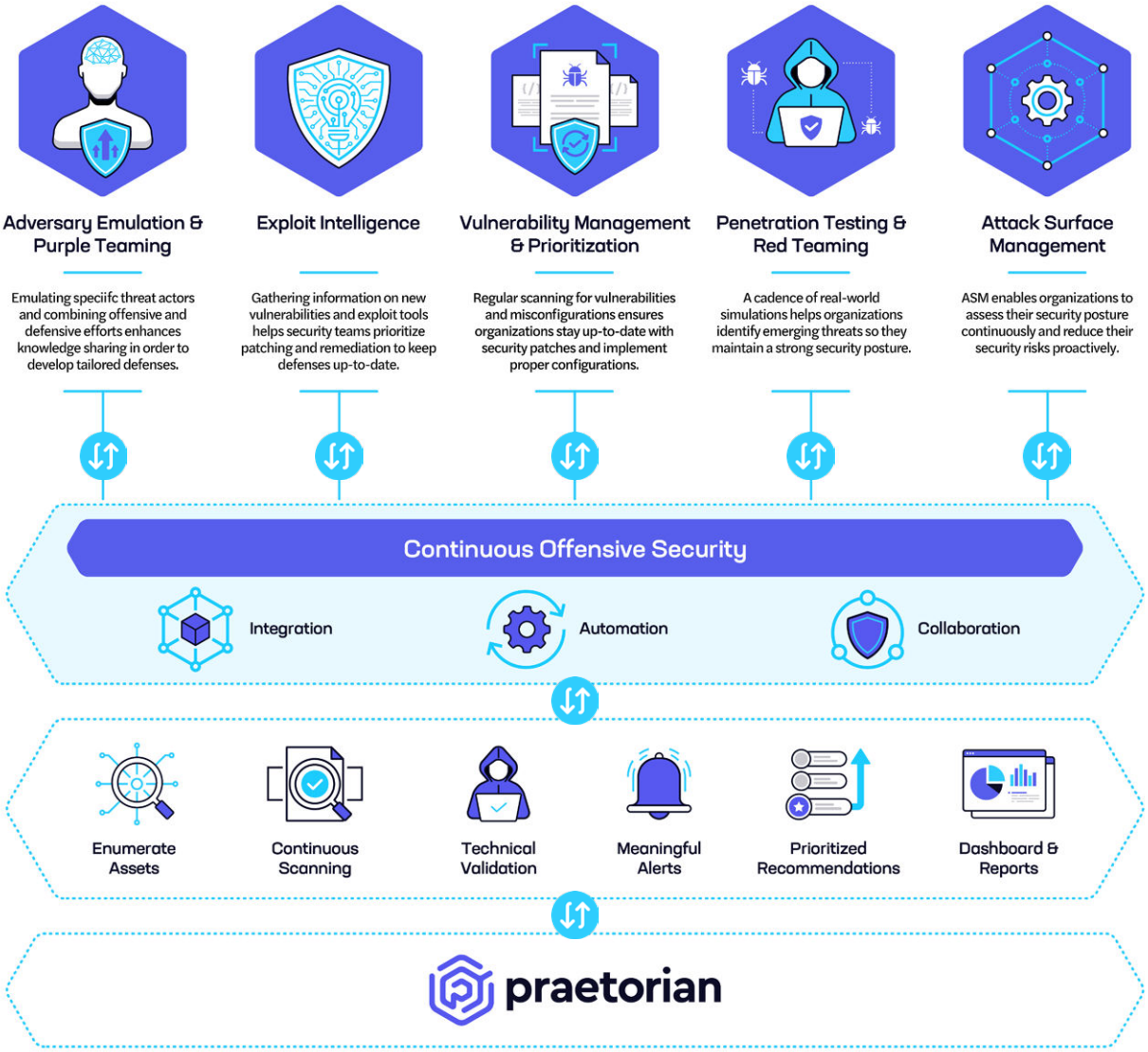
INSIDE THIS REPORT

In an ever-evolving cyber security landscape, the art of identifying vulnerabilities and preventing breaches serves as a harmonious counterpart to the science of detecting and responding to threats. Just as in the balance of yin and yang, where one complements and cannot exist without the other, identification and prevention provide that critical equilibrium to detection and response. If we view detection and response as our reaction to breaches after they have occurred, then identification and prevention are the proactive measures taken to ensure those breaches never happen in the first place. For a truly holistic cyber security approach, an organization must recognize that prevention is as vital, if not more so, than cure. Hence, shifting our perception of offensive security from a mere tactical activity to a strategic directive ensures that we're not just reacting to threats but anticipating and mitigating them. This allows organizations to shift from an "assume breach" mentality to a prevention first strategy.

What Is Continuous Offensive Security?

Traditionally, offensive security – involves tactical activities such as penetration testing and red teaming – that are leveraged as a periodic check on the organization's cyber defenses. While undoubtedly valuable, this perspective restricts its foundational benefit. Continuous Offensive Security, on the other hand, represents a paradigm shift in cyber security strategy. It shifts the organization from viewing offensive security as a tactical, point in time review of their cyber security posture to a continuous central security strategy of active defense through offensive initiative.

Specifically, COS is an advanced approach to cybersecurity that proactively and continuously simulates the tactics, techniques, and procedures of real-world adversaries. By combining multiple offensive security solutions into a unified platform, COS aims to strengthen an organization's security posture. In this way, COS prevents breaches by continuously emulating attackers to help you identify and mitigate your material risks before threat actors have the opportunity to exploit them. By staying ahead of emerging threats, organizations can maintain a strong security posture and avoid the high costs associated with a data breach.



At the core of COS is a locate and demonstrate compromise through continuous offensive security testing. This involves prioritizing vulnerabilities based on their impact on an organization's business objectives and allocating resources to address the most critical vulnerabilities first. This is accomplished by combining several offensive security solutions into a single platform that includes attack surface management, red teaming and penetration testing, vulnerability triage and prioritization, exploit intelligence, and adversarial emulation. As a managed service, COS solutions augment defensive teams with external offensive security expertise. This approach makes th value proposition turn key with immediate uplift to an organization's cyber security maturity.

COS also involves a continuous improvement process, which means that the program is **constantly evolving and adapting** to new threats and vulnerabilities. This can include new asset discovery, vulnerability triage and validation, regular red team exercises, and real-time monitoring of exploit intelligence feeds. According to a 2020 survey by Forrester Consulting, 80% of organizations that adopted a proactive approach to cybersecurity testing reported improved con dence in their security posture.

The Need For Continuous Offensive Security

Continuous offensive security solutions prevent breaches by continuously emulating attackers to help you identify and mitigate your material risks before threat actors have the opportunity to exploit them. By staying ahead of emerging threats, organizations can maintain a strong security posture and avoid the high costs associated with a data breach.

> ! This change in threat environment necessitates a shift from reactive to proactive security measures and from point in time security assessment to continuous security testing.

COS **proactively identifies potential threats**, identies weaknesses in systems and applications, and helps defensive teams demonstrate the risk of vulnerabilities and advocate for their remediation before they are exploited by an attacker. The end results of a COS program include the following:

- A more resilient and agile response to emerging threats
- Greater visibility into an organization's risk exposure and potential attack vectors
- Improved security posture through constant discovery of unknown material risks
- Better alignment of security practices with business objectives

Furthermore, COS can help organizations avoid the potentially signi cant nancial impact of a successful attack. According to the Ponemon Institute's 2022 Cost

of a Data Breach Report, the global average cost of a data breach in 2021 was $4.35 million. By adopting a more proactive and continuous approach to security testing, organizations can reduce the risk of a successful cyber-attack and potentially avoid the high costs associated with a data breach.

Why Choose Continuous Offensive Security Over Other Solutions?

The market offers several different approaches to cybersecurity testing and validation, including bug bounty programs and separate point products for attack surface management, breach and attack simulation, and continuous automated red teaming. A COS managed service solution is a better option for several reasons.

First and Foremost: A Partnership, Not a Product.

A successful COS program is not just about the technology, but also about the people and processes that support it. That's why we take a partnership approach with our clients to help them achieve their cybersecurity goals. Understanding their unique security challenges and objectives enables us to tailor our services to meet their speci c needs.

We base our partnership approach on the following principles:

1. **Trust:** We believe that trust is essential to a successful partnership. Our clients trust us to provide them with the best possible cybersecurity solutions and to act in their best interests at all times.

2. **Collaboration:** We work closely with our clients to develop a deep understanding of their security needs and objectives. This collaboration helps us to develop tailored solutions that are speci cally designed to meet their unique requirements.

3 **Expertise:** Our team of security experts has years of experience in the cybersecurity industry. We leverage this expertise to provide our clients with the best possible guidance and advice. This includes being credited with 68 CVEs and 33 MITRE ATT&CK TTPs.

4 **Continuous Improvement:** Cybersecurity threats are constantly evolving, and so are our solutions. We are committed to continuous improvement and work closely with our clients to ensure that our solutions are always up-to-date and effective.

Our partnership approach has been key to our success in delivering effective COS solutions to our clients. By working closely with our clients to identify and remediate vulnerabilities before they can be exploited, we help them build a more resilient and agile security posture. Our clients have peace of mind knowing that they have a trusted partner who is committed to their success.

Other Key Differentiators of Continuous Offensive Security

Consolidation Savings: COS combines several areas of spend, including attack surface management, red teaming, penetration testing, breach and attack simulation, vulnerability verification and prioritization, and exploit intelligence into a single managed offering, reducing the total cost of ownership and vendor complexity.

Augmented with Experts: Since COS is a managed service, it includes security experts who have the expertise to identify and remediate vulnerabilities. They also can provide actionable insights to improve security posture. In contrast, point products often require in-house expertise to operate effectively, which can be a significant challenge for organizations that do not have dedicated security teams.

Risk-Based Prioritization: COS takes a risk-based approach to security testing, which prioritizes vulnerabilities based on their impact on an organization's business objectives. This ensures that resources are allocated to address the most critical vulnerabilities, resulting in a more efficient and effective security posture.

Zero False Positives: Because COS is managed by experts, the solution guarantees zero false positives from the verification and validation process with a commitment to only signal when a risk is both real and material.

Provides Proactive Defense: COS keeps organizations several steps ahead of attackers by continuously identifying and mitigating potential vulnerabilities and attack vectors before attackers can exploit them. By adopting a more proactive and continuous approach to security testing, organizations can potentially avoid the high costs associated with a data breach.

Includes Full Scope: COS challenges industry norms around applying an artificial "scope" to testing. Traditionally, organizations have focused on testing a specific subset of their systems or applications based on predefined criteria such as the most critical assets or the most likely attack vectors. This approach can result in blind spots and cause organizations to miss material exposures and vulnerabilities that exist outside of the defined scope.

Satisfies 3rd Party Penetration Testing Compliance Requirements: COS is designed to help organizations achieve compliance with regulatory frameworks such as GDPR, HIPAA, and PCI DSS. Managed service partners have expertise in compliance and can help organizations navigate the complex regulatory landscape.

Common Use Cases for Continuous Offensive Security

Mergers and Acquisitions: During M&A activities, organizations must assess the cybersecurity posture of the target company. COS techniques like red teaming and penetration testing can help identify vulnerabilities, assess security risks, and ensure a smooth integration of digital assets.

Supply Chain Risk Management: As organizations rely on third-party vendors and service providers, they must ensure that these partners maintain strong security practices. COS can evaluate the security posture of third parties, identify potential risks, and develop strategies to mitigate these risks.

FDA Premarket Submission and Postmarket Monitoring: In the healthcare industry, the FDA requires medical device manufacturers to ensure the security of their devices before they can be marketed in the US. COS validates medical device security as part of the premarket submission and then continuously monitors the security of medical devices post-market. This helps ensure that medical devices remain secure against evolving cyber threats, protecting patient safety and data privacy.

Securing Digital Transformation: As organizations increasingly migrate to the cloud, they must ensure that their cloud-based assets are secure. COS can help identify miscon gurations, vulnerabilities, and potential attack vectors in cloud environments, enabling organizations to secure their cloud infrastructure effectively.

Satisfying Regulatory Compliance Requirements: Regulatory frameworks, such as GDPR, HIPAA, and PCI DSS, require organizations to maintain strong security practices. As a managed service that includes manual penetration testing, COS satis es compliance annual penetration testing requirements.

Validating Incident Response Preparedness: Organizations must be prepared to respond effectively to security incidents. COS can help organizations develop and test their incident response plans, ensuring they are ready to respond quickly and effectively when an incident occurs.

Conclusion

Overall, Continuous Offensive Security can be a valuable tool for any organization that wants to proactively defend its digital assets against cyber threats. By employing COS techniques, organizations can identify vulnerabilities, assess risks, and remediate security gaps before attackers successfully exploit them. This can result in a more resilient and agile security posture, better alignment of security practices with business objectives, and improved compliance with regulatory frameworks.

RESOURCES

"The State of Network Security, 2020-2021."
Homes, David and Shey, Heidi. Forrester Consulting. 2 August 2021.

"2022 Cost of a Data Breach Report."
Ponemon Institute. 2022.