2025

seceon

Seceon aiSecurityScore360: Illuminating the Hidden Risks of Your Attack Surface

A comprehensive approach for uncovering hidden external vulnerabilities and reducing cyber risk.

Table Of Content

1. **Introduction**
2. **The Expanding and Evolving Attack Surface**
3. **Seceon aiSecurityScore360- Gaining Complete Attack Surface Visibility**
4. **Benefits of Seceon aiSecurityScore360**
5. **How aiSecurityScore360 Works:**
6. **Conclusion**

Introduction:

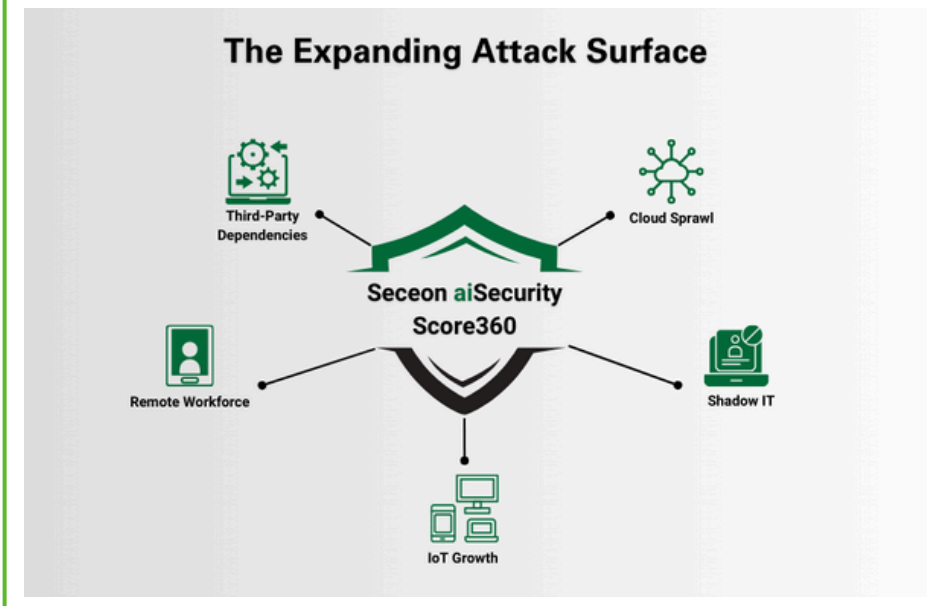
The rapid adoption of cloud, remote work, IoT, and third-party services has shattered the traditional network perimeter. This expansion has introduced new vulnerabilities and blind spots that traditional security tools fail to address. Cloud adoption, remote workforces, IoT devices, and the increasing reliance on third-party services have blurred the traditional network perimeter, creating new vulnerabilities and blind spots. Traditional security tools, often focused on internal threats, struggle to provide a comprehensive view of an organization's external risk exposure. Seceon aiSecurityScore360 offers a powerful solution, providing continuous attack surface management (ASM) to illuminate these hidden risks and empower organizations to proactively defend against evolving cyber threats. This white paper explores the challenges of modern attack surface management and demonstrates how aiSecurityScore360 enables organizations to gain complete visibility, prioritize remediation efforts, and significantly improve their security posture.

The Expanding and Evolving Attack Surface:

The digital transformation has brought about significant benefits, but it has also dramatically expanded the attack surface. Organizations now contend with:

- **Cloud Sprawl:** Complex cloud footprints obscure visibility.
- **Shadow IT:** Unauthorized apps introduce hidden risks.
- **IoT Growth:** Weak device security expands entry points.
- **Remote Workforce:** Off-network endpoints are harder to secure.
- **Third-Party Dependencies:** Vendor vulnerabilities become yours.

This expanded attack surface presents a significant challenge for security teams, who struggle to maintain visibility and prioritize remediation efforts. Traditional security tools, focused primarily on internal threats, often fail to address the external attack surface, leaving organizations exposed to a wide range of risks.



Seceon aiSecurityScore360: Gaining Complete Attack Surface Visibility:

Seceon aiSecurityScore360 is a comprehensive attack surface management platform that provides organizations with a continuous and holistic view of their external risk exposure. It goes beyond traditional vulnerability scanning to include a wide range of capabilities, including:

- **Comprehensive Attack Surface Discovery:** aiSecurityScore360 automatically discovers all internet-facing assets belonging to the organization, including websites, applications, servers, cloud resources, IoT devices, and more. This comprehensive discovery process ensures that no asset is overlooked.
- **Vulnerability Assessment:** The platform identifies vulnerabilities in internet-facing systems and applications, including known exploits, misconfigurations, outdated software, and other weaknesses. It goes beyond simple vulnerability scanning to assess the actual risk posed by each vulnerability.
- **Dark Web Monitoring:** aiSecurityScore360 actively monitors the dark web for compromised credentials, data leaks, and other sensitive information that could be used to target the organization. This proactive approach helps organizations identify and mitigate potential threats before they can be exploited.
- **Domain Masquerading Detection:** The platform monitors for domain registrations that are similar to the organization's own domains, helping to protect against phishing and other attacks that rely on spoofed domains. This includes checking for typosquatting, homoglyph attacks, and other domain variations.

Know Every Asset You Own

Comprehensive discovery ensures no internet-facing asset is overlooked—because you can’t secure what you can’t see.

Misconfigurations: The Silent Threat

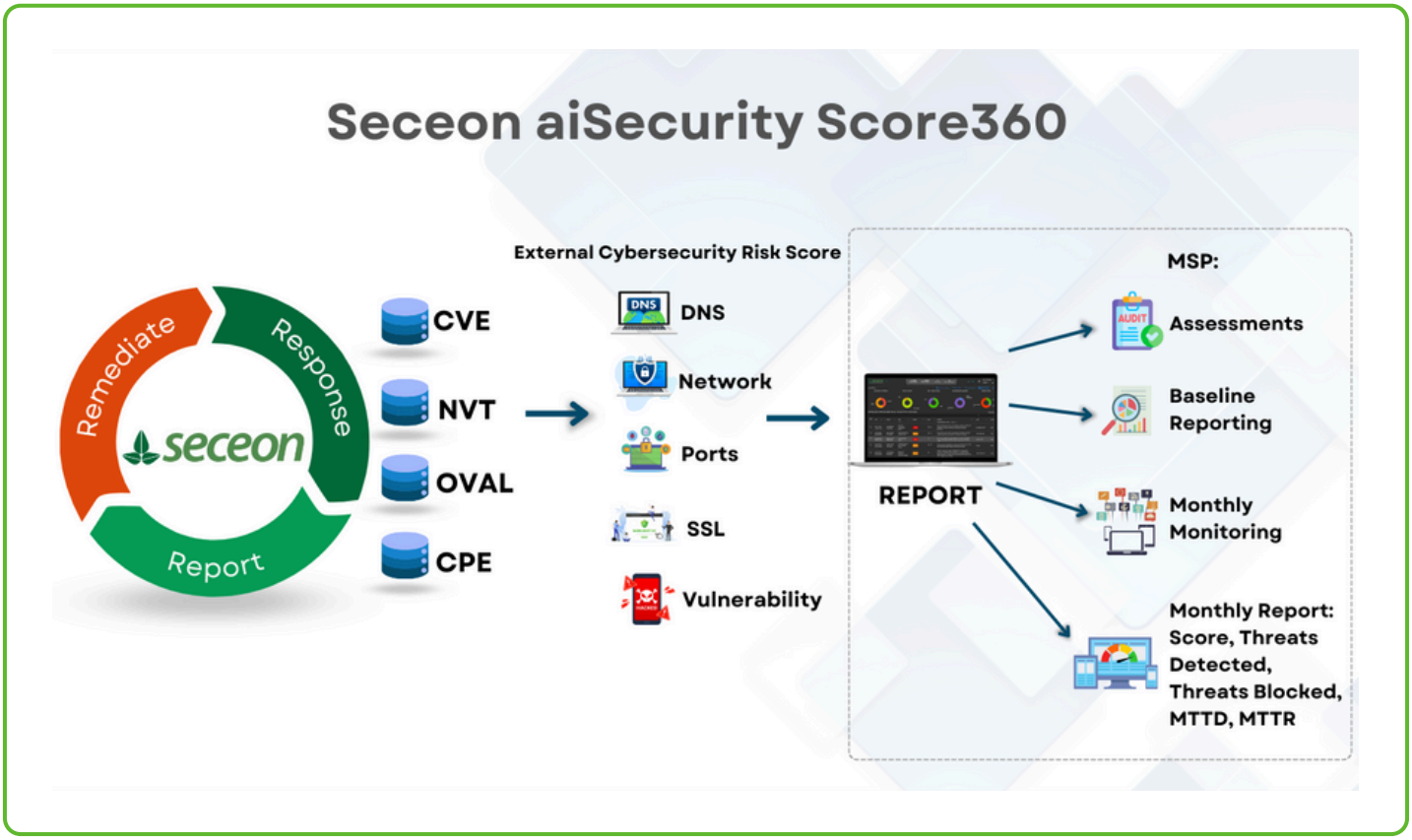
Simple missteps like open ports or default credentials can expose you—continuous assessment uncovers hidden weaknesses before attackers do.

- **SSL Certificate Monitoring:** aiSecurityScore360 monitors SSL certificates for expiration, misconfigurations, and other issues that could create security vulnerabilities or disrupt business operations. This includes monitoring all domains and subdomains associated with the organization.
- **Application Misconfiguration Analysis:** Beyond just identifying known vulnerabilities, aiSecurityScore360 also checks for application misconfigurations that could create security weaknesses, such as open ports, default credentials, or overly permissive access controls.
- **Internal Security Posture Monitoring:** aiSecurityScore360 extends its capabilities to the internal network, scanning for vulnerabilities and misconfigurations in internal systems and applications. This provides a holistic view of the organization's security posture, both external and internal.
- **Risk Scoring and Prioritization:** The platform assigns a risk score to each identified vulnerability and risk, based on its severity, potential impact, and exploitability. This allows organizations to prioritize remediation efforts and focus on the most critical threats.
- **Threat Intelligence Integration:** aiSecurityScore360 integrates with threat intelligence feeds to identify vulnerabilities that attackers are actively exploiting. This helps organizations prioritize patching and other mitigation efforts.
- **Actionable Insights and Remediation Guidance:** The platform provides actionable insights and specific recommendations for remediating identified vulnerabilities and mitigating risks. This helps security teams quickly address security gaps and reduce their attack surface.

- **Continuous Monitoring and Reporting:** aiSecurityScore360 continuously monitors the attack surface for new vulnerabilities and changes in risk exposure, providing organizations with an up-to-date view of their security posture. Comprehensive reporting and analytics capabilities help organizations track their security posture over time and identify trends in their risk exposure.

Benefits of Seceon aiSecurityScore360:

- **Proactive Risk Management:** By identifying and prioritizing vulnerabilities and risks, aiSecurityScore360 helps organizations proactively manage their cybersecurity risks and prevent attacks before they occur.



- **Reduced Attack Surface:** The platform helps organizations reduce their attack surface by identifying and remediating security gaps, misconfigurations, and other weaknesses.
- **Improved Security Posture:** Continuous monitoring and assessment help organizations maintain a strong security posture and stay ahead of evolving threats.
- **Faster Remediation:** Actionable insights and remediation guidance help security teams quickly address vulnerabilities and reduce the risk of exploitation.
- **Reduced Costs:** By preventing security breaches, aiSecurityScore360 can help organizations avoid the significant financial losses associated with cyberattacks.
- **Compliance Support:** The platform helps organizations meet compliance requirements by providing visibility into their external risk exposure and demonstrating their commitment to security.

Continuous Visibility, Zero Blind Spots

Asset discovery, dark web monitoring, and domain protection work around the clock to detect risks as your attack surface evolves.

How aiSecurityScore360 Works:

- **Asset Discovery:** aiSecurityScore360 automatically discovers all internet-facing assets belonging to the organization.
- **Scanning and Assessment:** The platform performs scans and assessments to identify vulnerabilities, misconfigurations, and other security weaknesses.
- **Dark Web Monitoring:** The platform continuously monitors the dark web for compromised credentials and other sensitive information.
- **Domain Monitoring:** The platform monitors for domain registrations that are similar to the organization's own domains.

Focus Where It Matters Most

Not all risks are equal. Prioritizing high-impact vulnerabilities ensures your team addresses what truly matters—fast.

- **SSL Certificate Monitoring:** The platform monitors SSL certificates for expiration and other issues.
- **Risk Scoring and Prioritization:** The platform assigns a risk score to each identified vulnerability and risk.
- **Threat Intelligence Integration:** Threat intelligence feeds are used to identify vulnerabilities being actively exploited.
- **Reporting and Analysis:** The platform generates reports and provides analytics on the organization's risk exposure.
- **Remediation:** Security teams use the information provided by aiSecurityScore360 to remediate vulnerabilities and mitigate risks.

Seceon aiSecurity Score360 Dashboard

Conclusion:

In today's complex and dynamic threat landscape, managing the attack surface is a critical challenge for organizations of all sizes. Seceon aiSecurityScore360 provides a powerful and comprehensive solution, enabling organizations to gain complete visibility into their external risk exposure, proactively identify and prioritize vulnerabilities, and significantly improve their security posture. By combining advanced scanning techniques, dark web monitoring, domain protection, and threat intelligence integration, aiSecurityScore360 empowers organizations to stay ahead of evolving threats and protect their valuable assets. See how Seceon aiSecurityScore360 can uncover your hidden vulnerabilities and reduce cyber risk. Contact us for a demo today.

About the Author

Chandra S. Pandey

Founder & CEO, Seceon Inc.

As a Founder and CEO of Seceon, Chandra Pandey brings over 20 years of cybersecurity and networking experience. He leads the development of integrated SIEM, SOAR, and XDR solutions, helping over 8,800 organizations simplify security, reduce costs, and achieve real-time threat protection.

© 2025 Seceon Inc. All rights reserved. aiSIEM, aiXDR, are trademarks and registered trademarks of Seceon Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.