Balbix

9 Attack Surface Metrics That Will Slash Your Risk Exposure — Starting Now

9 Attack Surface Metrics That Will Slash Your Risk Exposure — Starting Now

Organizations are facing an ever-expanding attack surface in terms of complexity and scale. Without a keen understanding of your organization's attack surface, you're leaving open doors for bad actors. It's not just about securing systems; it's about knowing your vulnerabilities, managing them effectively, and continuously closing gaps.

The days of running periodic vulnerability scans and calling it a day are long gone. Cybercriminals don't wait, and neither should you. Attack surfaces are now borderless, from internal networks to user devices, from on-prem systems to cloud environments. Every entry point is a potential target; failing to monitor them continuously and precisely is a recipe for disaster.

This is where the nine attack surface metrics come into play. These aren't just numbers to toss into a report — they're game-changing insights that can make an organization more resilient to cyberattacks. You are already ahead of most organizations if you can get these metrics and actively track them.

Asset Visibility and Exposure Metrics

The following three metrics provide a complete view of your organization's digital assets, both internal and external, and help identify which are vulnerable to attack. Tracking exposed assets and endpoint protection gaps ensures you know risks across your infrastructure, enabling proactive defenses.

1. Attack Surface Visibility (Internal, External, Digital, User, Cloud)

Attack surface visibility provides a complete view and enumeration of all assets — internal assets, external-facing assets, digital properties, user and user devices, and cloud environments.

Example

According to the Cloud Security Alliance, 23% of organizations have no visibility into their cloud environments and 77% report suboptimal transparency. This gap in visibility could leave numerous vulnerabilities unaddressed, leaving organizations susceptible to breaches. Every organization should consider an asset management system to aggregate and discover assets, including shadow assets.

Actionable Guidance

Organizations should deploy tools that automatically discover and inventory assets across internal, external, digital, user, and cloud environments for comprehensive attack surface visibility. An asset inventory is an excellent foundational step to build other IT and security programs.

Challenges such as shadow IT, misconfigurations, and outdated systems may complicate visibility efforts. Regular audits, automated asset discovery, and security integrations can help overcome these issues and maintain a robust security posture.

2. Number of Exposed Assets (Externally Exposed)

Externally exposed assets, such as public-facing servers and applications, are prime targets for attackers. The higher the number of exposed assets, the greater the potential for exploitation.

Example

A 2023 Qualys report shows that, for the average organization, only 4% of network assets are externally exposed. Security teams should swiftly remediate these exposures and inform the CISO if their external exposure rate is significantly higher than the industry average. This would justify investment in security monitoring and tools to better secure assets and reduce the financial risk to the company.

Actionable Guidance

Organizations should monitor all public-facing assets to reduce the risks posed by externally exposed assets. Prioritizing these assets based on their business impact allows teams to focus on the most critical targets first.

Challenges such as gaps in asset discovery, resource constraints, and ongoing maintenance can hinder these efforts. Addressing these through automated scanning, proper configuration, and regular updates ensures that exposed assets remain secure.

3. Percentage of Assets Without Endpoint Protection

Endpoint devices like desktops/laptops and servers are entry points for attackers. Assets without endpoint protection are vulnerable to malware, ransomware, and other attacks. Tracking the percentage of all assets without endpoint protection and reducing that percentage over time reduces the potential for such exploits.

Example

According to Expert Insights, one-third of the UK and US small businesses rely on free, consumer-grade cybersecurity solutions, and 23% use no endpoint security platform. A plan to deploy enterprise endpoint security on all devices will reduce the risk of exploitation.

Actionable Guidance

Implementing EDR on more devices is critical to improving endpoint coverage, but several challenges may arise. User resistance to change, configuration and permission issues, and the need for regular maintenance and updates are common obstacles. This highlights the importance of having strong visibility and adopting a defense-in-depth strategy to address these challenges effectively.

Vulnerability and Risk Management Metrics

The following three metrics focus on identifying, prioritizing, and addressing vulnerabilities across your organization. By targeting critical CVEs and misconfigurations, security teams can mitigate risks with the highest impact on the organization's security.

4. Unpatched Critical Vulnerabilities

Unpatched critical vulnerabilities are low-hanging fruit for attackers. These weaknesses can be easily exploited if not addressed promptly, leading to data breaches or system compromises.

Example

According to the recent Ponemon report, sponsored by Balbix, unpatched critical vulnerabilities are prime targets for cyberattacks. If unresolved, these vulnerabilities can lead to millions in financial losses. Security teams should prioritize the remediation of these vulnerabilities based on their potential financial risk.

Actionable Guidance

Unpatched critical vulnerabilities are prime targets for cyberattacks, making immediate remediation essential. To address these efficiently, prioritize remediation based on the vulnerabilities that would have the highest financial impact on your organization if breached. Implement automated patch management systems to streamline this process and reduce human error. Regular vulnerability scanning can help identify new weaknesses quickly.

Challenges include patching delays due to system incompatibility or resource limitations. Organizations can overcome these by establishing clear patching policies, conducting regular audits, and leveraging third-party tools for patch deployment across diverse environments.

Honing in on and quickly remediating unpatched critical vulnerabilities that would have the highest financial impact on your organization and remediating them first allows you to burn down risk with minimal resource impact.

5. Number of Critical Vulnerabilities in Applications (and Closed)

Tracking the **Number of Critical Vulnerabilities in Applications (and Closed)** provides insight into an organization's risk posture. Application vulnerabilities, such as **SQL injection, cross-site scripting (XSS), buffer overflows, authentication flaws**, and **insecure deserialization**, represent significant security risks. These vulnerabilities, when exploited, can lead to data breaches, system compromises, or denial of service attacks. Monitoring open and closed vulnerabilities helps assess the effectiveness of vulnerability management. Automated tools can streamline identifying and patching these vulnerabilities, though challenges include resource allocation and timely remediation across complex environments.

Example

Multiple cybersecurity frameworks recommend companies remediate critical vulnerabilities within 24 to 72 hours to minimize exploitation risks. Security teams should report to the CISO if current detection and response times are suboptimal, recommending investment in tools to accelerate vulnerability remediation and enhance security posture.

Actionable Guidance

Automated tools such as vulnerability scanners and patch management solutions can streamline identifying and closing critical vulnerabilities. However, be aware of challenges in large, distributed environments, such as resource limitations and patching complexity.

6. Number of Misconfigurations Detected (and Closed)

Similar to CVEs, misconfigurations can lead to security incidents. Examples of misconfigurations include:

- **Weak/default Permissions:** Overly permissive access rights to data or systems
- **Exposed Cloud Storage:** Cloud storage buckets (e.g., AWS S3) left publicly accessible
- **Lack of Multi-Factor Authentication (MFA):** Relying solely on passwords increases the risk of account compromises

Example

According to OWASP, in 2024, 90% of applications tested showed at least one misconfiguration, with an average incidence rate of 4.5%. This highlights the importance of continuous monitoring and quick remediation to prevent costly breaches. Organizations should identify and quickly remediate critical application misconfigurations that can expose sensitive company and customer data, potentially resulting in millions in losses.

Actionable Guidance

Cloud Security Posture Management (CSPM) tools are essential to maintain continuous oversight over misconfigurations in complex environments. These solutions automatically discover, track, and monitor assets across internal systems, external platforms, cloud environments, and user devices, providing real-time visibility. This helps identify and flag misconfigurations — such as weak permissions or exposed cloud storage — across multiple systems.

Implementing and maintaining these solutions can be resource-intensive, requiring skilled personnel and ongoing updates. Additionally, managing large volumes of data from multiple systems can lead to alert fatigue, where critical misconfigurations may be overlooked. Integration between tools can also be complex, making it harder to ensure seamless visibility across the entire infrastructure.

Network and User Access Control Metrics

The following three metrics help manage and secure access to your internal systems, ensuring that breaches are contained and elevated access is controlled. Proper network segmentation and user access control reduce the risk of lateral movement and insider threats.

7. Internal Network Segmentation Status

Proper network segmentation helps contain breaches by limiting lateral movement within the network. Without segmentation, attackers can move freely, escalating access and causing more damage. Metrics may include tracking:

- **Access Control Rules:** Regularly review network access control policies, including firewalls and ACLs, to regulate traffic between segments and limit unauthorized access.
- **Segmentation Testing:** Conduct penetration tests and simulated attacks to measure how effectively segments prevent unauthorized access and limit lateral movement across the network.
- **Segmentation Policy Compliance:** Ensure adherence to industry standards (e.g., PCI-DSS) through micro-segmentation tools that provide insights into policy compliance and minimize attack surfaces.

Example

2024 IBM Cost of a Data Breach Report notes that organizations with solid segmentation measures save, on average, 20% on breach costs compared to those without segmentation. This is due to the potential for lateral movement through a compromised network after gaining initial access, giving broad access to valuable assets. Segmenting the network is essential in reducing the scope of future attacks and mitigating potential financial damage.

Actionable Guidance

Reviewing access control rules and policies ensures that inter-segment traffic is appropriately regulated. Testing through penetration and segmentation analysis helps identify weaknesses in current defenses. Adhering to segmentation policies aligned with industry standards, such as PCI-DSS, improves security posture.

Maintaining segmentation across dynamic environments can be resource-intensive. Enforcing consistent policies, testing regularly, and managing compliance in complex networks require dedicated attention and ongoing monitoring.

8. Mean Time to Detect (MTTD) of Exposed Assets

This metric measures the average time it takes for an organization to identify a potential security threat or vulnerability from the moment it occurs. Rapid detection is crucial for minimizing exposure and mitigating potential risks promptly. MTTD ensures organizations can respond swiftly to emerging threats. A lower MTTD translates into faster incident response and reduced attack windows for adversaries. MTTD is calculated by dividing detection time by the number of vulnerabilities.

Example

According to the 2024 IBM Cost of a Data Breach Report, organizations extensively using security AI and automation identified and contained data breaches nearly 100 days faster on average than organizations that didn't use these technologies. This demonstrates the financial and security benefits of faster threat detection using automated monitoring tools and real-time threat detection systems.

Actionable Guidance

To improve MTTD, organizations should implement automated monitoring tools and real-time threat detection systems. Regular vulnerability assessments and continuous asset monitoring can decrease detection time, ensuring faster action against threats.

Achieving a low MTTD requires significant resources, such as advanced monitoring tools and skilled personnel. Lack of visibility into asset exposure and delayed threat intelligence may also hinder efforts to reduce detection time.

9. Number of Over-Privileged User Accounts Detected (and Closed)

Privileged user accounts are critical to an organization's security, granting access to sensitive data, systems, and administrative functions. However, they are also prime targets for attackers due to their elevated access, making them vulnerable to insider threats and external exploitation. If compromised, privileged accounts can allow cybercriminals to exfiltrate data, disable security protocols, or disrupt operations due to two types of overprivileged users:

- **Insider Threats:** Employees or contractors with privileged access can intentionally or unintentionally misuse these accounts, leading to significant breaches. As the 2024 Verizon Data Breach Investigations Report highlights, insider threats are responsible for a substantial portion of data breaches.
- **External Exploitation:** Attackers often target privileged accounts through phishing, brute-force attacks, or credential stuffing, giving them direct access to critical systems. Reducing unnecessary privileged accounts and enforcing least-privilege policies can mitigate these risks by limiting exposure and ensuring that access is granted only when necessary.

Example

The 2024 Verizon Data Breach Investigations Report indicates that 74% of breaches involve the human element, including privileged misuse. By closing unused privileged accounts and applying the principle of least-privileged access, organizations can remove a major insider threat and reduce their attack surface, minimizing the risk of privilege escalation attacks.

Actionable Guidance

Over-privileged users pose a significant insider security threat if left unchecked. Reducing the number of unnecessary privileged accounts helps mitigate insider threats and limits the potential damage from external attacks. Organizations should regularly audit privileged accounts, identify over-privileged users, and close or reduce unnecessary permissions.

Manual auditing is time-consuming and resource-intensive. Also, resistance from users accustomed to broader access can slow down the implementation of tighter controls. Automate privileged access reviews with a PAM tool and enforce least-privilege policies to ensure that users only retain necessary permissions for their roles. This improves security posture while minimizing operational disruption.

Conclusion

Monitoring these nine attack surface metrics provides critical insights into where your organization is most vulnerable and allows for targeted actions that significantly reduce risk exposure. By addressing exposed assets, unpatched vulnerabilities, misconfigurations, and more, organizations can slash their risk of cyberattacks and demonstrate proactive security management to stakeholders.

Request a demo to learn more about how Balbix can help you improve your security.

About Balbix **balbix.com**

Balbix is revolutionizing cyber risk management by providing businesses with the tools to effectively identify, prioritize, and mitigate their most critical security exposures. By integrating data from across the organization and leveraging advanced AI technologies, Balbix offers a unified platform for exposure assessment and risk quantification. Fortune 500 companies trust Balbix to protect their operations and ensure compliance in an ever-evolving threat landscape. Balbix was recognized in Forbes America's Best Startup Employers 2024 by CNBC in their 2022 Top 25 Startups for the Enterprise and ranked #32 on the 2021 Deloitte Fast 500 North America.

Balbix®