appgate

ADVANCED PENETRATION TESTING SERVICE

Introduction

Understanding how attackers view your infrastructure and network vulnerabilities is crucial to preventing potential breaches. Appgate's Penetration Testing Service simulates sophisticated, real-world attacks under controlled conditions, providing an unparalleled view of your actual security risks. Our cutting-edge Service goes beyond conventional penetration testing methodologies by aligning these findings with the principles of Zero Trust to provide you with unparalleled insights into your security posture. Our experts provide point-in-time assessments that offer:

- **Deep Testing Capabilities:** Our expert team can evaluate any part of your digital ecosystem, including networks, applications, wireless infrastructure, IoT devices, XaaS, and the humans who use them to uncover vulnerabilities that could be maliciously exploited.
- **Safety and Confidentiality:** We keep your data confidential and secure, keep you informed at every step, and maintain consistent engagement standards to continually earn your trust.
- **Tailored Exploit Development:** We develop custom exploits specific to your environment, so we consistently identify vulnerabilities that automated tools miss.
- **Zero Trust Alignment:** We operate on the principle that no user, device, or network should be trusted by default. This approach reflects the priorities of a modern Zero Trust architecture, frustrates today's advanced threat actors, and eliminates swaths of vulnerability exposure.
- **Actionable Intelligence:** We go beyond identifying issues to deliver a clear, detailed and prioritized roadmap for risk mitigation and security enhancement.
- **Proven Expertise:** Our team brings unmatched experience and insight to every test and assessment. With a 15-year history and thousands of tests conducted, including engagements with Fortune 20 clients across various critical infrastructure sectors, we have the expertise to handle your security needs.

By leveraging Appgate's Penetration Testing Service, you gain a strategic advantage, strengthening your defenses against both current and emerging threats. Our service not only identifies potential compromises, it also empowers you to proactively address vulnerabilities before they can be exploited. This safeguards critical assets, enabling you to scale your business securely. Our comprehensive blend of in-depth assessments and adversary tactics enhances your organization's resilience.

The Zero Trust Advantage

Appgate's Penetration Testing Service is fundamentally grounded in the Zero Trust security model, which operates on the principle that no entity inside or outside the network should be inherently trusted. This approach is essential in today's evolving threat landscape, where perimeter-based defenses alone are no longer sufficient. By assuming that all network activity is potentially hostile, our service rigorously tests access points, user permissions and system defenses to ensure your organization's security architecture and systems are resilient and capable of adapting to emerging threats.

In line with the key pillars of Zero Trust, we verify explicitly by testing every access request as though it originates from an untrusted network, ensuring that robust validation mechanisms are in place. We also evaluate whether your systems enforce least privilege access, confirming that users and devices have only the minimum access necessary to perform their functions, thus minimizing the risk of unauthorized escalation. Additionally, we operate under the assumption that a breach has already occurred, simulating sophisticated attacks to rigorously test your detection, containment and response capabilities.

USE CASES

Cybersecurity Hygiene: Build a continuous testing regimen across the full scope of your IT infrastructure. This validates the security of your products and services as you update them.

New Product Deployment: Evaluate potential risks and vulnerabilities before a product moves from development to operation to ensure a confident deployment or integration.

Compliance Validation: Test your security environment to verify compliance with regulatory standards like PCI-DSS, HIPAA, or GDPR.

Internet Exposure: Evaluate your organization's external internet exposure to identify the most critical gaps in your security posture and prioritize their closure.

IoT and OT Security Testing: Assess the vulnerabilities in Internet of Things (IoT) and Operational Technology (OT) environments to protect critical infrastructure and assets.

Network Segmentation Testing: Validate the effectiveness of network segmentation controls to limit lateral movement and secure sensitive areas of the network.

Appgate's Penetration Testing Service is designed to evaluate and reinforce systems in alignment with the seven core Zero Trust pillars:

- **Identity:** We validate that systems properly verify user identities and ensure the enforcement of the principle of least privilege. This ensures users and non-person entities have only the access necessary to perform their tasks, and excess permissions are removed once they're no longer needed. We also assess the provisioning and deprovisioning processes to ensure they align with organizational policies. Key identity validation measures, such as multi-factor authentication (MFA) and other controls, leveraged to validate identity are included in this phase.
- **Device:** We verify that only authorized devices are present on the network and ensure they meet organizational expectations. This includes confirming the legitimacy of virtual devices, enforcing network rules for device retirement, and verifying that decommissioned devices are correctly removed. Additionally, we assess device security posture to confirm that appropriate protections are in place, such as endpoint security measures and compliance with security baselines.
- **Network:** We evaluate how effectively systems segment the network, ensuring that access is restricted based on defined trust levels. This includes validating network access controls, isolating sensitive resources, and confirming that communication between segments adheres to security policies. Proper network segmentation limits lateral movement and mitigates the risk of unauthorized access.
- **Application:** We examine the security of applications, confirming that they enforce identity verification and device posture checks. This includes assessing how applications manage access controls, enforce session limits, and validate user and device states before granting access to critical data. We also analyze how applications are updated and patched to address vulnerabilities.
- **Data:** We test how data is protected both at rest and in transit, ensuring that encryption standards and data access policies are properly implemented. This includes validating data classification mechanisms, assessing encryption key management, and ensuring data visibility is limited to authorized users. Our goal is to confirm that data access aligns with Zero Trust principles, minimizing the risk of exposure or breaches.
- **Visibility and Analytics:** We assess the effectiveness of monitoring and analytics systems to ensure they provide comprehensive visibility into user and device activities. This includes evaluating log collection, anomaly detection and alerting capabilities to confirm that potential threats can be quickly identified and addressed.
- **Automation and Orchestration:** We examine how well security processes are automated to reduce manual intervention and enhance efficiency. This includes evaluating the integration of security tools, automated response capabilities and the adaptability of systems to changing conditions based on predefined policies and threat intelligence.

By aligning our penetration testing approach with Zero Trust principles, we provide an in-depth, realistic assessment of your security posture. Our comprehensive approach not only identifies vulnerabilities but also equips you with actionable insights and strategies to build a more resilient and adaptive defense system that can withstand the complexities of modern cyberthreats.

Advanced Penetration Testing Service: How it Works

Appgate's Advanced Penetration Testing Service emulates real-world attackers with tests customized to your environment. Our tests combine the power of automated tools (20%) with the depth and expertise of manual testing (80%). This includes deep analysis and custom-crafted attacks that closely mimic the strategies of sophisticated adversaries, giving you a clear understanding of your vulnerabilities and empowering you to proactively strengthen your defenses. Our tests emphasize the following key elements:

- **Identity Verification and Least-Privilege Access:** We test your systems' ability to verify identities and enforce least-privilege access, ensuring that only authorized users and devices have access to critical resources.
- **Segmentation and Isolation:** By testing how well you protect your critical assets within your network, we identify areas where adversaries could escalate privileges, move laterally, and gain unauthorized access.
- **Data Validation:** We understand how important data is to your business, but it must be secure. We test how data is ingested into your infrastructure to ensure you consistently receive the information you need without compromising safety.
- **Tactical Lateral Movement and Privilege Escalation Simulation:** We simulate real-world attacks involving lateral movement and privilege escalation to evaluate your environment's response capabilities and identify areas for improvement.
- **Actionable Reporting:** We provide a detailed risk analysis report that prioritizes vulnerabilities based on severity and potential business impact, coupled with specific Zero Trust-aligned remediation steps to fortify your security posture.

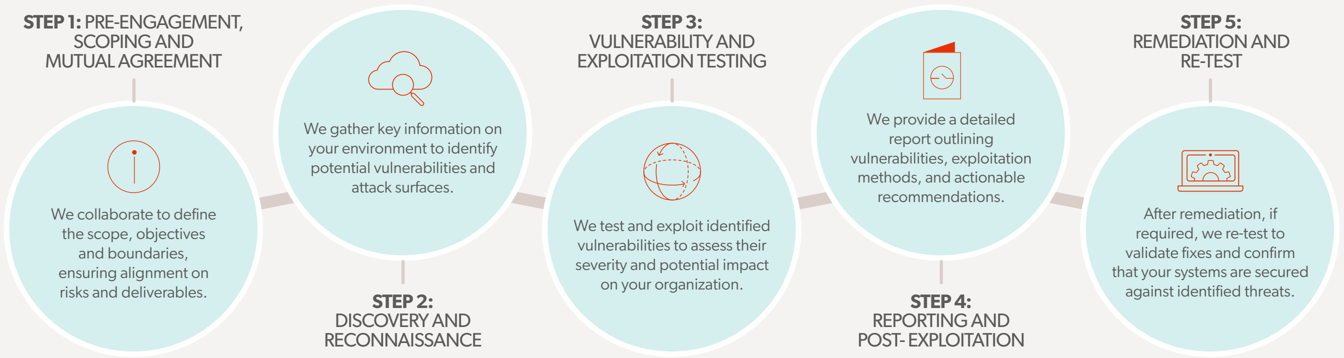
CRITICAL CAPABILITIES

Expert-led Engagements: Our seasoned professionals bring extensive experience to every engagement, ensuring thorough assessments and insights based on real-world adversary tactics.

Zero Trust Methodology: Our testing approach is rooted in the core pillars of Zero Trust. Our testing approach is designed to evaluate access controls, device validation, network segmentation, and breach detection to align with modern security best practices.

Comprehensive Attack Simulation: We emulate sophisticated, real-world attacks across your networks, applications, IoT devices, and human factors to provide a holistic view of your security posture.

Detailed Recommendations: Our penetration tests deliver actionable recommendations and prioritized risk remediation steps aligned with Zero Trust principles, thereby hardening your defenses against evolving threats.



STEP 1: PRE-ENGAGEMENT, SCOPING AND MUTUAL AGREEMENT

We collaborate to define the scope, objectives and boundaries, ensuring alignment on risks and deliverables.

STEP 2: DISCOVERY AND RECONNAISSANCE

We gather key information on your environment to identify potential vulnerabilities and attack surfaces.

STEP 3: VULNERABILITY AND EXPLOITATION TESTING

We test and exploit identified vulnerabilities to assess their severity and potential impact on your organization.

STEP 4: REPORTING AND POST- EXPLOITATION

We provide a detailed report outlining vulnerabilities, exploitation methods, and actionable recommendations.

STEP 5: REMEDIATION AND RE-TEST

After remediation, if required, we re-test to validate fixes and confirm that your systems are secured against identified threats.

Appgate's 5-step penetration testing process involves defining objectives, gathering intelligence, assessing vulnerabilities, delivering detailed findings, and validating remediation to ensure a secure environment.

Enhancing Your Zero Trust Journey

Appgate's Penetration Testing Services help organizations transition to a modern Zero Trust architecture by offering actionable insights that align with Zero Trust principles. Our services bring greater security throughout your IT infrastructure, guiding you as you move to a more advanced, segmented security model. Whether you're beginning your Zero Trust journey or looking to enhance existing defenses, our tailored engagements provide the expertise and strategic recommendations needed to identify vulnerabilities, mitigate risks, and strengthen your security posture.

Conclusion

Appgate's Penetration Testing Service is a proactive step toward strengthening your organization's defenses. By leveraging Zero Trust principles and real-world attack simulations, we provide a clear, actionable roadmap to strengthen your security posture. Our approach ensures that you not only identify vulnerabilities but also gain the strategic advantage needed to mitigate them effectively, safeguarding your business-critical assets and securely supporting your organization's growth.

About Appgate

Appgate secures and protects an organization's most valuable assets and applications. Appgate is the market leader in Zero Trust Network Access (ZTNA) and online fraud protection. Appgate products include Appgate SDP for Universal ZTNA and 360 Fraud Protection. Appgate services include threat advisory analysis and ZTNA implementation. Appgate safeguards enterprises and government agencies worldwide. Learn more at appgate.com.

appgate