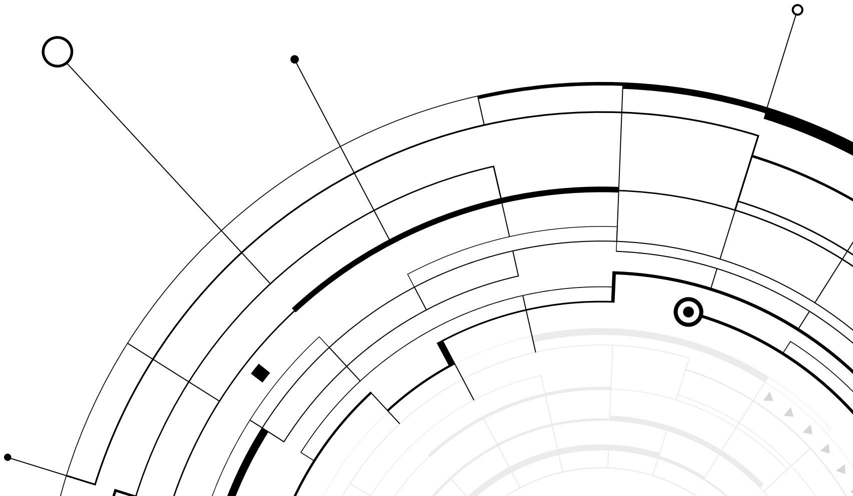
VONAHI SECURITY

WHITE PAPER

10 Ways SMBs Can Benefit From Automated Network Penetration Testing

Table of Contents

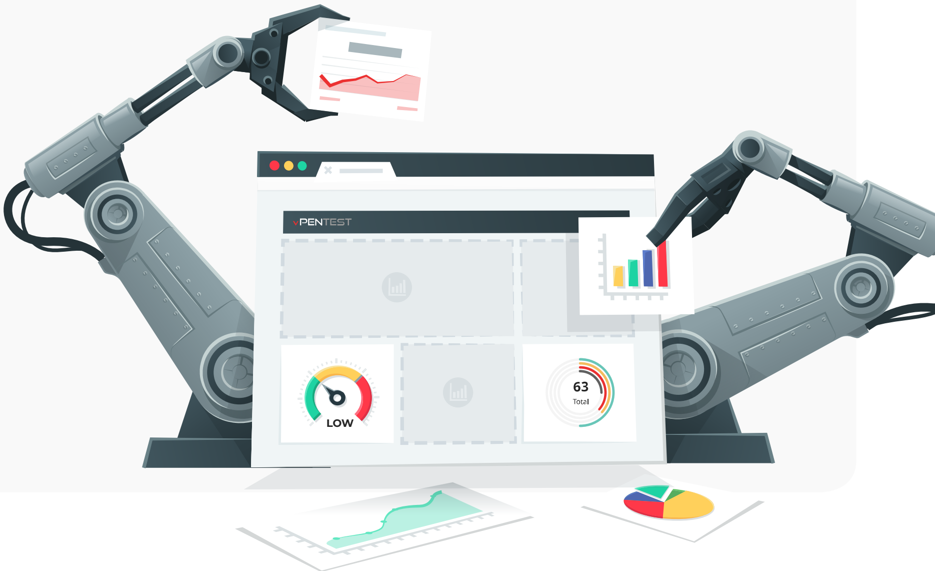


OVERVIEW

When a cyberattack makes the news, it's usually because the target was a major corporation or a (local) government. Yet growing cyber threats also put small and mid-market firms at risk of business disruption, data loss and more. Last year, **47% of reported data breaches involved small to mid-sized businesses (SMBs)**, so say what you will about cybercrime, but it does not discriminate.[1]

However, in comparison with larger organizations, SMBs usually have very few resources to draw on in order to protect themselves against cyber threats and to help them recover if they experience a security breach. In line with this, a 2021 survey found that **25% of SMBs suffering a data breach** in the previous 12 months ended up filing for bankruptcy and 10% actually went out of business.[2]

Fortunately, smaller companies can benefit immensely from the rise of automation in cybersecurity, which provides them with a range of new opportunities to improve their security posture. This white paper outlines 10 major benefits of automated penetration testing (also known as pentesting) platforms such as Vonahi Security's **vPenTest**.



0x01

OVERCOME BUDGET LIMITATIONS

While cybercrime doesn't discriminate, the same cannot be said about security vendors. Sure, many of them offer basic products like consumer-grade antivirus for free, but more sophisticated security products are often tailored to large enterprises and come with hefty price tags. Moreover, the cost of security solutions is trending upwards, further reducing the amount of companies that can actually afford them. However, recent advances in cybersecurity are increasingly disrupting this pattern by driving down the costs of advanced solutions, thereby making them available to smaller companies with limited budgets.

OVERCOME BUDGET LIMITATIONS WITH AUTOMATED PENETRATION TESTING

Small firms can now take advantage of pentesting platforms like vPenTest that are significantly more affordable than traditional assessments. As a result, it has become far easier for your small business to add a much needed offensive dimension to your cybersecurity efforts. Moreover, if your SMB currently relies on manual assessments, you can save money by switching to automated pentesting. You could invest these savings in strengthening other aspects of your security strategy, such as mitigating the issues uncovered by vPenTest.

TL;DR

Automated penetration testing platforms like Vonahi Security's vPenTest provide more value at a lower cost compared to traditional assessments and make pentesting accessible to SMBs that couldn't afford it before.

0x02

OVERCOME STAFFING LIMITATIONS

When it comes to cybersecurity, SMBs are not just at a disadvantage compared to bigger firms because they have less money to spend on advanced solutions. According to a recent industry study, the biggest challenge preventing small companies from optimizing their security strategy is actually a lack of qualified staff, which affects a whopping 77% of SMBs.[3] Automation can help smaller organizations overcome this issue by reducing the number of qualified security experts needed to improve the company's cybersecurity posture.

OVERCOME STAFFING LIMITATIONS WITH AUTOMATED PENETRATION TESTING

By making it possible to carry out a full penetration test with the click of a button, vPenTest provides you with the ability to take advantage of the knowledge and skills of seasoned penetration testers without having to create a position for this or hire external consultants.

TL;DR

vPenTest lets you carry out a penetration test with the click of a button, so you can take advantage of the expertise of seasoned pentesters without hiring one.

0x03

STREAMLINE CYBERSECURITY

A robust cybersecurity strategy involves lots of moving parts, and keeping track of these through manual processes alone is often not just inefficient, but downright infeasible given the limited resources available to most SMBs. Automation, if properly implemented, can greatly simplify the security efforts of small and mid-market companies.

STREAMLINE CYBERSECURITY WITH AUTOMATED PENETRATION TESTING

One major source of frustration for companies relying on traditional penetration testing is the time and effort it takes to get from the decision to perform an assessment, to receiving the final report. In the first stage of this process, the firm needs to find a reputable security vendor and schedule a penetration test. Companies usually need to plan assessments weeks or even months in advance due to a combination of busy consultant schedules and the need to assess the expertise of consultants and ensure the quality of the deliverables. Next, the organization must provide the consultant with the right network access and, in the case of a local engagement, a physical workspace. Once the test has been completed, the company may need to wait several weeks more to receive the final report. vPenTest solves many of these challenges by letting you control when assessments are launched and how frequently this happens. Moreover, because the report is generated during the assessment, you receive it as soon as the test completes.

TL;DR

Instead of planning assessments months in advance and then waiting weeks more for the final report of a traditional pentest, vPenTest lets you carry out assessments whenever you want, and provides you with the final report upon completion.

0x04

CONTINUOUS SECURITY

According to a recent study[4], a staggering 76% of US SMBs suffered a cyberattack last year, and 69% experienced a data breach. Most SMBs realize that things are likely to get even worse this year since the cyber threat landscape is constantly evolving, with campaigns getting more targeted, increasingly sophisticated and more severe in terms of their impact on compromised organizations. In order to address mounting cyber threats, organizations of all sizes need to be able to monitor their cybersecurity posture on an ongoing basis, so they can address issues as soon as they come up. This is where automation can play a crucial role.

IMPLEMENT CONTINUOUS SECURITY WITH AUTOMATED PENETRATION TESTING

Since traditional penetration testing requires significant resources, mostly in terms of time and money, organizations usually conduct only one or a few assessments per year. Moreover, the number of human testing hours allocated per penetration test is often kept to a minimum, with two in three SMBs allowing less than 8 hours per assessment.[5] As a result, penetration testers are unlikely to uncover all or even most serious gaps in security during a single engagement. Moreover, problems that arise outside of the testing window may persist until the next assessment, which could be months or even a year away. In this sense vPenTest is a game-changer, because it enables you to perform penetration tests on an ongoing basis. With your environment being continuously scanned and probed, you can keep track of your organization's risk profile in near real-time, allowing you to promptly address issues and check the effectiveness of those mitigations.

TL;DR

With vPenTest you can perform penetration tests on an ongoing basis. Continuous pentesting allows you to monitor your organization's risk profile in near real-time, and therefore to promptly address issues and check the effectiveness of those mitigations.

0x05

OVERCOME PATCH FATIGUE

Since 2017, over 22,000 new software and hardware vulnerabilities have been disclosed every year, leaving organizations of all sizes struggling to keep their systems updated.[6] SMBs often need over a month to install critical patches affecting operating systems (35%) and third-party software (58%), putting them at risk of cyberattacks exploiting brand new vulnerabilities.[7] Further complicating matters is the fact that many threat campaigns exploit vulnerabilities with relatively low CVSS scores that companies are less likely to prioritize.[8] In order to address these issues, SMBs should try to automate their patch management strategy as much as possible.

OVERCOME PATCH FATIGUE WITH AUTOMATED PENETRATION TESTING

vPenTest can supercharge your patch management strategy by detecting, exploiting and thereby revealing known vulnerabilities in your environment that should be prioritized for patching. This is especially beneficial if you use vPenTest to carry out security assessments on an ongoing basis.

TL;DR

vPenTest can supercharge your patch management strategy by revealing known flaws in your environment that should be prioritized for patching.

0x06

IMPROVE PASSWORD MANAGEMENT

Recent research reveals that four out of five data breaches are the result of threat actors exploiting weak and/or stolen passwords.[9] Many SMBs are vulnerable to password-based attacks because they have not implemented a proper password management strategy. For instance, only 41% of small and mid-market firms enforce periodic password changes, just 38% prevent password reuse on internal systems and a mere 29% require a minimum password length.[10] To make things worse, few companies regularly check if employee email accounts have been compromised in a data breach. Here, automation can make a tremendous difference as well.

IMPROVE PASSWORD MANAGEMENT WITH AUTOMATED PENETRATION TESTING

Automated penetration testing can enhance your password management strategy in different ways. During an assessment, vPenTest uses various techniques to obtain password hashes and then attempts to reuse these across the network. The password hashes are also sent to a cracking server capable of revealing weak and default passwords. In addition, vPenTest checks company websites for the presence of email addresses, which it tests against a database of accounts that were previously compromised in a data breach. You can use all of this information to adjust your password policy where necessary in order to prevent employees from using weak or compromised credentials. Again, you will benefit the most if you are performing regular or continuous assessments with vPenTest.

TL;DR

vPenTest can take advantage of weak or compromised credentials on your network, thereby revealing shortcomings in your password management strategy that you can use to improve it.

0x07

OPTIMIZE CONFIGURATION MANAGEMENT

Patching operating systems, devices and applications against known vulnerabilities is not the same as securing them, since services may still create holes in an organization's cyber defenses if they are not properly set up. Threat actors are well aware of this, and actively probe targeted networks for misconfigurations that may hand them the keys to the kingdom. This strategy is often effective because many companies struggle with configuration management, at least in part because the rise of web apps and cloud computing continues to add to the complexity of IT ecosystems. It is no coincidence that far more records were exposed in data breaches last year as the result of misconfigured services than due to hacks or fraud.[11] SMBs can fight this trend by using automation to boost their configuration management efforts.

OPTIMIZE CONFIGURATION MANAGEMENT WITH AUTOMATED PENETRATION TESTING

vPenTest is capable of detecting and exploiting insecure configurations in a great variety of services. This information allows you to address misconfigurations in your environment. If you take advantage of continuous penetration testing, this approach becomes especially effective, since the security benefits and potential drawbacks of different configurations can be tested on an ongoing basis, allowing you to detect and address new issues in a timely manner.

TL;DR

vPenTest can expose insecurely configured services in your environment, allowing you to make adjustments where necessary to strengthen your firm's security posture.

0x08

ENHANCE NETWORK SEGMENTATION

Another security issue that threat actors love to exploit, is the failure of companies to divide up their network into smaller, separate elements, or subnets that are configured with firewalls to prevent unauthorized communication between network segments. The absence of such segmentation makes it very easy for threat actors to comb the entire network in search of valuable data after gaining a foothold. By contrast, a properly segmented network doesn't allow users to move between systems without proper authentication. This may prevent threat actors from accessing valuable data even if they manage to gain access to one system, and will at the very least slow down lateral movement.

ENHANCE NETWORK SEGMENTATION WITH AUTOMATED PENETRATION TESTING

During an assessment, vPenTest attempts to execute various techniques for moving laterally across the internal network. Therefore, you can use the results of automated assessments to verify the effectiveness of network segmentation in your environment. With continuous penetration testing, you can monitor the impact of changes to the network in near real-time by connecting or disconnecting systems in between assessments.

TL;DR

vPenTest will try to exploit shortcomings in network segmentation, providing you with the opportunity to address these issues in a timely manner.

0x09

ASSESS YOUR THREAT DETECTION CAPABILITIES

In order to optimize their cybersecurity strategy, SMBs must regularly assess the performance of their security solutions so they can fine-tune configuration settings or replace flawed solutions altogether. While this may seem obvious, companies often put their faith in security solutions without properly testing if these actually perform as expected. This can be the result of resource limitations, naivety, or something else. Whatever the reason, this approach is likely to invoke a false sense of security since sophisticated cyber threats cannot be easily detected or blocked, not even by advanced solutions. In fact, last year the vast majority of SMBs was targeted with exploits and/or malware that evaded their anti-virus (82%) and intrusion detection system (69%).[12]

ASSESS YOUR THREAT DETECTION CAPABILITIES WITH AUTOMATED PENETRATION TESTING

By simulating a real-world cyberattack, vPenTest lets you review the effectiveness of different security solutions including anti-virus, intrusion detection systems, firewalls and even log management software when it comes to detecting and blocking malicious activity on your network. As with various other benefits discussed above, most value can be obtained if you perform penetration tests on a continuous or regular basis.

TL;DR

By simulating a real-world cyberattack, vPenTest lets you assess to what extent various security solutions enable you to detect and block malicious activity on your network.

0x10

ACHIEVE COMPLIANCE WITH EASE

In response to rising cybersecurity challenges, both governmental and private bodies are increasing their regulatory efforts in this domain. At the time of writing, most SMBs already have to deal with regulations such as GDPR and CCPA, and the number of compliance standards that apply to the average small firm is bound to increase in the coming years.

ACHIEVE COMPLIANCE WITH AUTOMATED PENETRATION TESTING

Automated pentesting makes it dead simple to maintain compliance under standards requiring your company to carry out security assessments on a yearly or more frequent basis. Moreover, vPenTest can enable your organization to improve the implementation of various specific compliance requirements, such as the PCI DSS requirement for isolating your cardholder data environment (CDE) from the rest of your network through network segmentation.[13]

TL;DR

vPenTest makes it easy to meet compliance standards demanding regular security testing as well as more specific requirements.

REFERENCES

[1] Verizon (2019). Source (pdf):
https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf

[2] National Cyber Security Alliance (2019). Source:
https://staysafeonline.org/small-business-target-survey-data/

[3 / 10 / 12] Keeper Security & Ponemon Institute - 2019. Source:
https://start.keeper.io/2019-ponemon-report

[4] Ibid.

[5] Synack - 2020. Source:
https://go.synack.com/2020-compliance-report.html

[6] Risk Based Security - 2020. Source (pdf):
https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20Year%20End%20Vulnerability%20QuickView%20Report.pdf

[7] Kaseya - 2019. Source:
https://www.kaseya.com/resource/2019-it-operations-survey-report/

[8] RiskSense - 2019. Source:
https://risksense.com/press_release/risksense-spotlight-report-exposes-top-vulnerabilities-used-in-enterprise-ransomware-attacks/

[9] World Economic Forum - 2020. Source:
https://www.weforum.org/press/2020/01/forgotten-your-password-not-having-one-will-make-you-safer-says-world-economic-forum

[13] Risk Based Security – 2020 (ii). Source:
https://pages.riskbasedsecurity.com/2019-year-end-data-breach-quickview-report

ABOUT US

Vonahi Security is a cybersecurity company that developed vPenTest, a SaaS platform that automates network penetration testing, a valuable service that mimics the way a hacker would target an organization to obtain confidential information. This market is currently serviced by outsourced consultants providing manual testing. The high cost makes penetration testing primarily a once a year test that leaves major gaps in security.

Through automation, our platform delivers continuous testing at a fraction of the cost of an outsourced consultant. We eliminate inefficiencies, increase the scope, free up budget for other cybersecurity initiatives, and ultimately make the organization more secure.

www.vonahi.io

Visit it our website to learn more about our services, schedule a demo, or request a quote.

HELLO WORLD. MEET MODERN SECURITY.

VONAHI
SECURITY

www.vonahi.io

info@vonahi.io

1. 844.VONASEC (866-2732)

@vonahisec