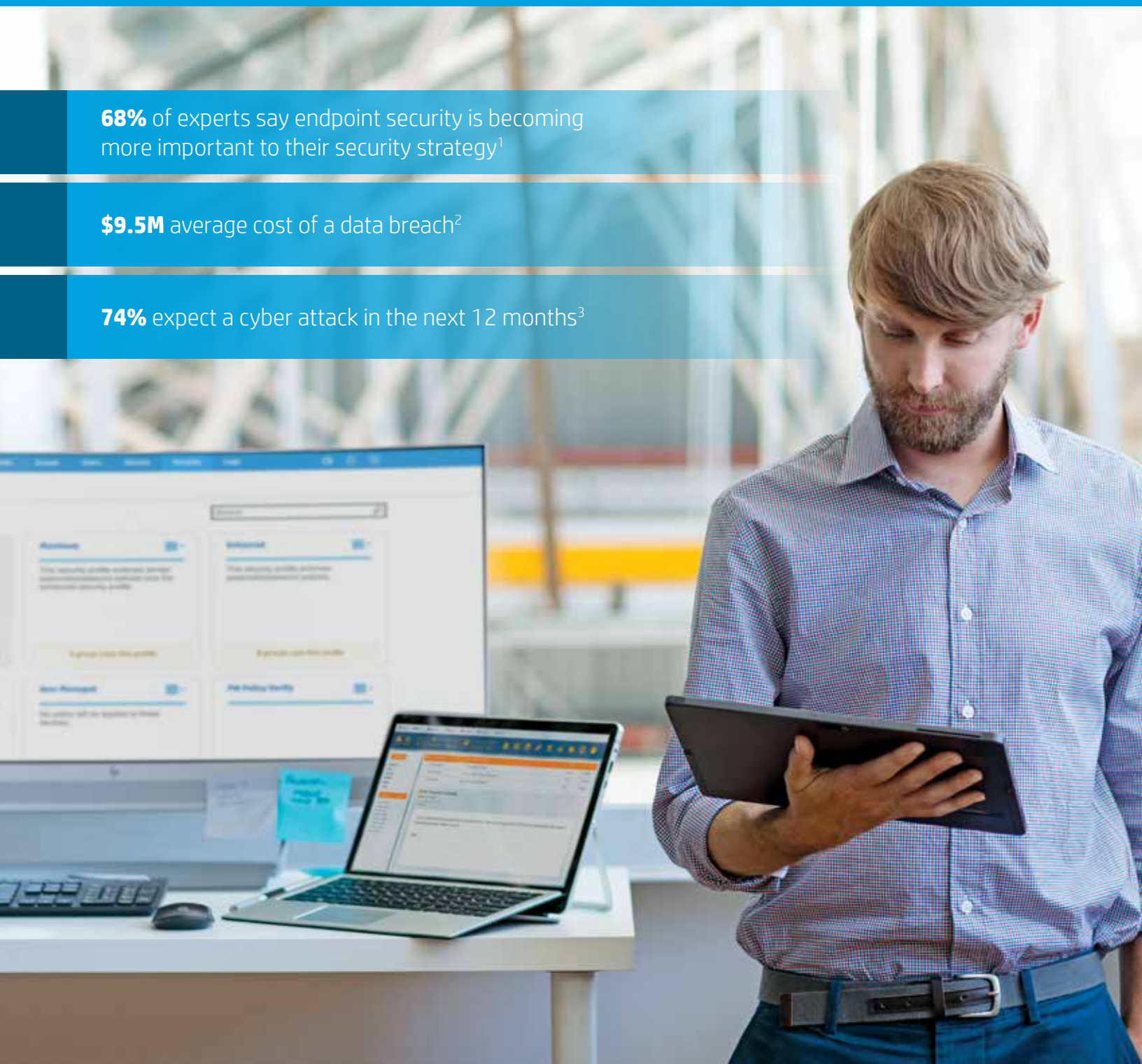
Defend your personal systems with HP Security Advisory Services

68% of experts say endpoint security is becoming more important to their security strategy[1]

$9.5M average cost of a data breach[2]

74% expect a cyber attack in the next 12 months[3]



Attacks targeting notebooks and desktops have increased by 200%.[4]

In today's complex business security climate, it's more important than ever to stop problems before they begin.

HP Security Advisory Services can help, with complete, tailored, end-to-end consultation and assessments for your multi-brand/multi-OS personal devices.

HP knows security

Get a personalized assessment and plan of action from an HP team that includes experts with up to 25 years of relevant, hands-on experience servicing and supporting highly manageable PC security architectures from the ground up.

Here to help before you have an issue

Free up your constrained IT security resources for other tasks and rely on experts who complement and enhance them, proactively identify gaps in your endpoint security profile, and recommend risk-reducing procedures to address vulnerabilities.

Designed for your company-owned and personal devices

HP works with any device—whether it's an Apple product, or a PC, tablet, or smartphone running Windows or Android—to close security gaps with services that focus on securing multi-OS and multi-device environments.

Are your devices safe?

Your endpoint devices—including all brands of PCs, tablets, and smartphones—are emerging as the predominant security risk. HP experience and trusted security specialists can help protect all your devices through security audits, vulnerability scans, penetration tests, and the identification of infrastructure gaps. With our services complementing your IT staff, you can focus on other activities.

HP is your one-stop shop for security advisory services for all PC devices.

We will work with all brands, including Apple products, Lenovo, Dell, and Samsung, to build the most secure endpoint devices with our unparalleled security expertise.

HP's expert security consultants, proactive risk reduction, and lifecycle service approach help ensure your devices and your brand are protected.

PC audit

The same security domains that exist within print devices also exist within personal systems, and our audit teams follow the same criteria in their approach, assessing the level of security in each domain:

Device protection

Data protection

Document protection

Monitoring/managing

The current processes and methodologies performed by the HP Print Security Team can be replicated in an advisory offering, targeting personal systems in a corporate environment.

Pre-assessment

Our security experts carefully review the current environment and gain an understanding of goals and objectives.

Assessment

We then conduct a qualitative and quantitative analysis of the environment, in which we interview key stakeholders regarding security best practices, and scan personal system configurations against industry recommended standards.

Post-assessment

We report and present our findings in a way our customer will understand.

Vulnerability scans

Malicious agents, intent on compromising an organization's sensitive information, will look for computing systems with:

- Outdated software versions
- Missing patches
- Misconfigurations
- Deviations from best security practices

These systems are soft targets for attackers, and usually the first attack vector targeted by advanced persistent threats and hackers.

Implementing vulnerability scans as part of a vulnerability management lifecycle:

- Checks compliance with host application usage and security policies
- Provides information on targets for penetration testing
- Offers insight on how to mitigate discovered vulnerabilities
- Demonstrates the effectiveness of an organization's patch process
- Quantifies an organization's exposure to surface vulnerabilities

HP helps stop costly data breaches before they happen. Our security experts follow crucial steps in the vulnerability scan process to make sure no weak spots are overlooked.

Pre-assessment

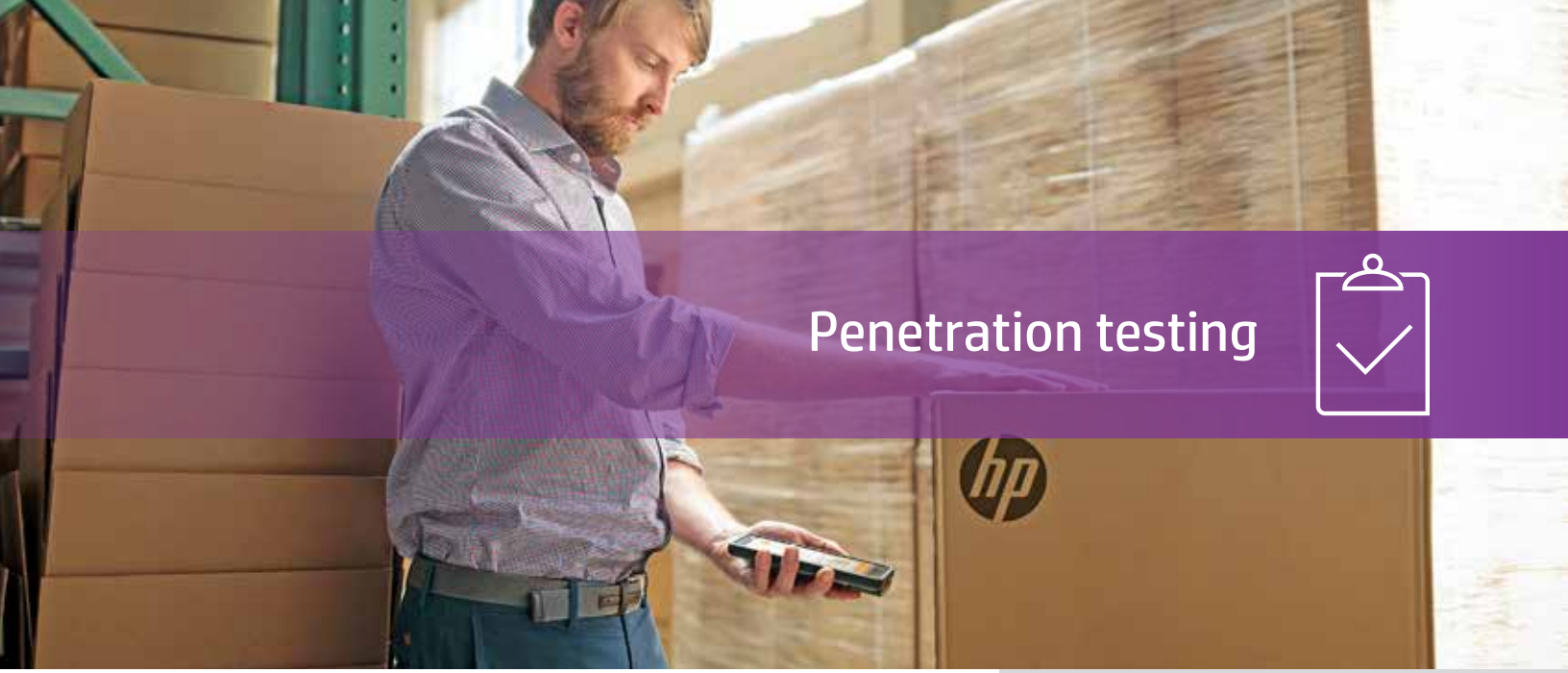
First, we scope systems and networks, identify system considerations and issues, and test logistics.

Assessment

We conduct regular internal and external scans for vulnerabilities, potential targets, and security risks.

Post-assessment

We conduct a high-level review of system vulnerabilities, analyze technical details of the results collected, and ultimately propose mitigation suggestions to the customer.



Penetration testing

An integral part of a security compliance program is to understand the threat vectors that exist within an organization. Many regulations require organizations to identify and mitigate these threat vectors as part of an information security management lifecycle. This may call for penetration testing, a critical component of an effective security compliance program governed by regulatory requirements.

We employ highly skilled penetration test consultants who have been trained to perform assessments using the latest testing tools, methodologies, and frameworks within the Information Security community. Our three-phase approach ensures each step of penetration testing follows industry-standard methodologies with regard to compliance and best practices.

Pre-assessment

We scope systems and networks, identify any system considerations or issues, and test logistics

Assessment

We conduct internal and external testing of systems and devices by way of intelligence gathering, threat modeling, vulnerability analysis, and exploitation.

Post-assessment

We deliver preliminary and final reports in a timely fashion.

Security architecture review

We are committed to ensuring an organization's security architecture is meeting or beating "best security practices." Our process of security architecture review and assessment is designed to:

Analyze threats and risks facing an organization

Provide recommendations to remediate identified risks

Provide a snapshot of an organization's current security posture

Pre-assessment

We assess security scope, drivers, and logistics.

Assessment

We analyze security documents, measures, managerial processes, and adherence, as well as conducting interviews with key stakeholders.

Post-assessment

We provide recommendations for improvements to reduce threats and mitigate related risks.

Get peace of mind for your endpoint devices with industry-leading HP security capabilities

Trained and certified experts

Trust a team that has multiple industry-recognized certifications related to penetration testing, auditing, system security and network security, and advanced degrees in Computer Science, Computer Engineering, and Information Technology.

Comprehensive and consolidated end of engagement reporting

Receive a detailed report of findings and recommendations for each security audit, vulnerability scan, and penetration test, delivered as a formal presentation to discuss how you can proactively address security risks and potential breaches.

Brand and OS-agnostic

Regardless of your brand or operating system, your HP team can leverage its endpoint device security expertise to jointly and simultaneously assess and advise you on your print and personal systems security.

1. Ponemon Institute, 2015 State of the Endpoint Report: User-Centric Risk, 2015. 2. Ponemon Institute, sponsored by HP, "2016 Cost of Cyber Crime Study & the Risk of Business Innovation," 2016. 3. Ponemon Institute, Annual Global IT Security Benchmark Tracking Study, March 2015. 4. Verizon, 2016 Data Breach Investigations Report, 2016. Approved and quoted by Gabriel Bassett, Senior Information Security Data Scientist, Verizon Data Breach Investigations Report. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

4AA7-1349ENW, September 2017, Rev. 1