Change your security posture from reactive to proactive.

Penetration Testing

verizon✓

You know you're at risk from evolving cyber threats, but exactly how much? Our security risk assessment and compliance services can help you identify vulnerabilities and reduce your exposure. Get an objective view of your ability to assess and respond to today's cyber threats. Our Penetration testing can help you move from reactive to proactive in securing your organization.

Penetration testing is an important part of managing risk as cyber threats continue to evolve. It helps you put resources where they're needed most and can be so effective that many compliance programs now require it.

Not all penetration tests are created equal. Some don't mimic what a real-world attacker would do when trying to steal corporate secrets or sensitive data. To find the potential gaps in your security, you need a trusted advisor who has the global visibility and experience with current threat actors and their tactics to help you assess risk and strengthen your security posture.

Reducing risks starts by knowing them first.

How it works.

Penetration Testing uses vulnerability scanning tools to probe your environment for gaps and measure the severity of the risk your network is facing. Our custom assessment of your environment can help you better define and manage your risk so you can respond to and avoid potential attacks. Most importantly, our assessments come with the guidance to prioritize the higher risk issues we've found and develop a solution that works best for your budget.

Each test begins with a project kick-off and planning meeting with your project manager, who will be your central point of contact.

Next, our security experts will use real-world scenarios to try to access sensitive data and compromise your systems.

Finally, we'll provide you with a report that includes a summary of what we've found, the severity and impact of our findings and our recommendation for solutions that best fit your needs.

Our Penetration Testing is focused on the three major categories that affect most businesses:

Network

Wireless

Web App

We offer both fixed or custom pricing options giving you flexibility to structure your plan to your needs. A representative will assist you with the price structure that works best for you.

Fixed-Price Service Packages

Pricing is available in four levels:

m	S	M	L
Mini	Small	Medium	Large

Penetration Testing service packages come in four levels, depending on the complexity of your operations. We offer fixed-price penetration testing to include networks, wireless (802.11) and web applications.

Network Penetration Testing

Network Penetration Testing attempts to discover and identify vulnerabilities and exploit those in an effort to determine to what extent a bad actor could compromise the target network.

The initial approach to this 'gray box' testing is overt, attempting to identify low to critical risk vulnerabilities and then exploiting vulnerabilities that could be used by an attacker to gain access into the environment.

Once the initial security gap has been discovered and exploited then additional testing would be performed, such as privilege escalation, situational awareness, pivoting and lateral movements, to ultimately attempt to gain additional access or credentials to data repositories.

Network Penetration Testing is offered in different fixed-price service plans, depending on your business needs, including the number of active IP addresses and unauthenticated applications.

Wireless Penetration Testing

Wireless Penetration Testing covers all aspects of wireless (802.11) security such as validating the actual physical perimeter of your wireless network, verifying the proper use of encryption and authentication, searching for rogue access points, and assessing how the client accesses the wireless infrastructure.

We will also review client-side security by validating how wireless clients are configured and secured against connection to rogue access points or hijackings over their wireless interface. Fixed-pricing service plans are based on the number of SSID's and number of floors in your building served by your WiFi network.

Web App Penetration Testing

Web App Penetration Testing is an assessment to identify weaknesses in the application layer controls. This testing helps identify security weaknesses in the application logic, authentication mechanisms, session management, input validation and other application layer components. The fixed price service plans are dependent on the number of dynamic pages and the number of user roles.

Why Verizon?

The better your security partner, the more useful your penetration test. We've investigated many of the largest data breaches on record, and are regularly conducting incident investigations.

Our security team has collected and examined security data for more than a decade, analyzing more than 250,000 incidents and over 8,000 confirmed data breaches.

Lean on our experience and expertise to help find the gaps in your environment now to help reduce the risk of data breaches.

- A global company with 40+ dedicated experienced Penetration testers'

- Our approach, methodology and deliverables are consistent worldwide.

- Verizon has been conducting penetration testing for more than 15 years.

- All Verizon consultants are senior level, in-country, full-time Verizon employees.

- Verizon does not out-source or off-shore its Professional Security Services.

- Verizon Professional Security Services consultants hold 40+ industry and vendor certifications, including OSCP, OSCE, CISSP, GIAC , CEH, CISSP, CISA, GIAC, GSEC, ISO 270 0x Lead Auditor, ITIL, PCI-QSA, and PMP.

A Verizon account representative will help you determine the service level that fits your business needs.

Learn more:

For more information, contact your account representative or contact us:

verizonenterprise.com/support/sales

For more information about the other products and services we offer, visit:

verizonenterprise.com/products/security