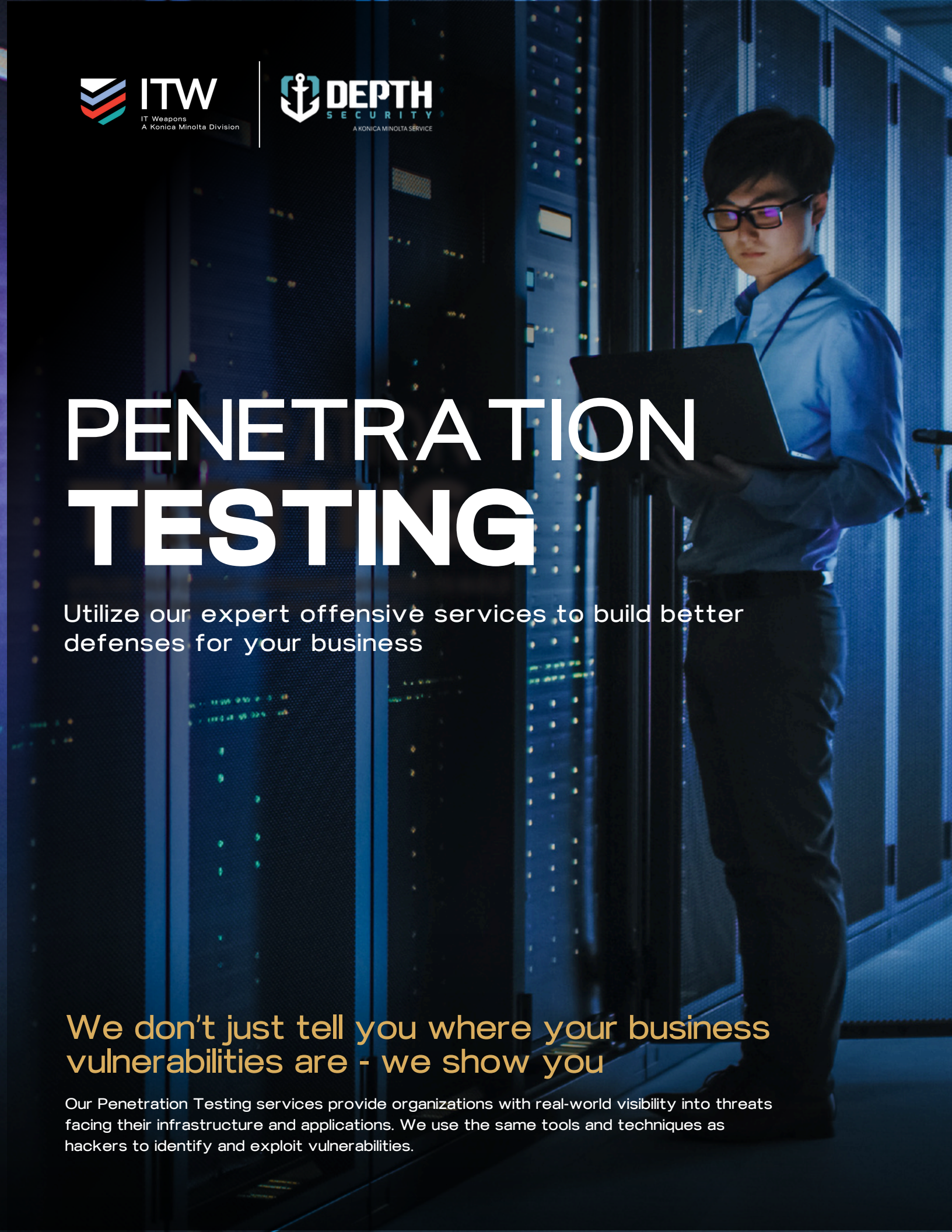


ITW
IT Weapons
A Konica Minolta Division

DEPTH SECURITY
A KONICA MINOLTA SERVICE

PENETRATION TESTING

Utilize our expert offensive services to build better defenses for your business

We don't just tell you where your business vulnerabilities are - we show you

Our Penetration Testing services provide organizations with real-world visibility into threats facing their infrastructure and applications. We use the same tools and techniques as hackers to identify and exploit vulnerabilities.

AT A GLANCE
HOW WE CAN HELP

• Identify threats/vulnerabilities that pose the highest information protection risk as it pertains to client data including but not limited to: availability, confidentiality, and integrity

•Adhere to critical component of industry framework such as the NIST Cybersecurity Framework

• Fulfil compliance requirements (PIPEDA etc.)

• Achieve peace of mind knowing attack surface has been minimized

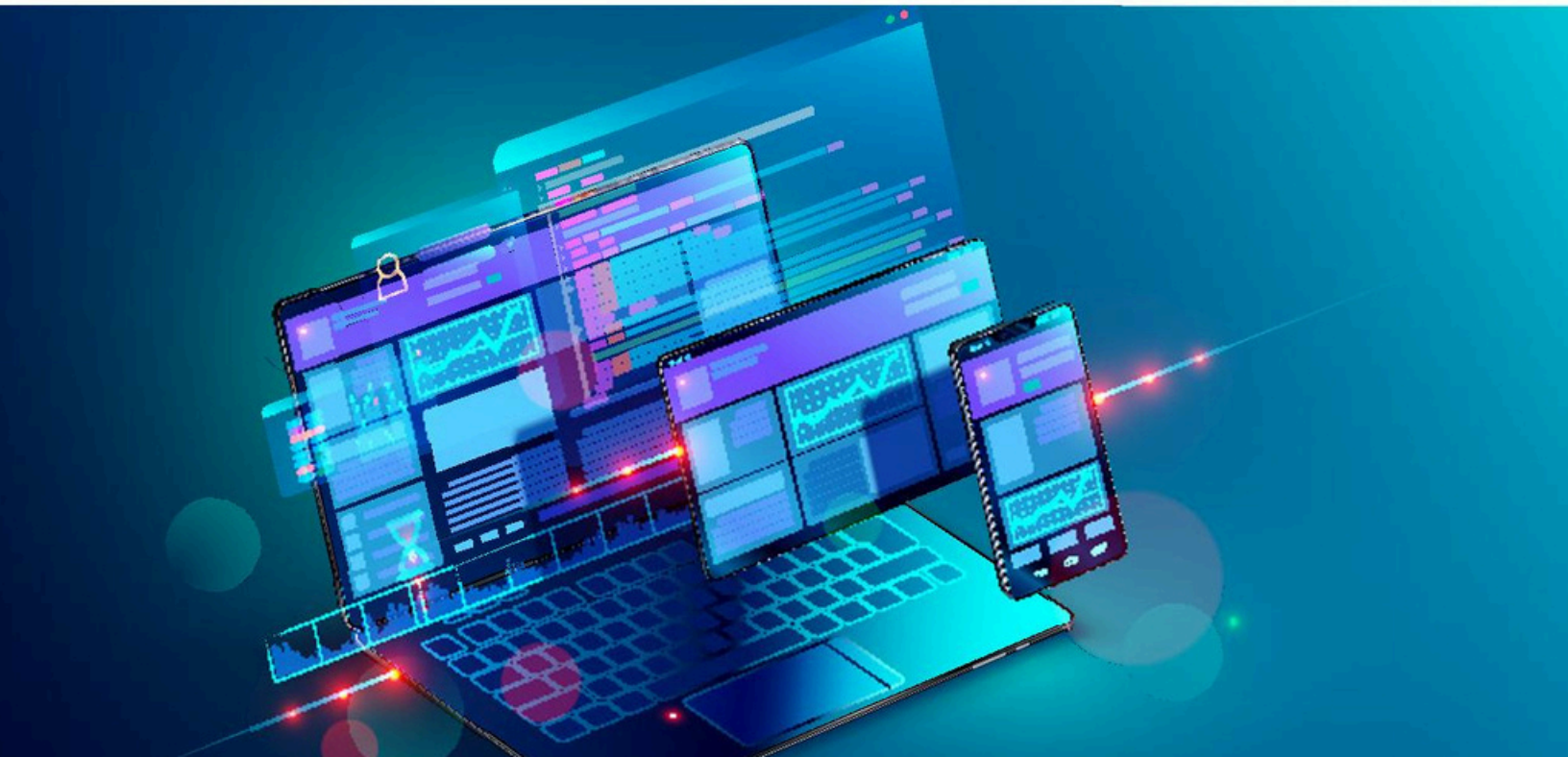
• Reduce risk of ransomware

• Receive quantitative results that help measure the risk associated with your critical assets

• Find vulnerabilities that traditional control-based testing methodologies often miss

• Uncover critical and exploitable vulnerabilities in your existing technology, people and processes

• Measure the current level of security to help plan future improvements



APPLICATION PENETRATION TESTING

Web applications are the most vulnerable areas within an organization's environment. A vulnerable application puts data at risk and allows attackers to pivot and attack your entire internal enterprise. The convenience of access provided to customers, employees, and partners can also serve as the same to potential attackers. Weaknesses within the design, development, and deployment of applications can be exploited to gain unauthorized access to confidential data from anywhere. Our application security assessment service helps organizations identify weaknesses within their applications. Our testing methodology emulates the methods used by an attacker utilizing both automated and manual testing.

• WEB: Our web application penetration testing services test your applications from both public (not logged in) and authenticated (logged in) perspectives. If your app uses multiple permission roles, we'll test inter-role authorization to ensure privilege escalation isn't possible. For multi-tenant apps, we ensure unintended cross-tenant access is prevented.

• API / WEB SERVICES: Don't make the mistake of thinking your B2B web service is not a target just because it has no user interface. If it speaks HTTP and connects to a database, it better be secure. Our API / Web Services penetration testing identifies flaws within these interfaces and verifies that they are being used as intended.

NETWORK PENETRATION TESTING

• EXTERNAL DISCOVERY: It is difficult to defend yourself without knowing your complete attack surface. But more than ever, security leadership and staff are placed in that exact position. Our Perimeter Discovery service gives you a solid view of your external-facing systems and data. Our experts go beyond simple DNS and IP enumeration to find what you don't know is out there.

• EXTERNAL NETWORK: Performed from an internet-based attacker's perspective, we simulate real-world attacks on your organization by focusing on internet-exposed assets and users.

• INTERNAL NETWORK: Performed from the inside of your organization's network, this engagement simulates an attack by an agent with internal access to your network such as a rogue employee or contractor.

• WIRELESS: Performed from the perspective of an attacker who is within wireless range. We evaluate the wireless network's security posture in the context of generally accepted network security "best practices."

• TRUSTED ACCESS: Performed from the perspective of an authorized entity with some level of access to your environment. Common scenarios include testing with the same level of access as partners and vendors connected to your organization's network through remote access technologies such as VPN, SSLVPN, Citrix, etc.

SECURITY REVIEWS

• PASSWORD AUDIT: While the world moves away from passwords as a sole means of credentials, password strength is still critical. Despite multi-factor authentication's ability to lessen the risk associated with weak passwords, its internal deployment remains challenging, and password security is still crucial. Our Password Audit service intentionally cracks user passwords to analyze their strength, offering actionable advice on enhancing your password environment.

• VULNERABILITY ASSESSMENT: Vulnerability assessments find system loopholes that are vulnerable to attack. During the assessment, testers use both manual and automated scans to noninvasively search through systems and applications. As a result, these systems and applications cannot be damaged by the scan. When the assessment is complete, a report shows all the vulnerabilities the assessment uncovered, categorized by severity.

• NETWORK INFRASTRUCTURE AND SECURITY HEALTH CHECKUP: A thorough examination of your network's overall health, assessing everything from performance to security risks. The goal is to identify vulnerabilities that could leave your system open to cyber threats. Performing this checkup regularly adds an extra layer of security by making your system as impenetrable as possible.

Start a conversation with one of our information security experts

Get in touch!

DEPTH SECURITY
A KONICA MINOLTA SERVICE

ITW
IT Weapons
A Konica Minolta Division