

CORE Impact for Endpoint and End-User Testing

Put Endpoint and End-User Security to the Test

CORE Impact Pro makes it easy to proactively assess endpoint security and measure end-user susceptibility to phishing, spear phishing and other social engineering threats. Each test is backed by comprehensive reports that assist with compliance initiatives and pinpoint ways to both harden endpoint systems and improve security awareness in your organization.

Safely Assess End-User Awareness of Social Engineering Threats

With Impact, you can test email-user security awareness by replicating realistic phishing and spear phishing attacks – with or without attempting to exploit the endpoint system.

- Identify publicly available email addresses from your organization, such as those on websites, in online documents, and in PGP and Whois databases
- Assess security awareness by identifying users who click links in phishing emails
- Leverage sample phishing templates, or create custom spear phishing emails
- Set web forms phishing traps to flag data leakage risks
- Test end-user machines for exploitable vulnerabilities and pivot to other network systems

Test Endpoint Security Prior to Deployment

Impact Pro can automatically run all client-side exploits against standard desktop images prior to deployment in your live network environment. This enables you to identify and validate vulnerabilities in endpoint operating systems, services and applications – without the need to challenge end users through social engineering.

Leverage Commercial-Grade Client-Side Exploits

Impact Pro's extensive library of client-side exploits cover threats that target:

- Endpoint applications: e.g., web browsers, email clients, instant messaging, media players, business applications and productivity tools
- Endpoint security solutions: e.g., antivirus, anti-phishing, anti-malware, host-based intrusion detection and prevention systems
- Endpoint operating systems and services: e.g., Windows, Mac, Linux

Created in-house at Core Security by a professional team of experts, the product's client-side exploits are Commercial-Grade – ensuring that they are current, effective and safe for your network. Automated capabilities allow you to test an endpoint system against multiple client-side exploits with a single click, adding efficiency and speed to security assessments.

Assess the Consequences of Successful Social Engineering

- View the local file system and mapped drives
- Upload and download files to and from the end-user system
- Open and interact with files on the compromised system
- Gather user names and passwords from endpoint applications
- Take a screenshot of current activity on end-user's desktop
- Harvest email addresses from mail clients
- Deploy a keylogger that tracks the user's keystrokes
- Perform a password dump from the user's web browser
- Automatically "listen" for clicks, launch exploits, and collect evidence of successful compromises

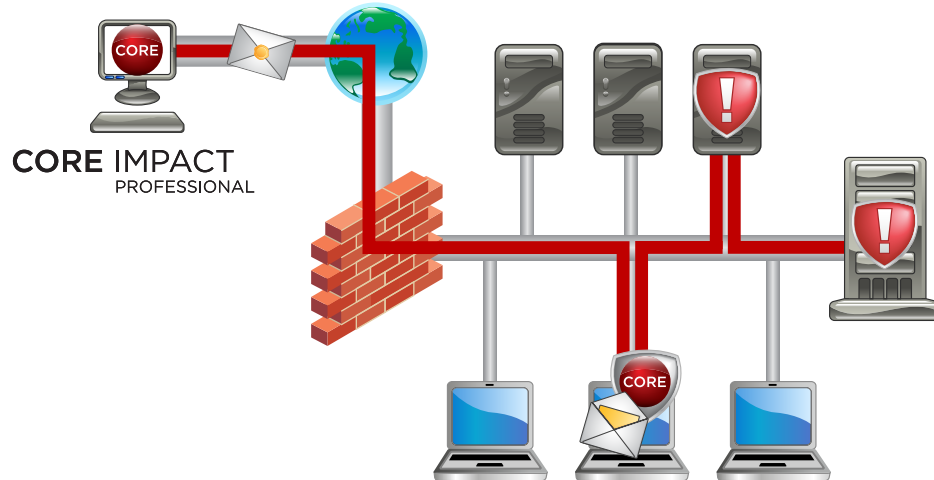
Determine the Risks of Insider Access

Impact also includes network penetration testing capabilities, that can leverage any compromised endpoint as a beachhead from which to launch subsequent tests on other systems in the end user's network – without uploading any code to the machine. This pivoting capability enables you to exploit trusted relationships and fully understand the “ripple effect” of threats that can occur when a single end-user system is compromised, replicating the steps attackers actually follow in the wild.

CORE Impact Pro enables you to replicate multistaged attacks that leverage compromised systems to target backend resources, revealing how chains of exploitable vulnerabilities can open paths to mission-critical systems and data.

You gain actionable data regarding:

- where critical exposures exist
- what systems and data are at risk
- what steps are necessary for remediation



Demonstrate the Progress of Vulnerability Management and Security Awareness Programs

CORE Impact Pro reports enable you to benchmark endpoint security, end-user awareness and incident response programs, while demonstrating ongoing security program improvements to executive management, auditors and compliance officers.

- Client-Side Penetration Test Report: a full audit trail of each test, including the email template sent (when applicable), exploits launched, vulnerabilities identified and validated, and details about compromised systems
- User Report: a report of which links were clicked, when they were clicked, and by whom

In addition, Impact Pro offers a variety of other ways to document your security assessments, including visual attack path reports, delta reports, and PCI and FISMA compliance reports.

Next Steps

CORE Impact Pro allows you to proactively test the security of network systems, web applications, endpoint systems, email users, mobile devices and wireless networks. Learn more by contacting us today to schedule a demonstration.

Core Security