ZERO-TRUST WEB PROTECTION

SOLUTION BRIEF

Zero-Trust Secure Browser

1 Zero-Trust Web Browsing

Six Billion More than 6 billion URLs and domains exist on the Internet.

50K domains In average 50,000 new web sites are registered everyday.

DefensX gives you total control of filtering the web. and block the known phishing and malware sources.

Block High and Medium Risk Web Sites

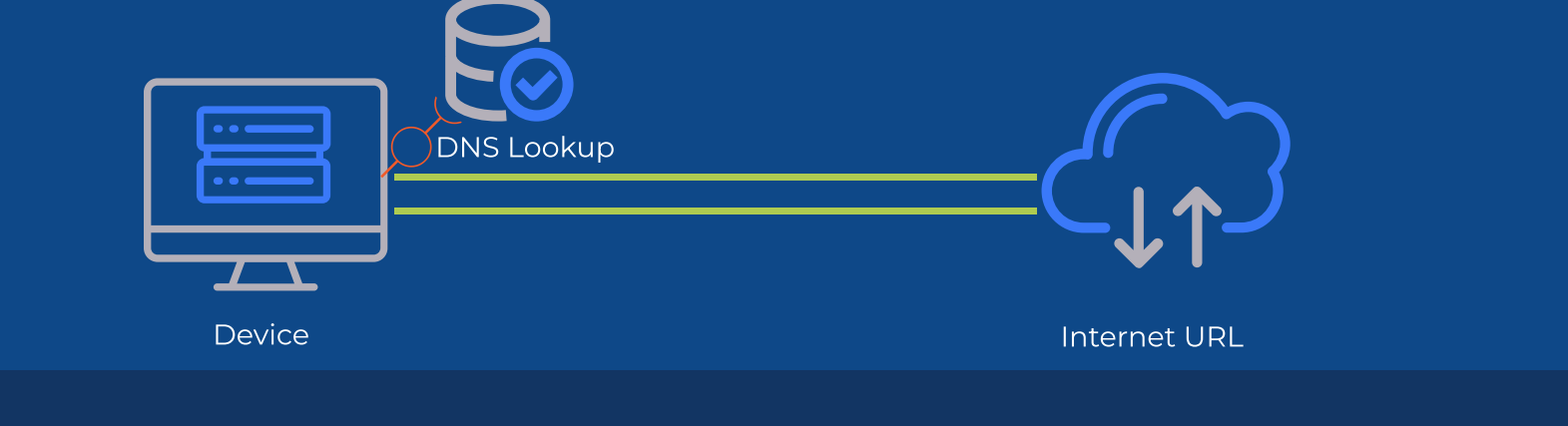
Read-only Access to Uncategorized Web Sites

Allow Access to Known Low Risk Web Sites

Block or Allow access based on the URL Category such as *Block Gambling* or *Block Adult Content.*

2 DNS Protection

DNS filtering does not provide sufficient protection for the web, but it perfectly fits the applications accessing SaaS resources. DefensX gives you the option to add DNS protection on top of the Web Filtering within the same suite for the same cost.



It is possible to enable DNS layer policies based on Web Filter rules and apply them on the endpoint with a single click.

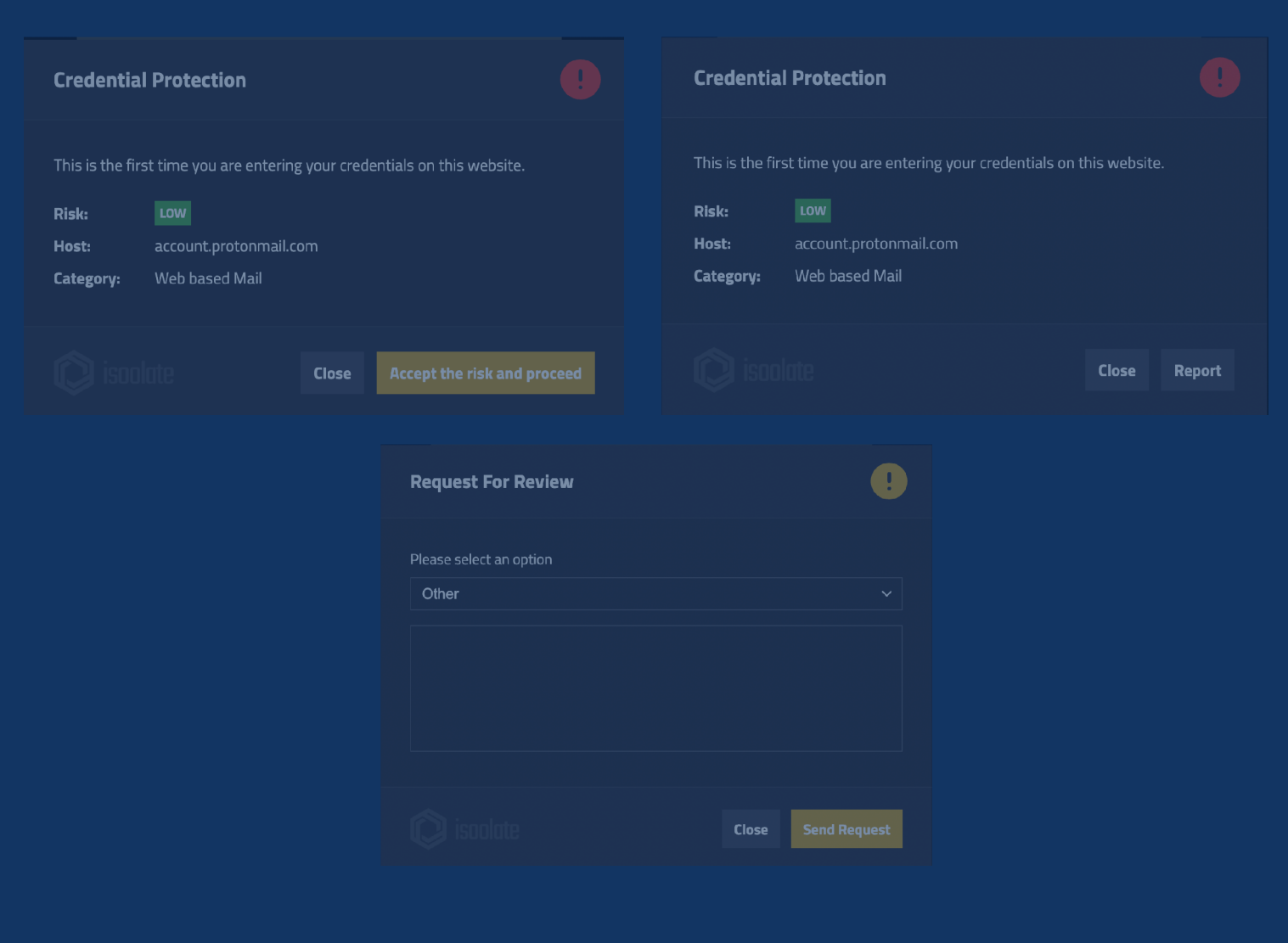
3 Zero-Trust Credentials

DNS or Web filtering can block known phishing and scam web sources based on the domain threat intelligence. But the modern nature of Javascript and HTML5 gives enhanced tools for the attackers.

61 percent 61% of the breaches involve credentials.

85 percent 85% of the breaches benefit from human error.

Because of widely adopted social engineering tricks and targeted digital marketing, anti-phishing solutions also fall short of protection from breaches. MFA protection is breached so easily with reverse-proxy attacks. DefensX provides the last millimeter protection for spear-phishing, reverse-proxy, and advanced credential attacks.

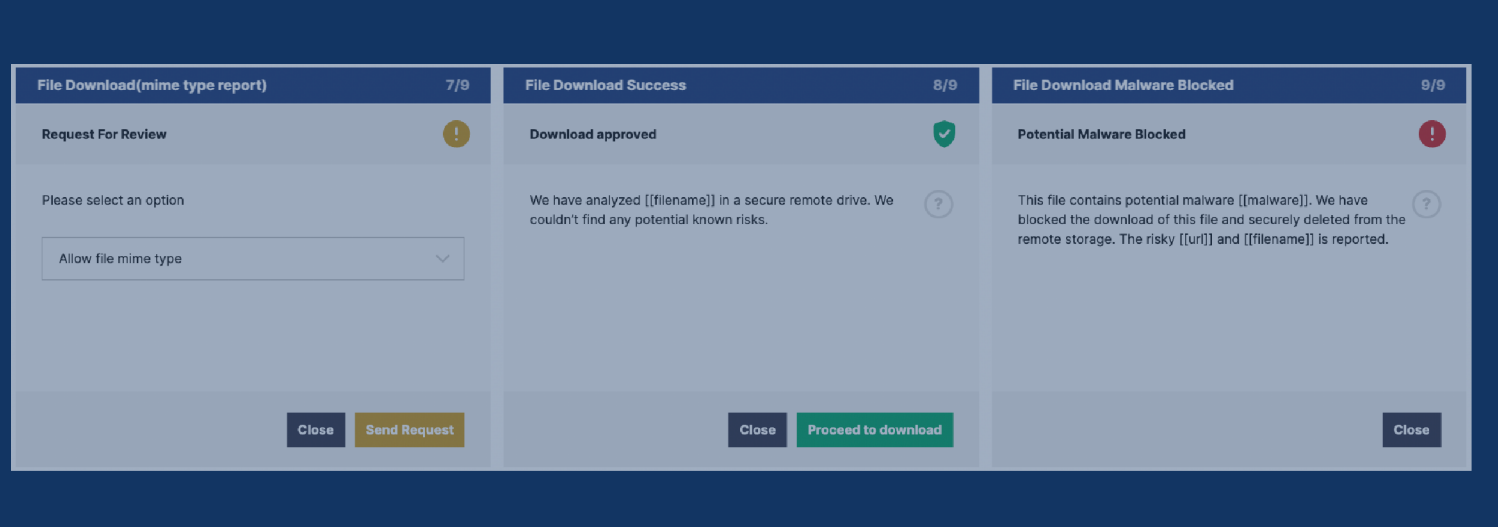


4 Zero-Trust File Protection

Drive-by-downloads are the main reason for the malware and ransomware injections because attackers improve their methods constantly. Using Javascript and Web assembly, they can deploy files invisible on the network.

Did you know **32%** of malware is zero-day

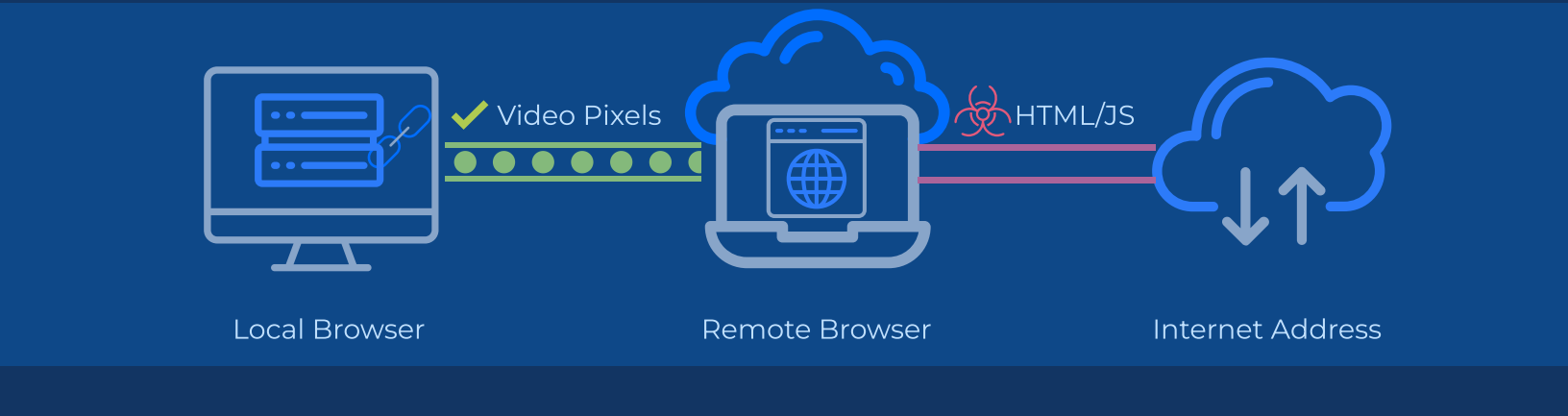
24 in 100 MALWARE attacks are invisible from the network layer.



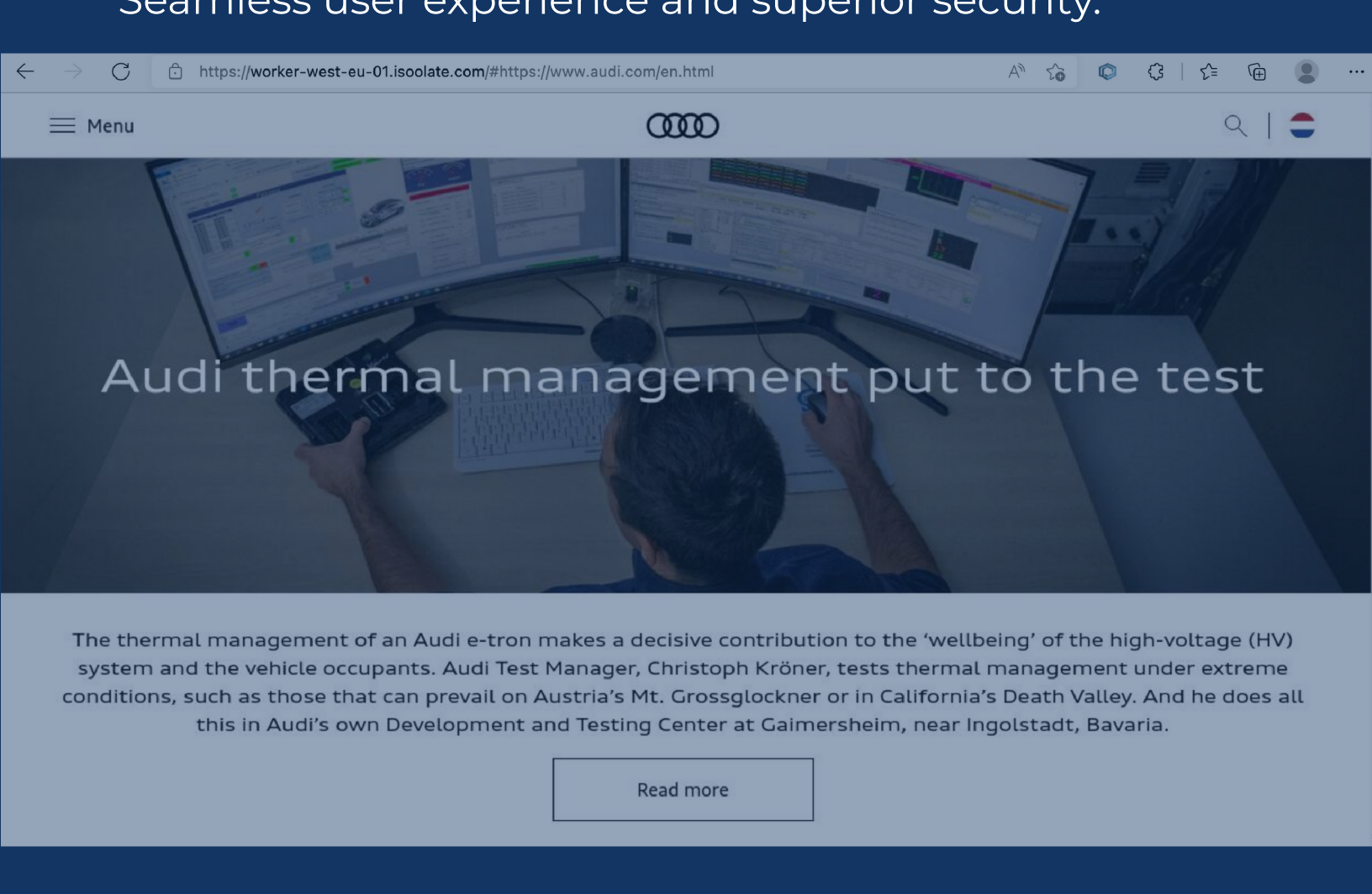
DefensX in-context protections override the web browsers' trust factor to the web and end-users. It embeds extra layers of security controls in every session and implements zero-trust web browsing.

5 Remote Browser Isolation

For the most advanced protection for the web, you need to use a remote browser in the cloud. It is like flying a drone remotely. Native web browsers will receive only the video of the remote web browser.



Seamless user experience and superior security.

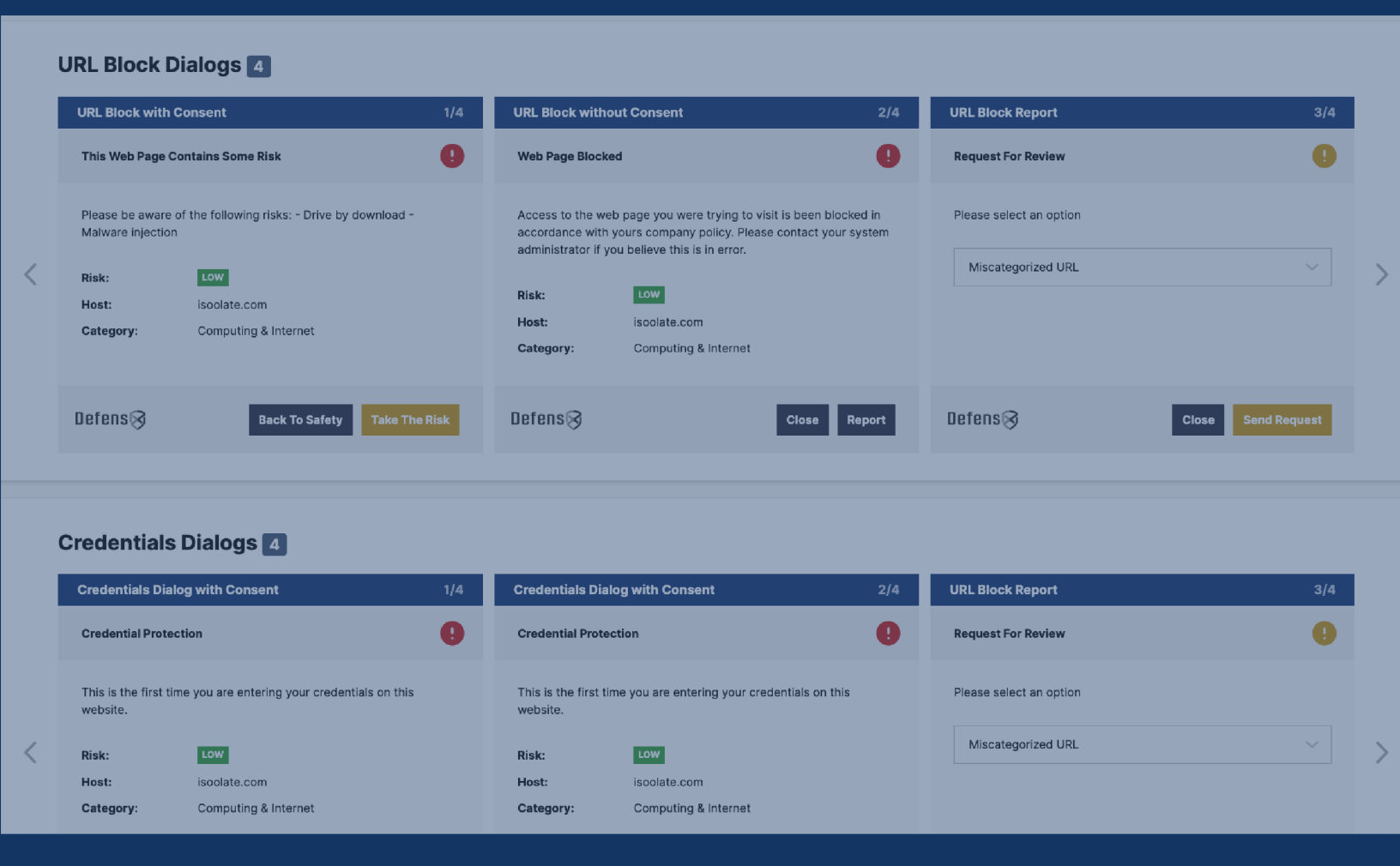


Uncategorized or unknown web pages can be viewed in remote browser isolation with a single click configuration.

6 Cyber Vigilance Training

End users are the weakest chain in the link. They are the first attack target for social engineering and credentials theft. Continuous cybersecurity training is highly recommended to create a solid cybersecurity posture.

80% 80% of organisations said that security awareness training had reduced their staffs' susceptibility to phishing attacks



MSPs can create their own custom training modules or use predefined configurations.

End Point Protection Framework

There are four essential components for endpoint protection. Where firewall and anti-virus are old technologies, EDR and endpoint web protection are novel protections. MSPs can offer lower-cost protection bundles to their clients by combining the below options.

Firewall
Microsoft Defender is a zero cost option for SMB's.

Antivirus
Microsoft Defender is a zero cost option for SMB's.

EDR
Microsoft Defender, SentinelOne are two solid alternatives for SMBs

Web Protection
DefensX zero-trust web browser and DNS Protection

info@defensX.com

v142201