Defens

Classic Vs. Core

Going Beyond DNS Protection to Create a Secure Digital Workspace

Table of Contents

03 Introduction

04 The Problem

05 Going beyond DNS Protection

06 Classic Vs. Core

07 All About Core

08 The Impact

09 The Stack

10 The MSP Deployment Experience

11 Acknowledgments

Introduction

In today's world - everything we do revolves around the browser. As the workforce moves beyond the bounds of traditional offices and with critical business applications and data racing to the cloud, the browser remains at the heart of the modern workspace.

However, advanced web threats and constantly evolving security and compliance standards have outpaced legacy security solutions, leaving the modern workspace vulnerable to web-based cyber and identity attacks or forced to implement a solution that disrupts the natural workflow and requires changes to end-user behavior.

DefensX is rewriting the rules for MSPs and organizations globally by turning your go-to browser into a secure digital workspace paired with complete DNS protection for legacy operating systems.

Gone are the days of the DNS Ceiling.

Welcome to the new era of DefensX Core.

The Problem

Security vs. Agility

Over the past 20 years, technology has advanced at an extraordinary pace and has transformed the way we live. From work to school and everything in between, technology—especially web browsers—has become central to our daily interactions and lifestyles.

However, with these advancements come new challenges that are evolving even faster: **cyber threats and identity attacks.**

- **Cyber crime statistics globally consider the browser to be the primary avenue for attacking end users.**
- **IBM reported in 2023 that phishing attacks cost businesses an average of $4.9 million per attack.**
- **70% of organizations have users actively being served malware ads on their browser at any given moment**
- **93% of organizations had two or more identity-related breaches in the past year.**
- **85% of breaches involve a human element**

It's obvious that security is vital, especially when it comes to the modern workspace, but at what cost?
There is no shortage of solutions that promise to keep you and your data secure. However, they force you to compromise on agility, productivity and behavior - everything that the browser was designed to bolster.

"By 2030, enterprise browsers or extensions will be the core platform for delivering workforce productivity and security software on managed and unmanaged devices for a seamless hybrid work experience."

Gartner®

Going Beyond DNS Protection

Why would we want to move to Core when Classic has been working just fine. Is DNS Protection not enough?

..... Let's Break it Down

Is DNS Protection Alone Not Enough?

DNS security was originally invented to protect against traditional attacks like the blocking of malicious or forbidden websites or applications at the DNS level.

However, attack methods have changed in frequency and advancement with modern day identity and credential theft attacks leading the way. In fact, there has been a 95% increase in attacks in 2024 since 2023 with credential theft making up 90% of those attacks (MGM Grand, TicketMaster).

This has resulted in traditional standalone DNS giving a false sense of security while not having enough threat intelligence to properly protect the users from the most frequent type of attacks we see on the daily.

Do I still need DNS Protection?

DNS security remains a vital component of any comprehensive security strategy, which is why we include it as part of our core secure browser platform, ***complimentary***.

However, traditional DNS protection was designed to filter web content and defend against known risks—it cannot guard against modern day and Zero-Day attacks. This leaves enterprises blind to what is really happening beneath the surface. With DefensX, enterprises gain complete protection against both traditional and modern threats, including identity theft, credential theft, malicious advertisements, and data loss risks often linked to popular AI platforms.

Best of all, DefensX delivers this advanced protection without requiring any changes to user behavior, browsers, or devices. The result? Seamless policy adherence, satisfied users, and uninterrupted efficiency, productivity, and cost-effectiveness.

So, why DefensX Core?

Classic vs. Core

With credential and Identity theft being responsible for 90% of attacks, DefensX Core ensures that organizations are protected at every single layer while maintaining DNS protection for legacy operating systems

CLASSIC
DNS FILTERING

- Secure DNS Filter
- Roaming Agent
- Kernel Driver
- Bookmark Manager

CORE
CREDENTIAL AND IDENTITY THEFT PROTECTION

- Advanced Secure DNS
- Secure Web Browser
- Password, Credential and Idendity Protection
- Company Resilience Reporting and Dashboard
- 30-day Log Retention
- RMM / PSA Support

Plus everything in Classic

All About Core

Easy as 1, 2, 3

1

Complete Web and DNS Protection

DefensX provides the ultimate foundation for a secure digital workspace with comprehensive web and DNS protection. Organizations can categorize URLs into over 200 groups, each assigned a risk score based on policy settings. Beyond simple allow-or-block options, DefensX enables tailored responses like Remote Browser Isolation or Read-Only mode, customized for each user's needs.

2

AI-Supported Identity Theft and SaaS Access Protection

As cyber attacks and data breaches become more sophisticated, it's essential to move beyond traditional network and DNS protections and implement dynamic identity theft and SaaS Access controls. With DefensX, organizations can verify domain credibility and control user credential entry while utilizing AI image processing and AI assisted risk controls. Given that 80% of data breaches involve credentials and the average phishing attack costs businesses $4.9 million, this feature proactively blocks unauthorized logins and phishing attacks, while preventing the most sophisticated MiTM credential theft attacks.

3

AI Based Human Risk Management

At DefensX, we believe organizations should have seamless, real-time visibility into their entire enterprise's risk and security posture. Our human risk management dashboard provides automated, in-depth reports on human risk and vulnerabilities, empowering organizations worldwide to effortlessly achieve Zero Trust and cyber resilience.

> “"It was a no brainer to upgrade to DefensX CORE from Classic DNS. With just a click in the backend, we were able to immediately add identity theft protection and ad blocking for our clients for about the same price of what others are charging for just DNS. Great to work with a future proof platform."

The Impact

Engineered for MSP's Efficiency

By dynamically filtering content and files while simultaneously guarding every session, user and credential across the web, ***MSPs can boost efficiency, effortlessly scale, and exceed enterprise-level security standards—all with complete DNS protection for legacy operating systems.***

20%

DefensX reduced MSP's cost of managing their customers digital workspaces by 20%

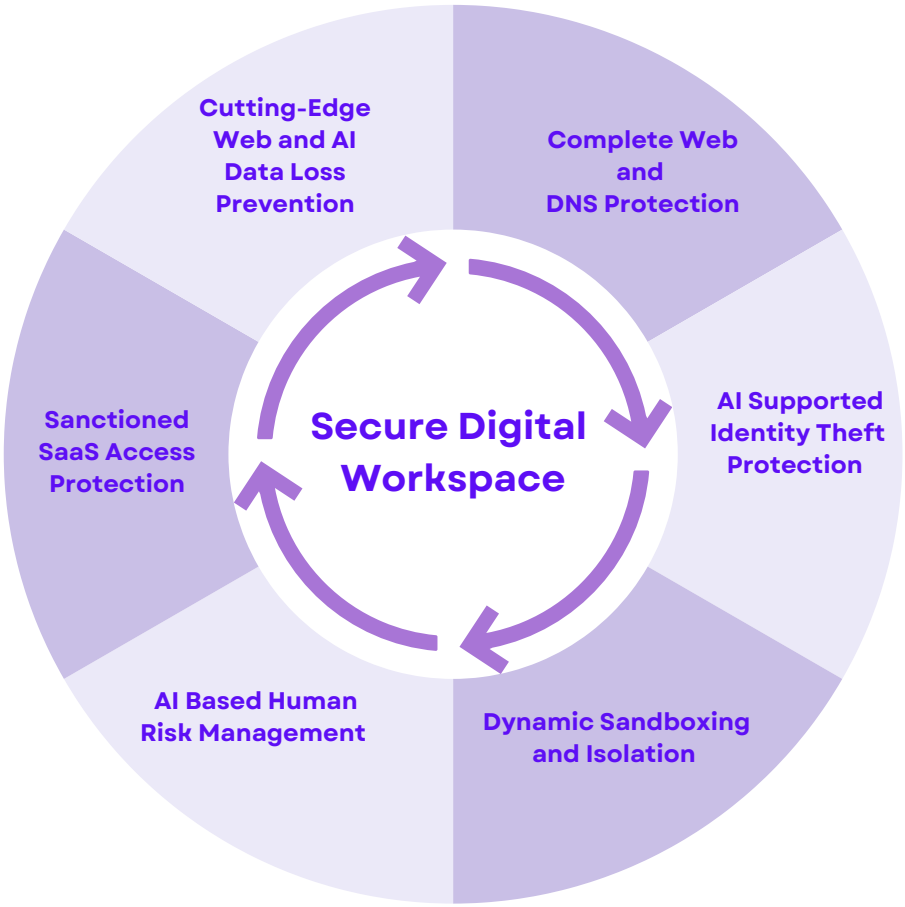
30%

MSPs using DefensX improved their average cyber resiliency by 30% in the first 6 months

40%

MSPs using DefensX improved their users password hygiene by 40% in the first 6 months

Web Browser + DefensX = The Fastest, Most Cost-Effective Solution for a Secure Digital Workspace



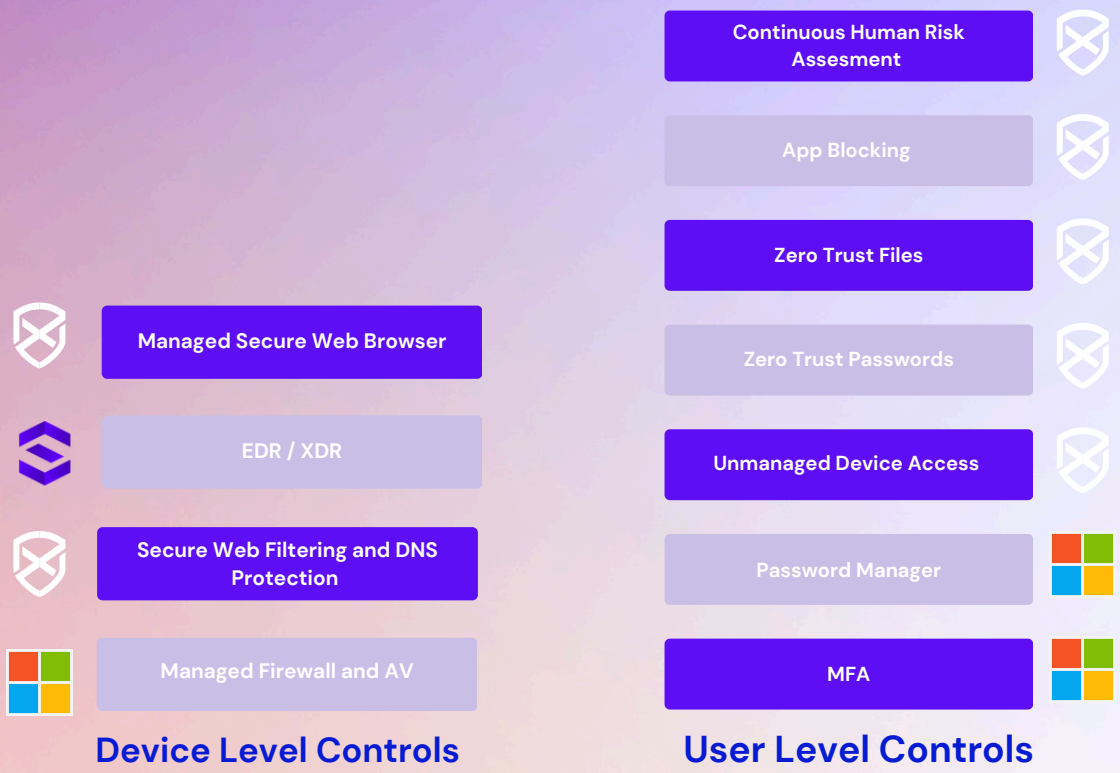
💡 *Fun Fact: MSPs can fully deploy DefensX Core in under 2 minutes*

Let’s Stack About it

There comes a time where we all have to address the elephant in the room: The Stack.

Luckily, DefensX Core makes this conversation easier for everyone involved by drastically consolidating and modernizing tools in your cybersecurity stack.

By completely addressing modern day identity and credential threats while managing legacy DNS threats in a single platform, you can live life a little lighter and focus on enhancing legacy tools such as EDR, AV and email security with modern protection for browser sessions.



The MSP Deployment Experience

DefensX Core was designed for MSPs Efficiency and Success

Onboarding and Deployment Process: At A Glance

WEB FILTER POLICY CREATION

- The web filter policy configuration process lays the foundation of your secure digital workspace.
- To start, MSPs will customize web-filtering responses based on category and assign risk scores.
- Tailored responses like Remote Browser Isolation, Read-Only, or Block will ensure seamless and secure web access for every user.

CREDENTIAL PROTECTION

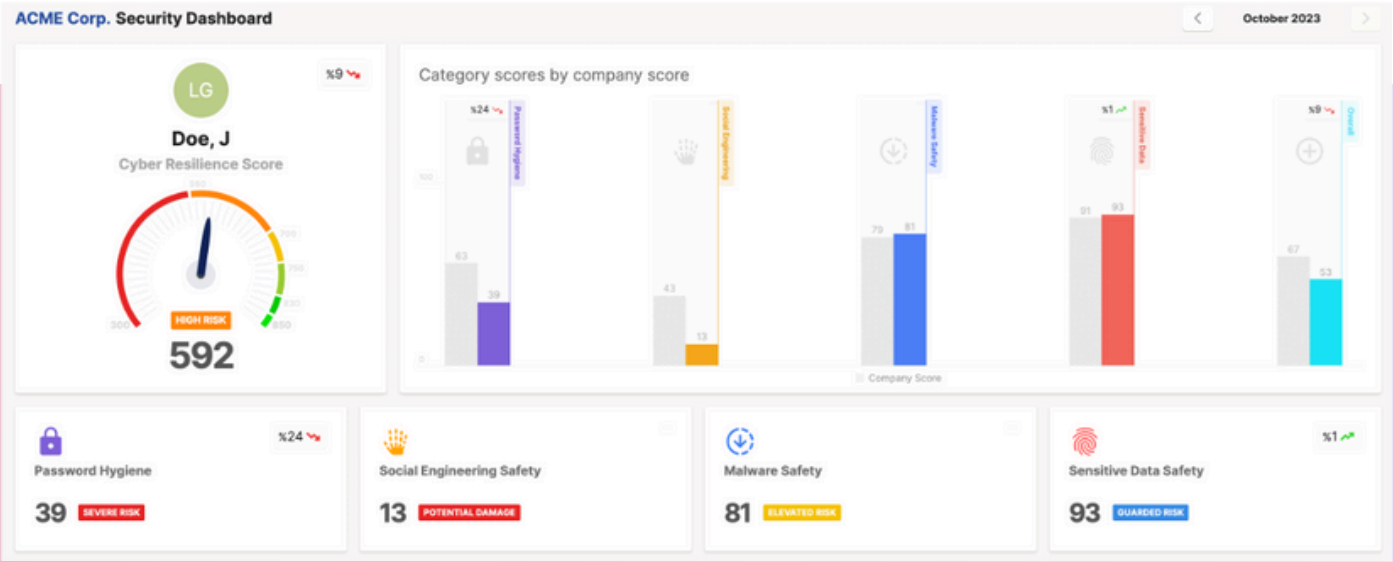
- Next, MSPs will efficiently establish credential protection policies.
- DefensX safeguards users against credential exposure by rendering risky content in Read-Only mode.
- MSPs can dynamically configure credential input policies while automatically tracking and logging all credential inputs.

AD BLOCKING

- After web filter and credential policies are set, MSPs will be able to quickly set up ad blocking policies.
- The DefensX system automatically blocks ads on websites to ensure safe browsing and the reduction of malware ad risks.

BRANDING AND USER CREATION

- Once core policies and settings are established, MSPs will be able to edit alert messaging and branding to ensure a seamless experience for end users.
- In addition to that, MSPs will be able to dynamically provision DefensX subscription tiers to each user - allowing a perfectly tailored secure browser environment for each client and end user.



Gone are the days of the DNS Ceiling.

Welcome to the New Era of DefensX Core

Acknowledgements

National University. (n.d.). Cybersecurity statistics: The growing threats in 2022 and beyond. Retrieved November 18, 2024, from https://www.nu.edu/blog/cybersecurity-statistics

Brooks, C. (2024, June 5). *Alarming cybersecurity stats: What you need to know in 2024*. Forbes. Retrieved November 18, 2024, from https://www.forbes.com/sites/chuckbrooks/2024/06/05/alarming-cybersecurity-stats-what-you-need-to-know-in-2024/

Gartner, Inc. (2023, April 14). Emerging Tech: Security — The future of enterprise browsers (ID G00782898).

Cybersecurity Ventures. "Web Browsers Are Doorways to Cyberattacks." *Cybersecurity Ventures*, https://cybersecurityventures.com/web-browsers-are-doorways-to-cyberattacks. Accessed November 19, 2024.