WHITEPAPER

The Novel Approach To Stop Breaches:

Zero Trust Web

Table of Contents

Removing the traditional trust relationship between the employees and the Internet is the essence of a modern security architecture.

Introduction

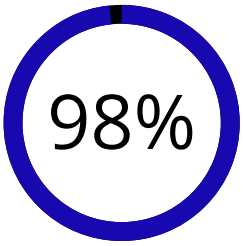
To Modern Business Owner,

Given the dramatic rise in remote working, the explosion of cyberattacks on enterprise networks, data, and applications, and the overall expansion of multi-cloud computing, Internet browsing is drastically increasing the attack surface.

In this business white paper, you will learn more about the increasingly sophisticated attacks using the browser to initiate a variety of attacks, and how cloud-native remote browser isolation eliminates risk as users see a rendering of a web page, but not the page itself, protecting against invisible downloading of malware and viruses onto their device, and into enterprise networks. This approach protects against zero-day threats and enhances an overall cybersecurity posture.

The DefensX Team

Traditional Trust is the Problem



According to Gartner, 98% of external attacks over the last few years were carried out over the public Internet. Of those attacks, 80% were targeted directly at end-users through their browsers.

Zero-trust assumes there is no traditional edge to protect.

Social Engineering

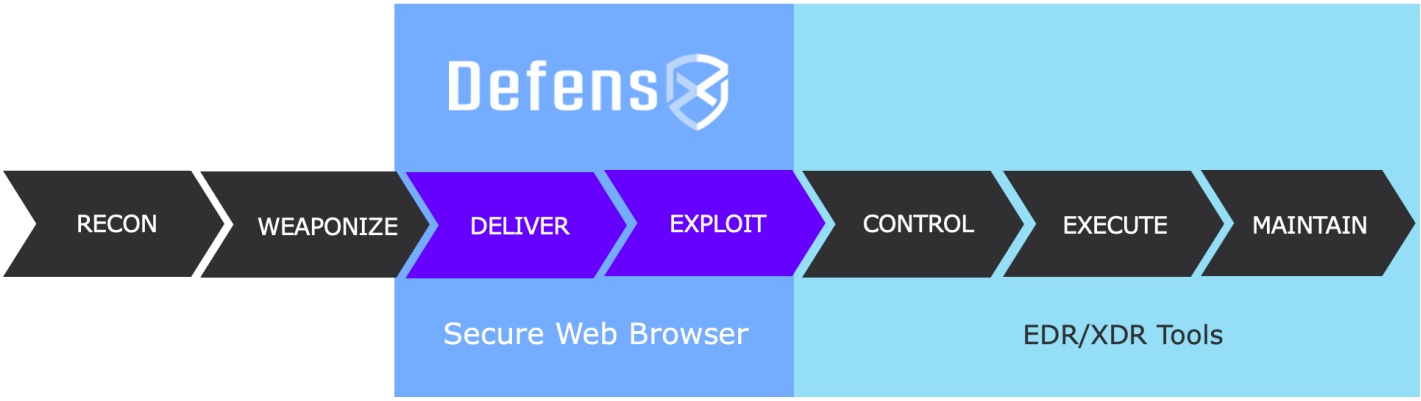
Attackers generally break into the network utilizing social engineering to deliver targeted malware to vulnerable systems and people.

Once they are in, attackers stay quiet to avoid detection, then map out the organizations' defenses from the inside, making it possible to deploy multiple parallel kill chains to ensure success.

Attackers usually target unprotected systems and capture information over an extended period. This captured information is sent back to the attack team's base to be analyzed for further exploitation, fraud, or worse.

Most malware and ransomware attacks start with the web browser and directly target Internet users when they are searching and interacting online. With increasingly sophisticated attacks, which ramped up dramatically in 2022 as millions of employees, contractors and partners were forced to work from home. Attackers easily bypass network level controls.

THE CYBER KILL CHAIN



WHAT IS APT?

ADVANCED PERSISTENT THREATS

Especially given the massive growth of remote working, employees, contractors, partners, and customers use browser-based productivity applications. Whether using Office 365, Google Drive, Slack, Zoom, or many dozens of other collaboration and communications applications, browsers remain open throughout the workday with many tabs open at the same time on desktops, laptops, tablets, and smartphones.

Whether those devices are issued by the organization, or owned by the end-user (Bring Your Own Device or BYOD model), without remote browser isolation, attackers now have the potential to breakthrough browsers as they become acquainted with the whole system.

As attackers target web browsers as the major infiltration point to deliver and exploit, you need to protect them .

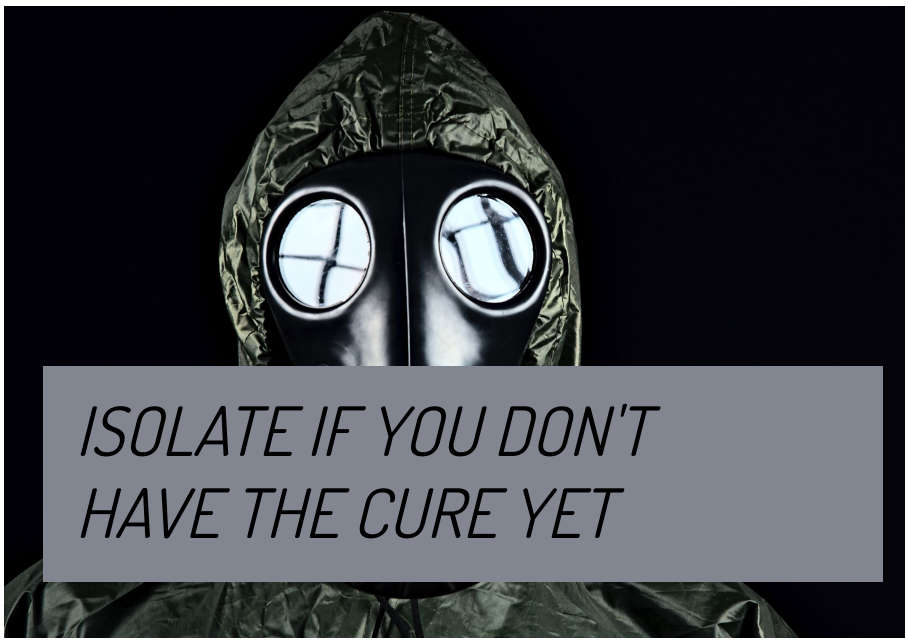
45%

Of the attacks target Web Browsers

ISOLATE THE RISK

REMOTE BROWSER ISOLATION IS NOT OPTIONAL IT IS MANDATORY

In an email, the user clicks on a link, which is assumed safe, given investments in email content security. That link opens a web browser, and there is always the possibility that the user's device may get infected as part of a phishing attack. However, the browser has already executed code that could lead to an infection. Even pop-up blockers are not enough to protect under specific attacks. For instance: The user may click on a link on their device, the pop-up blocker blocks access, and often the user does not notice.



WHY NOT JUST BLOCK USERS FROM BROWSING THE WEB?

Enterprises for years have been blocking massive numbers of websites to protect assets, which has led to productivity degradation for many employees and a great deal of frustration.

These workers find workarounds, including switching to a second device to access blocked websites rather than being able to access a "rendition" of those sites protected from embedded malicious code and criminal campaigns.

> “Almost all successful attacks originate from the public Internet, and browser-based attacks are the leading source of attacks on users. Information security architects can't stop attacks but can contain the damage by isolating end-user internet browsing sessions from enterprise endpoints and networks. By isolating the browsing function, malware is kept off of the end-user's system and the enterprise has significantly reduced the surface area for attack by shifting the risk of attack to the server sessions, which can be reset to a known good state on every new browsing session, tab opened or URL accessed.”
>
> GARTNER

REMOTE WORKING IS PERSISTENT

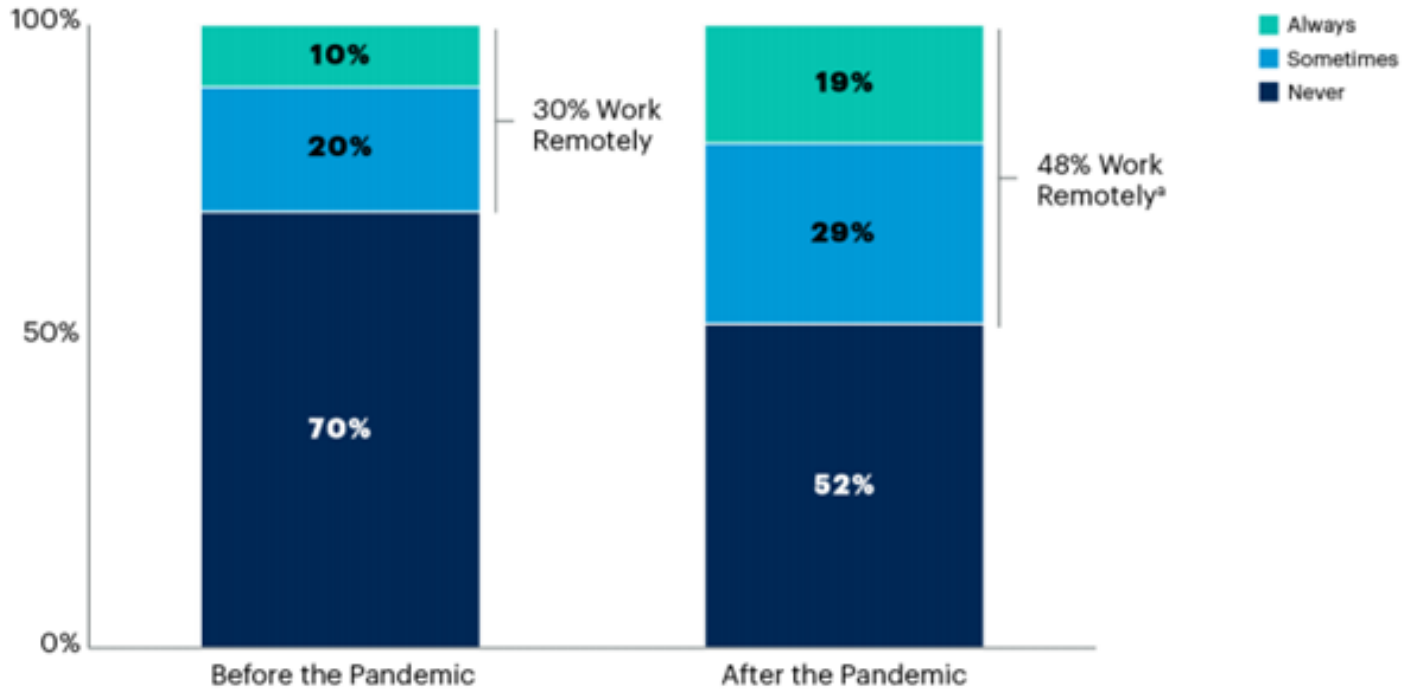
IMPACT OF REMOTE WORKING

The working environment and employee behavior have changed forever due to the COVID-19 pandemic.
This is a global transformation changed billions of employees and millions of enterprises.

These sweeping changes and unprecedented levels of disruption have created a work from home landscape focused on individuals working from anywhere, using any device, and accessing a network of their choice; it is no longer built around office building locations.

Any cyber defense technology should consider employees working anywhere on any device. Protecting only desktops is yesterday's way of thinking. The adoption to the new normal is lagging behind the novel threats of today creating greater risks for the enterprises.

Projected Percentage of Employees Working Remotely, Before and After the Pandemic



40% **Modern employees would now choose to spend 40% of their time working from home**

GROWTH OF CLOUD NETWORKS & PRODUCTIVITY APPLICATIONS

The global productivity management software market is expected to reach USD 102.98 billion by 2027, according to Grand View Research, Inc. "The growing demand for workforce management among several businesses, coupled with the need for communication and collaboration between the remote workers, is expected to drive market growth for productivity management software market. The increased adoption of Bring Your Own Device (BYOD), cloud-based SaaS solutions, and enterprise mobility among the small and medium-sized enterprises is expected to propel the demand for productivity management software solutions."

Grand View Research

EVERYTHING TO SaaS TRANSFORMATION

Digital transformation initiatives and the move to the cloud are accelerating, given the benefits of "as a service" models.
Combined with the continued growth of remote working, the rise of browser-based activities is driving the demand.

WHY TRADITIONAL APPROACHES ARE NOT ENOUGH

- Latency issues
- Poor performance
- Scalability issues
- Outdated centralized architecture • Poor user experience
- Expensive to maintain
- Office building focus

99% of the organizations use at least one SaaS application as of 2022

A web browser is the #1 access tool for the SaaS

RIGHT TECHNOLOGY AND GREAT BENEFITS

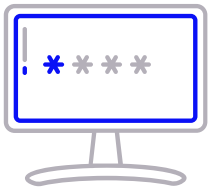
Zero-Trust Web Browsing

Remote Browser Isolation

Zero-Trust File Protection

DNS Protection

Cyber Vigilance Training



Zero-Trust Credentials

01 Protect your investment

Businesses that understand the modern risks of the Internet are protecting their investments by using DefensX's superior technology. Business owners focus on growing their business instead of thinking about the financial risks of a breach or reputation damage.

02 Maximize Productivity

Keep employees focused on their daily tasks and away from distracting sites, measure their cyber hygiene, and educate them on the cyber security strategies of the company. Enterprises using DefensX improve the cyber integrity and create self-imposed cyber security practices without any friction.

03 Comply with regulations

Gain unparalleled visibility on your company's digital exposure without any extra investment. Enterprises using DefensX have access to credentials exposed, ShadowIT, shared or downloaded files, visited web pages, and employee cyber risk score visibility. Protection starts with correctly understanding the risk.

DefensX converts a traditional web browser into a zero-trust secure browser. Zero-trust threat prevention technology protects users from advanced cybersecurity attacks by isolating threats from reaching end-point devices, such as desktops, laptops, smartphones, and tablets.

Reach out to us today and let's start your protection.

The DefensX Team

DefensX

info@defensX.com