REDUCE RISK AND IMPROVE PRODUCTIVITY: AUTOMATICALLY BLOCK WEB THREATS USING ADVANCED THREAT ISOLATION TECHNOLOGIES

Given the dramatic rise in remote working, 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.

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

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.

INTRODUCTION

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 2020 as millions of employees, contractors and partners were forced to work from home, attackers are easily bypassing preventative controls including signature-based malware scanning, firewalls and secure web gateways (SWGs).

WHAT IS REMOTE BROWSER ISOLATION AND HOW DOES IT WORK?

A remote browser isolates the user's browsing activity from the end user's device and from the enterprise's networks and systems. This effectively creates an 'air gap' between inevitable attacks and the enterprise network, in effect restricting the ability of an attacker establishing a foothold, move laterally within the organization and breach other enterprise systems to exfiltrate data.

Remote browser offerings are a subset of browser isolation technologies that remove the browsing process from the end user's desktop and transfer it to a designated browser server or cloud-based browser service. The remote browser servers then render the browser content remotely and send a bidirectional stream which represents the rendered session out to the user's local browser which includes audio, video, and keyboard and mouse interactions back to the session.

HOW DO ATTACKERS BREAK THROUGH THE WEB BROWSER?

Attackers generally break into the network by means of 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. This makes 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.

THESE ATTACKS ARE REFERRED TO AS ADVANCED PERSISTENT THREATS

Especially given the massive growth of remote working, employees, contractors, partners and customers are using browser-based applications for productivity. 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.

This happens on desktops, laptops, tablets, and smartphones, and 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.

USERS ARE PREDOMINANTLY ATTACKED THROUGH E-MAIL AND WEBSITES

In an email, the user clicks on a link, which is assumed safe, given investments in e-mail 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. Even pop-up blockers are not enough to protect under certain 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. However, the browser has already executed code which could lead to an infection.

WHY NOT JUST BLOCK USERS FROM BROWSING THE WEB?

Enterprises for years have been blocking massive numbers of websites to protect assets. This has led to a reduction in productivity for many employees, and a great deal of frustration when research is hampered, for example. 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.

A user tries to access a potentially malicious webpage

Defined policies are applied to the request automatically; if there is a match, the platform creates an isolated browser session

The platform connects to the webpage and loads the content onto the remote isolated browser

Rendered web content is streamed to the end user’s native browser as pixels over an HTML5 canvas

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 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®

RISING NUMBER OF ATTACKS

New research shows significant increase in phishing attacks in 2020. The 2020 Phishing Attack Landscape Report, commissioned by GreatHorn and conducted by Cybersecurity Insiders, asked a sample of 317 professionals ranging from executives to IT security practitioners across the greater cybersecurity industry, to provide insights based on their personal experiences.

According to this survey data, the frequency of phishing threats rose considerably in 2020, with companies experiencing an average of 1,185 attacks every month.

38% of respondents reported that a coworker fell victim to an attack within the last year. As a result, 15% of organizations are now left spending anywhere from one to four days remediating malicious attacks. More than half (53%) of those surveyed said that they had witnessed an increase in phishing activity since the start of the pandemic.

Results showed considerable increased frequency of attempted phishing attacks, and by extension a major increase in time allocated towards attack mitigation, removal and additional incident response.

The organizations surveyed on average remediated 1,185 phishing attacks every month. With 15% of organizations spending 1-4 days remediating attacks, the amount of total time lost due to this increase in attacks is hurting the bottom line.

The survey also found that 64% of employees felt confident in their ability to identify and avoid a phishing email in real time. Still, 38% of respondents confirmed that a member of their organization had fallen victim to a phishing attack within the last year, and over a third (39%) felt that such an error reflected poorly on the victimized employee.

> "Keeping employees apprised of the ever-advancing threat landscape is paramount. We're proud to have facilitated this survey that exposes the realities of coming face-to-face with phishing attacks in real-time, particularly in mass quantities, and we hope that this data serves to promote better phishing education and protection across the industry."
> Holger Schulze, CEO and Founder of Cybersecurity Insiders

Cybersecurity
INSIDERS

IMPACT OF REMOTE WORKING

The working environment and employee behavior have changed forever due to the COVID-19 pandemic.

This is a global transformation affecting billions of employees and millions of enterprises. According to Work Statistics, 55% of the US workforce is now working from home and it is predicted that at least 25 to 30% of the workforce will be working from home multiple times a week after 2021.

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

According a Gartner report, when it comes to work from home productivity and cybersecurity environments, "The cost to the enterprise varies widely per geography and availability of services but generally is within the $40 to $150 per-month per-user range and usually in the $60 to $90 range. While this may seem high (for example 1,000 users would equate to $1.2M per year), it can be fully or partially offset by the reduction of costs for facilities, including real estate and security." By securing the "new perimeter" CIOs, CISOs and CXOs can reduce costs, and remote browser isolation is one part of a complete cyber security posture.

GROWTH OF CLOUD NETWORKS & PRODUCTIVITY APPLICATIONS

Digital transformation initiatives and the move to 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 for:

WEB **PROTECTION**

Protect workforce anywhere

URL Category & Risk Score based controls

SAAS APPLICATION **ACCESS PROTECTION**

Best User Experience

O365 Protection

PHISHING **PROTECTION**

Foolproof

Credential Exposure Protection

ACCESS **ISOLATION**

Secure Remote Access

No VPN No RDP No DaaS

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."

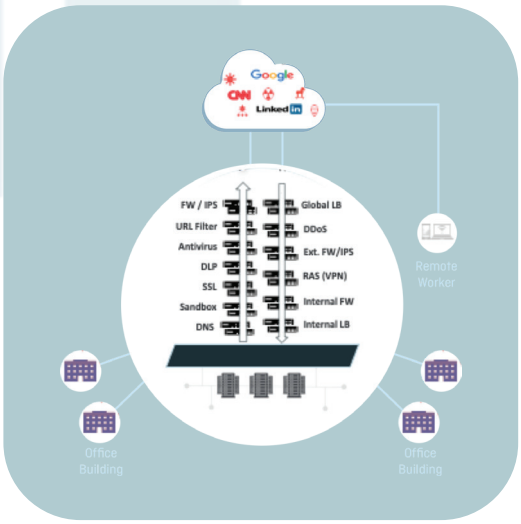
GRAND VIEW RESEARCH

WHY TRADITIONAL APPROACHES ARE NOT ENOUGH

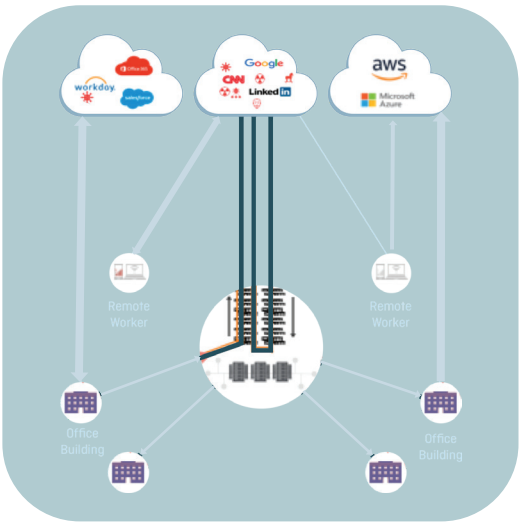
Experience shows that hybrid (on-prem and cloud) solutions are complex, expensive and fall short. Among the challenges:

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

ON-PREM APPROACH



HYBRID CLOUD APPROACH

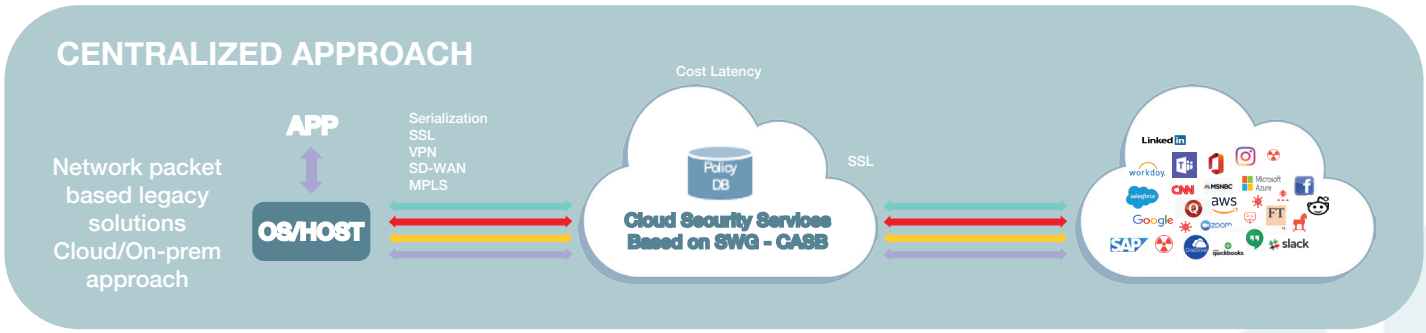


ADDRESSING THE GAPS

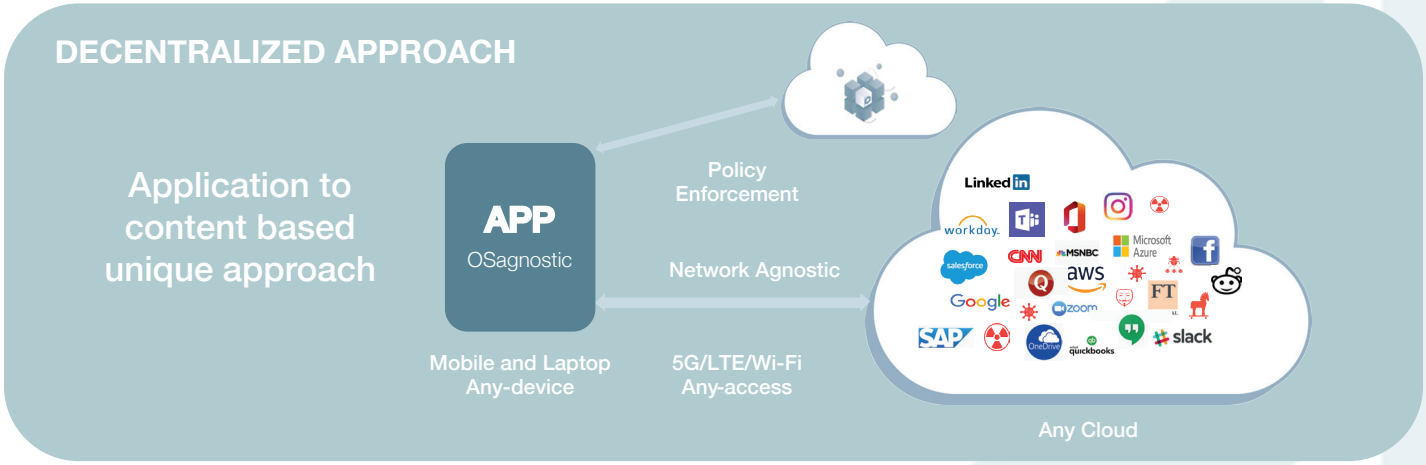
Using advanced threat isolation, with 5G/LTE/WIFI network options, any device anywhere can support productivity and liberate users with:

- No latency
- Reliable performance
- Scalable security
- Best of breed technology
- Excellent user experience
- Cost efficiency

CENTRALIZED APPROACH



DECENTRALIZED APPROACH



USE CASE EXAMPLES

WORLD'S SECOND LARGEST PROVIDER OF INSTRUMENTATION, SOFTWARE & SERVICES

- A medical products and equipment provider with >440 global branch locations with 70K+ employees
- Employees vulnerable to security breaches/attacks
- Broadcom/Symantec web security service deployment & partnership not going well
- Reliable phishing protection & VPN connection for expansion of remote users required because of COVID-19 pandemic

Use Case:

- Web Security Service
- Isolation/Phishing Protection
- VPN Replacement

ISOOLATE SOLUTION BRINGS:

- Best of breed technology
- No SSL certification inspection required as Isoolate lives in the browser
- Cost efficient
- Forward traffic for Risk Based Inspection (RBI) w/o Secure Web Gateway (SWG) / Next Generation Firewall (NGFW)
- Deployed from single Kubernetes container
- No SSL or No Load Balancer is required for High Availability (HA) at additional cost
- Security admin overheads reduced as maintaining a PAC file & pushing to endpoints to route traffic to SWG is no longer required
- Flexible deployment in seconds
- "Isoolate Anywhere" extension installed and pushed to endpoints in seconds
- Deployments both SaaS and IaaS integration
- No management or policy server required

USE CASE EXAMPLES

LEADING EUROPEAN CONTRACT RESEARCH ORGANIZATION IN THE PHARMACEUTICAL INDUSTRY

- Offers leading-edge analytical support throughout the process of developing innovative medicines for human use
- Strict cyber security measures in place due to mission critical business binding by EMA and FDA regulations
- Majority of scientists working from home due to COVID-19 pandemic
- Evaluated and tested ZScaler & other company solutions – decided to consider Isoolate

Use Case:

- Full remote browser isolation
- Threat protection for users anywhere
- Proxy Server, SWG Replacement
- Threat protection for users anywhere
- O365/MS Teams protection

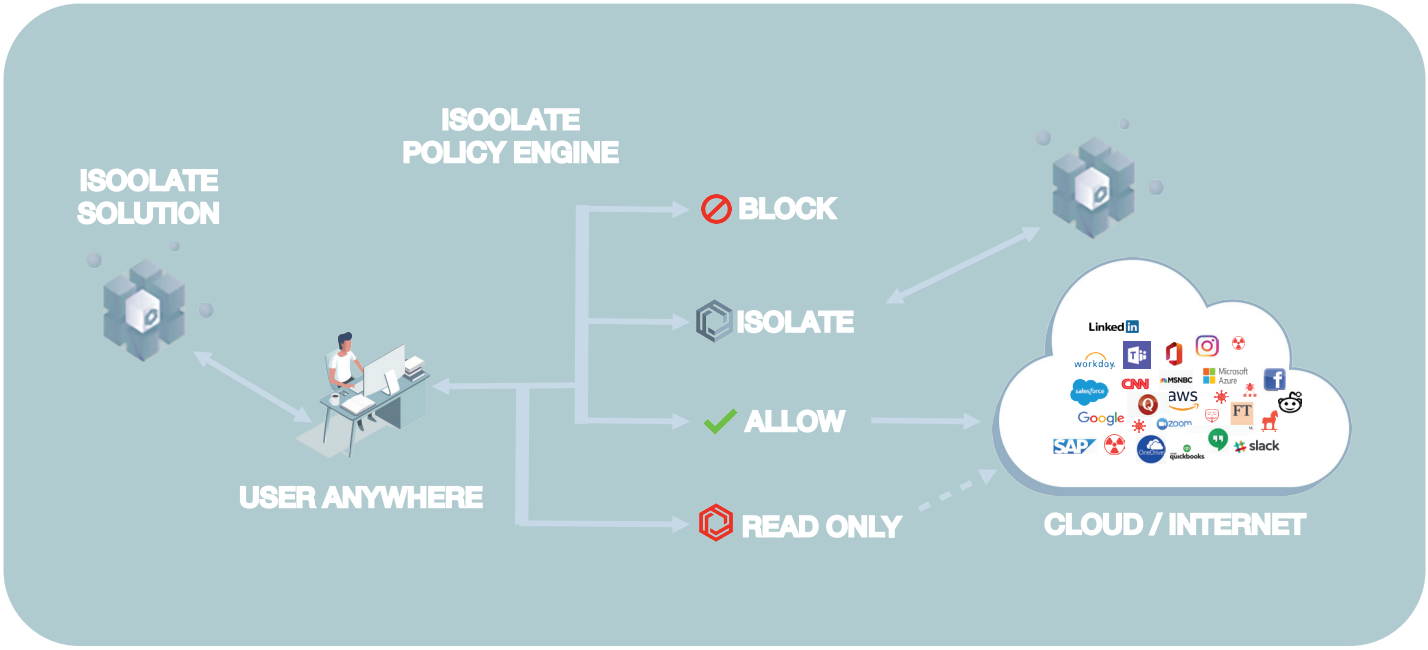
ISOOLATE SOLUTION BRINGS:

- Best of breed technology
- Full remote browser isolation delivered for as many concurrent sessions as customer requires
- Strict isolation policies in place (block/isolate) for all users working from home/anywhere
- Cost efficient
- Replacement of proxy server for phishing protection
- VPN replacement
- Flexible deployment in seconds
- “Isoolate Anywhere” extension installed and pushed to endpoints in seconds
- No management or policy server required

SIMPLICITY LEADS TO EFFICIENCY, FOR IT TEAMS AND USERS ALIKE

ISOOLATE'S SOLUTION – BRINGING SECURITY ANYWHERE

- No reliance on applications or network virtual appliances
- Web traffic from cloud to end user remains unmodified
- Instant threat reporting to ensure real-time response
- Ease-of-use for security professionals to manage company attack surfaces
- Fool proof phishing threat protection
- Remote browser isolation
- Unlimited scalability, agentless architecture
- Quick deployment (100K users in less than 5 minutes)



TEN QUESTIONS CIOs AND CISOs SHOULD ASK WHEN DEVELOPING A WEB ISOLATION SECURITY STRATEGY

- What is your organization doing today to protect from advanced web threats which are initiated on the browser?
- How are you protecting your infrastructure and assets associated with XaaS cloud-based applications which run on the browser?
- Are you currently using Secure Web Gateway (SWG) solutions and what are the true costs using a centralized model?
- How confident are you that security policies for remote browsing are being enforced and how much of that enforcement is owned by your IT security team vs. end-users?
- How are the solutions you are considering implemented? What do they cost, and how do they scale?
- Which browsers and operating systems (OS) are supported (Chrome, Microsoft Edge, Firefox, Brave, Windows, Mac, Android, iOS)?
- Which cloud platforms are supported (Azure, AWS, GCP)?
- Does the isolation solution protect end points from cyber threats by not allowing unmanaged traffic into your enterprise?
- Is the solution a “resource hog” or does it use disposable dockerized instances (not browsers), which prevents any attack from reaching the end user?
- Does the solution require your organization to install certificates at each end point to enable SSL inspection?

THE ISOOLATE SOLUTION

Isoolate is transforming the nature of cyber security by liberating users with a content to application approach. With its unique advanced web and threat protection technologies, Isoolate seamlessly and effectively prevent cyber threats of today and tomorrow, providing a better user experience anywhere, on any network and on any device, at a fraction of the cost.
Isoolate’s solution is:

- Device, operating system & network access technology agnostic
- Applicable to on-premises, hybrid or pure cloud networks
- Cloud Native, web-based plug-in solution
- Single solution for Working From Home (WFH), phishing, Microsoft Office365 security, access isolation for any desktop, laptop, or mobile device and Bring Your Own Devices (BYOD)
- Extremely scalable as it can onboard 100K users in less than 5 mins
- Bringing seamless & excellent user experience with zero latency
- Cost-efficient

SECURITY FOR THE CLOUD – DELIVERED ANYWHERE

Isoolate works on all devices, networks and operating systems

ABOUT ISOOLATE

Isoolate, founded in 2018 in New York, NY, is transforming the nature of cyber security by liberating users with an “application to content” approach. With its patent pending unique threat isolation technologies, Isoolate seamlessly protects users, from web and SaaS application content-borne threats, who work from anywhere, on any device, and over any network. For more information, visit **isoolate.com** or **linkedin.com/company/isoolate/**

Contact Us
selcan@isoolate.com