paloalto NETWORKS

PRISMA BY PALO ALTO NETWORKS

Prisma Access Cloud SWG

Defending Against Modern Web-Based Threats

TABLE OF CONTENTS

In recent years, the way we work has drastically changed. The majority of organizations have shifted to hybrid work, allowing their employees to work from anywhere, while some have even completely moved away from offices and embraced a permanent work-from-home model. Additionally, these organizations have predominantly turned to Software-as-a-Service (SaaS) tools to preserve, and even increase, the productivity of their remote workforce.

Overall, this new approach to how we work is good for employees and businesses, but even better for cyber criminals.

The mass adoption of hybrid work and SaaS applications have escalated the need for organizations to ensure safe access to the web for their employees, no matter where they reside. The increasing ability to access the web from anywhere with almost any device has drastically widened the threat landscape, giving attackers countless opportunities to breach an organization using highly-sophisticated and intricate techniques that overwhelm traditional security.

These advanced web-based threats call for a new approach to web security. Organizations can no longer rely on legacy approaches to stop today's new and never-before-seen threats. Instead, they need a solution with capabilities well-suited to keep up with adversaries and their modern methods.

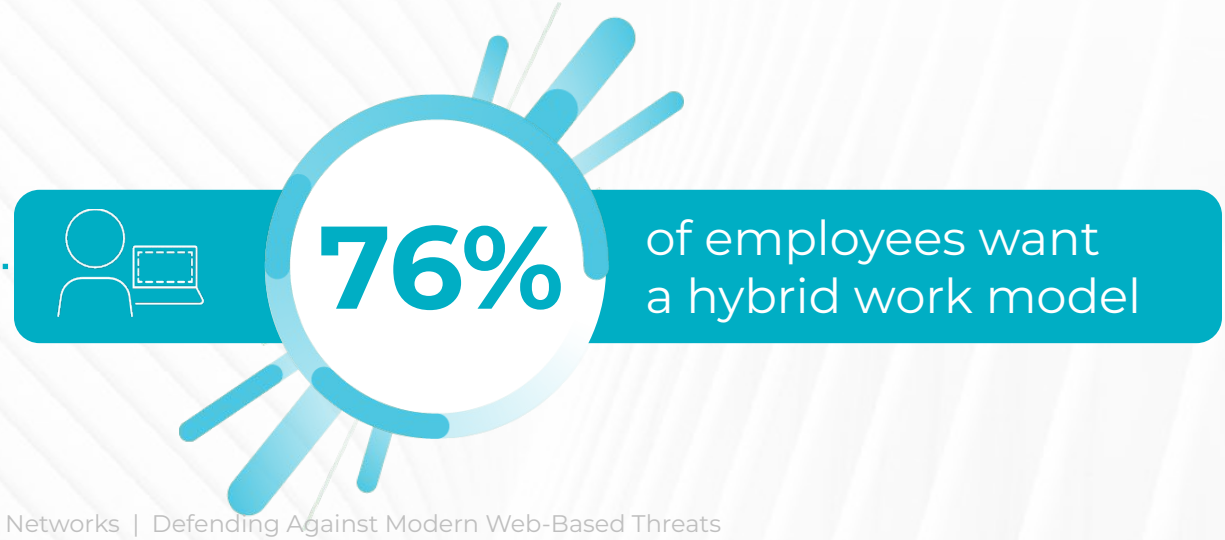
3 Reasons
the Web is Rapidly Growing as an Attack Surface

1 We rely on the web more than ever before

It is no secret that the web and the applications hosted on it are foundational to our everyday productivity. We access sites through various devices on any given day, whether it be for business or personal reasons. Although this use of the web has made us more efficient, it has also led to a larger attack surface for threat actors to exploit for malicious activity.

2 The work-from-anywhere model has made employees more vulnerable

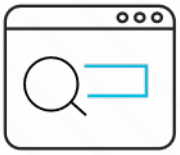
Work is no longer a "place," and is now an activity we perform. This means employees are free to work from the comforts of their own home, in public areas like coffee shops, or anywhere with a Wi-Fi connection. But along with the many benefits of remote work comes major risks. Employees are now relying on their home or public networks to handle sensitive tasks related to their company. Traditionally, organizations used technologies like virtual private networks (VPNs) and legacy Zero Trust Network Access 1.0 (ZTNA) security to protect their remote users, but these approaches lack flexibility and come with too many limitations. This leaves remote users vulnerable to threats that would otherwise be blocked by a private and secure network that an office would typically offer.



3 Threat actors are more sophisticated than ever

Today's adversaries are becoming well aware of the tactics traditional security use to stop their attacks, forcing attackers to evolve and uses advanced tactics of their own. Threat actors are increasingly using highly evasive techniques, such as cloaking, multi-step attacks and single-use links, to launch new and never-before-seen threats, allowing them to bypass security with ease.

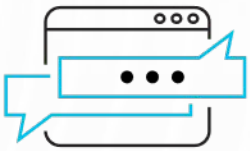
"Internet Minute" in 2022



5.7M
Google Searches

856
Minutes of Webinars on Zoom

6M
People Shopping Online



148k
Slack Messages Sent

Web-Based Threats You Should Know About

In this new era of how we work, there is a significant amount of sensitive work and collaboration done over the web.

Communication primarily happens over email, Zoom or Slack. We rely on SaaS business applications like Google Workspace or Microsoft 365 to collaborate and share confidential material within our organization. Additionally, employees can look to unauthorized applications like Trello, Asana, Dropbox, or Evernote for their own personal productivity. Therefore, this large dependency on the web and business applications have made it much easier for threat actors to get a hold of sensitive information, resulting in very serious and costly repercussions.

Amidst the many types of threats carried out through the web, we have seen attacks like phishing, ransomware, and malware become extremely popular amongst adversaries. Phishing attacks have a high success rate due to how easy it is to create and launch a malicious campaign; ransomware attacks can offer huge financial gains for attackers; and threats of malware introduce a number of opportunities for attackers, such as financial gain or data theft.

Phishing

A Growing Threat to the Enterprise

Phishing is a form of social engineering where a threat actor sends fraudulent communications, typically through email, SMS messages, social media or phone calls, to a user in an attempt to trick them into downloading malware onto a device or forfeit sensitive information such as login credentials, personal identifiable information (PII) or financial data. While phishing is not new and has been used by attackers for decades, it remains one of the most prevalent and dangerous types of cybercrime.

Due to the amount of communication done online, emails are an extremely popular delivery method for phishing attacks. In fact, studies have found that **96% of phishing attacks in 2021 were delivered through email.** Attackers will often use a "spray & pray" approach, meaning they will send a mass amount of emails loaded with malicious links, in hopes that at least one of them will be successful.

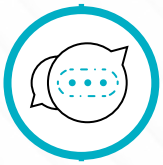
5 Common Types
of Phishing Attacks

Spear Phishing

A personalized and targeted email that often includes a link or attachment loaded with malware, which when opened, launches the malware onto the target's device and gives the attacker access to their private information.

Whaling

A form of phishing that targets high-profile executives of a company with the intent of stealing sensitive information, such as login credentials or financial data, or downloading malware onto the target's device.



Smishing

A form of phishing that occurs through SMS messages that often contains a fraudulent attachment or link, prompting the user to click from their mobile devices.

Vishing

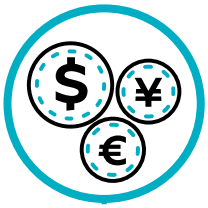
Also called "Voice Phishing," vishing is a form of phishing that targets victims over the phone and often acts as the victim's bank or a government agency to gain access to data.

Angler Phishing

A form of phishing that targets social media users. Attackers will impersonate a customer service agent from a legitimate company and target disgruntled customers with the intent of stealing their personal information or login credentials.

Risks of Phishing Attacks

Falling victim to a phishing attack can be devastating to an organization. The financial ramifications is what gets talked about the most but, of course, is not the only outcome.



Financial Loss

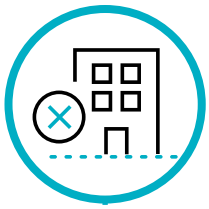
One constant result of a successful phishing attack is financial loss, which can happen in various ways. For instance, an organization or its employees can be tricked into transferring funds to an attacker; face hefty fines for non-compliance due to policies such as HIPAA, PCI, and PIPEDA; or suffer the costs of investigating a breach and compensating any affected parties.

Data Loss

Adversaries who have successfully phished a user can gain access to a variety of sensitive data. This could be login credentials; personal data, such as addresses and phone numbers; company data; medical information; or banking information.

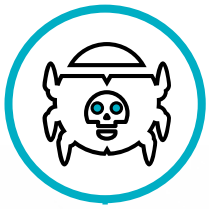
Reputational Damage

Companies often try to conceal the fact they've fallen victim to a phishing attack in order to preserve the trust of their customers and investors. This is especially important if an organization is known for managing the sensitive information of its customers.



Business Disruption

Phishing attacks that successfully infect devices with malware can lead to system downtime or a significant disruption in providing services, hindering business productivity.



Malware Infection

Successful phishing attacks can infect organizational devices with malware, leading to business disruption, data theft, network downtime, and more.

Ransomware

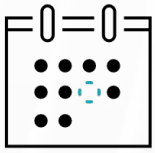
Ransomware, which is a form of malware, is a devastating impact of phishing attacks that can lead to financial and data losses. Attackers encrypt sensitive data and force the victim to pay a ransom for the decryption key in order to retrieve the lost information.

$14.8M

Average cost of a phishing attack in 2021.

$4.24

The average cost of a data breach in 2021.



50 Days

Malware attacks cause an average loss of 50 days for businesses.

The Rise of Ransomware Attacks

Ransomware is a form of malware designed to deny a user or organization access to valuable files, data, or information on a device. An attacker will encrypt these files and demand a large ransom from the victim for the decryption key.

Recently, ransomware attacks have dominated headlines and have shown no signs of slowing down. **In 2021, there were over 623 million ransomware attacks, marking an increase of 105% year-over-year.** This surge is largely due to Ransomware -as-a-Service (RaaS) which lowers the barrier to entry and makes tools widely accessible to adversaries of all skill levels, increasing the volume and frequency of ransomware attacks.

What is Ransomware-as-a-Service?

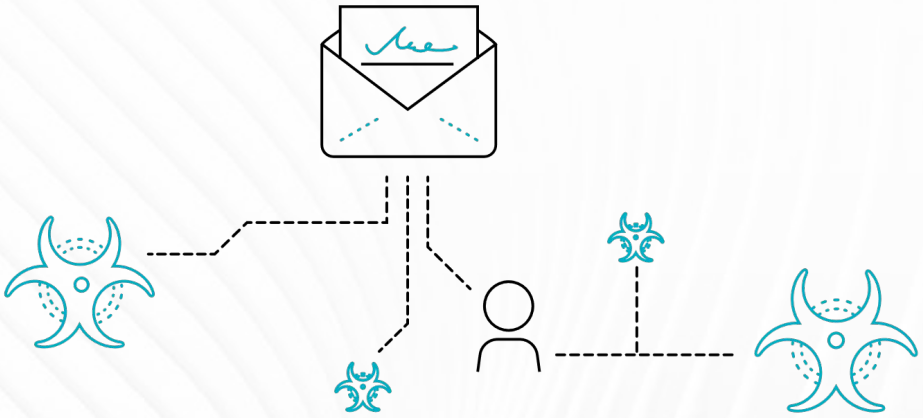
Ransomware-as-a-Service (RaaS) is a business run by cybercriminals, for cybercriminals. This business model lowers the barrier to entry and makes the tools to launch ransomware attacks widely accessible for adversaries of all skill levels. Affiliates collect monthly fees and earn a percentage of ransoms paid.

What is the Most Common Delivery Method of Ransomware?

Phishing emails

One of the most common methods adversaries use to deliver ransomware is through phishing emails, largely due to the sheer volume of emails sent daily.

Today, there are approximately **333.2 billion emails sent every day, meaning that 3.5 million emails are sent every second.** This overreliance on email as a primary means to communicate increases the likelihood of a user being tricked into clicking a malicious link and downloading ransomware onto their device. In fact, of those 333.2 billion emails sent everyday, **3.4 billion are phishing emails.** This means that for every 100 emails you get, 1 is likely to be a phishing email. And, depending on how many email addresses or email subscriptions you have, you can be exposed to multiple phishing emails every day.



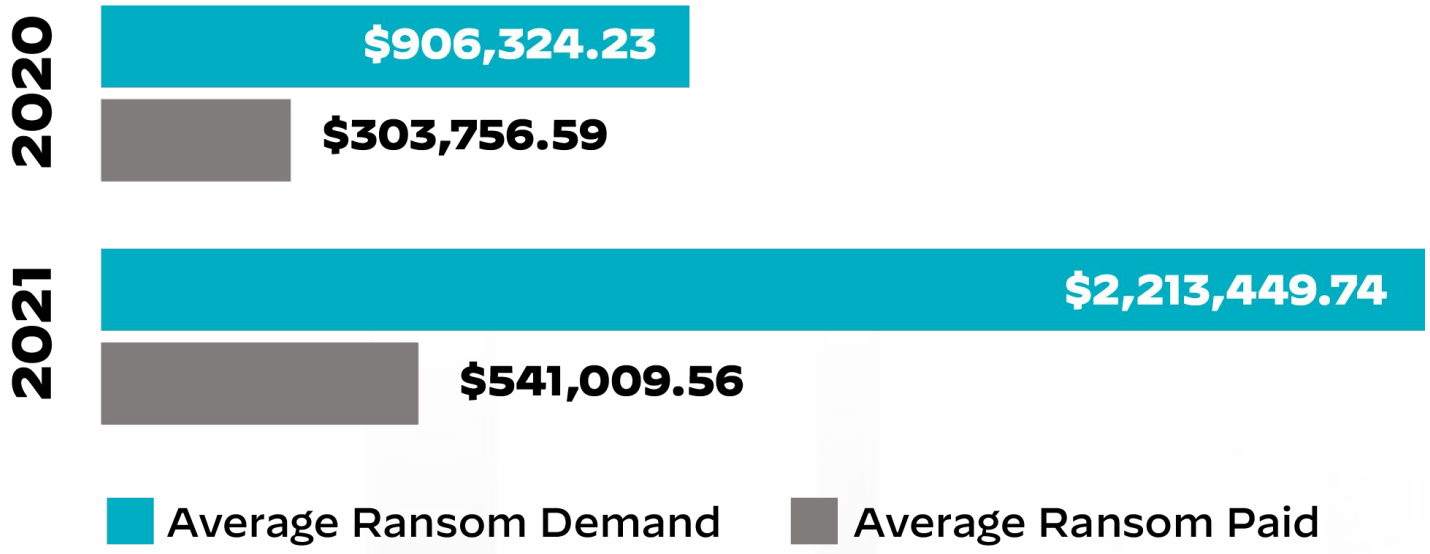
78% of organizations

in 2021 received a phishing email loaded with ransomware or a link to download ransomware.

Impact of Ransomware Attacks

While ransomware attacks continue to soar in volume, the costs of these attacks have also grown tremendously.

The average demand of a ransomware attack in 2021 was **$2.2 million, a 144% increase from 2020, while the average payment was $541,000, a 78% increase from the previous year.** The volume of these attacks coupled with the potential ramifications is what makes ransomware a truly devastating and damaging threat to victims.



Average ransom demands compared to average ransom payments in 2020 and 2021, according to Unit 42 incident response data

Malware

A Common Threat to All

Malware, also known as malicious software, is an adversary's number one tool to infect systems and networks.

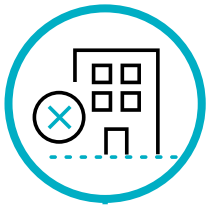
If an attacker is able to install malware onto a user's device, they can establish a **command-and-control channel, allowing them to gain remote access of an infected machine**, spread malware to unsuspecting users, gain credentials, investigate a user's local network, action objectives like steal sensitive data or deploy a bot, or even use their network to launch an attack on another organization. There is a wide variety of delivery methods attackers use to distribute malware, but phishing has become an extremely popular method since the rise increase in hybrid work.

What is Command-and-Control?

Command-and-Control (C2) is a technique used by threat actors to communicate with compromised devices over a network in order to deliver further instructions such as download additional malware, create botnets, or exfiltrate data.

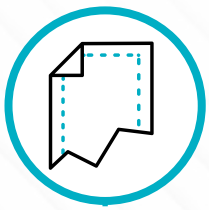
Impact of Malware

A successful malware attack can severely fracture a network's security infrastructure and cause several security issues to an organization, all while requiring lots of time and effort to rectify. Some common impacts of malware attacks include:



Business Disruption

Malware can hinder or freeze networks, disrupting business operations, and in some cases prevent a business from offering services. This can impede business productivity and result in catastrophic losses for an organization.



Data Loss

A business who loses data to a malware attack can face a number of serious implications, such as legal action, loss of client confidence, and reputational damage.

Reputational Damage

Falling victim to a malware attack not only involves the financial losses that come from halting operations, but can also come from the loss of customers, data recovery efforts, investigation costs, legal or regulatory fees, and settlement costs.

Challenges Traditional Security Faces

With the potential risks of attacks like phishing, ransomware, and malware infection, organizations are under immense pressure to ensure they do not become a victim. Although, due to the evolution of today's threat actors, this is proving to be a massive challenge for traditional security.

Adversaries Are More Sophisticated Than Ever

One of the key contributors to the success of today's web-based threats is the **sophistication of threat actors.** Over time, attackers have evolved their techniques to outsmart traditional security and evade defenses.

1. Attackers are largely adopting the use of evasive techniques, such as cloaking, Man-in-the-Middle reverse proxies, and using legitimate SaaS platforms to avoid being detected.

2. With easily accessible phishing kits and by leveraging cloud infrastructure, attackers can generate and launch thousands of phishing URLs within minutes.

3. Attackers are using new and never-before-seen threats that can't be detected by traditional security, allowing them to bypass any defenses with ease.

5 Common Types
of Evasive Techniques

Use of New and Never-Before-Seen URLs

Traditional web crawlers are not fast enough to detect new and never-before-seen malicious URLs, allowing attackers to easily bypass security defenses.

Hiding Malicious Content Through Cloaking

Since web crawlers do not analyze live web traffic, attackers can cloak malicious intent by sending security scanners to a benign site or a blank page before ultimately launching a malicious site.

Multi-Step Attacks and CAPTCHA Challenges

Adversaries hide malicious content behind a series of benign steps, such as CAPTCHA challenges, to prevent web crawlers from detecting the actual malicious content behind them.

Dynamic Links and Phishing Kits

With the help of phishing kits and automation tools, it is now cheaper and easier than ever before to generate new and never-before seen URLs in volume. This allows adversaries to use a bad URL for mere minutes, or seconds, before switching to a new URL, making it difficult for security to track.

Compromised Websites and SaaS Platforms

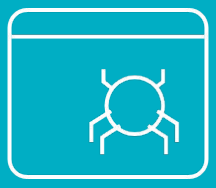
Attackers can compromise benign websites or leverage legitimate SaaS platforms to launch phishing attacks, allowing them to avoid traditional detections.

Why Traditional Security

Can’t Keep Up With Attackers

Many organizations rely on legacy methods, such as web crawler data, to stop today's sophisticated and highly-evasive threats, resulting in an increasing number of businesses falling victim to web-based threats like phishing.

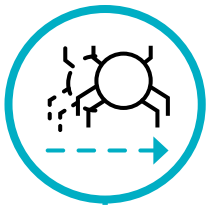
Although, these methods struggle against new and unknown threats. **56 million new malicious web pages** were created in 2021, it's no wonder that **93% of organizations were successfully phished in 2021.** Here are some reasons why traditional web security struggles to keep up with modern threats.



What is a Web Crawler?

A web crawler is a type of bot that "crawls", or browses, the World Wide Web searching and indexing sites, creating a list of pages that eventually appear in your search results.

The following page lists three reasons why traditional web security struggles to keep up with modern threats.



Web Crawlers Are Too Slow

The crawling and analysis done by web crawlers are not fast enough to keep up with the speed and evasiveness of modern threats. Attackers are constantly using automation tools and evasive techniques to quickly create new malicious web pages in volume, bypassing traditional defenses. Failing to prevent these threats before they enter your network can result in significant losses.

Traditional URL Filtering Databases Can't Scale

Traditional web security has long relied on the use of URL filtering databases, which consists of data gathered by web crawlers, to identify and block access to malicious sites, including phishing sites. Since web crawlers cannot scale fast enough, the URL filtering databases contain outdated data and cannot stop new and highly-evasive threats in time.

Most Web Traffic is Encrypted

Due to the majority of today's web traffic being encrypted, it is extremely easy for an attacker to hide their malicious activities. Despite 99% of browsing time on Chrome being done over HTTPS, most web security solutions today do not perform SSL/TLS decryption because it requires a significant amount of processing power to decrypt, inspect and re-encrypt the traffic. Without the proper technology, this decryption can greatly hinder a network's performance. Because organizations fail to decrypt traffic, they are increasingly falling victim to threats like phishing attacks. **In fact, 83% of phishing sites used today use SSL encryption to hide malicious activity from security scanners.**

The Right Methodology to Detect Evasive and Unknown Threats

When evaluating your web security needs, you must ensure that your vendor of choice offers the right tools and methodology that can keep up with the advances of threat actors.

What is Patient Zero?

A patient zero is the first person or system to be the victim of a previously unknown cyberattack. If an organization is alerted of a breach, protocol is to isolate or quarantine patient zero to prevent the spread of the attack.

5 Capabilities

Modern Web Security Needs

Data and Threat Detection

Modern web security requires detection capabilities that are informed by huge volumes of threat data. This data helps train machine learning models to accurately analyze and detect potential threats, without the need for human intervention and feature engineering.

Analyze Live Traffic

Traffic must be analyzed inline, meaning any malicious traffic is detected instantly as it enters the network. This is critical for stopping new and unknown threats because evasive techniques are not successful when analyzing live user traffic.

Real-time Enforcement

Not only do threats need to be detected as they enter a network, but they also need to be instantly stopped to prevent a patient zero. A solution must be able to stream traffic to the cloud for inspection and receive a verdict back in real time.

Cloud Analysis and Processing Power

Machine learning models require massive processing power to deliver results in milliseconds and provide a verdict in real time, preventing patient zero.

URL Database Delivering Instant Updates

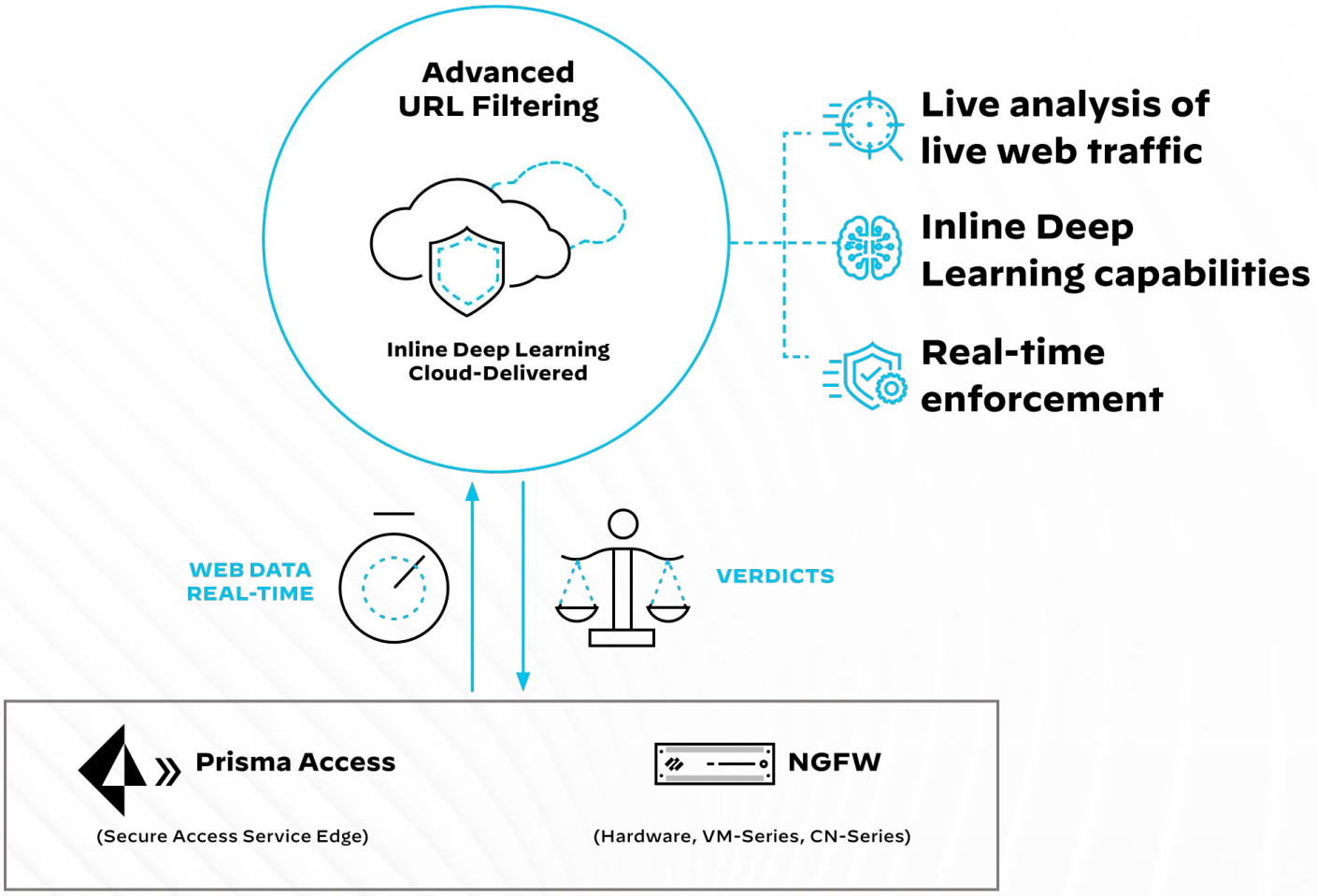
In order to evolve web security, we need to change our approach. Static databases are only one part of the solution. Ultimately, we need a cloud-delivered service that can leverage machine learning models to deliver instant verdicts on live data, so as to not fall victim to advanced techniques used by attackers.

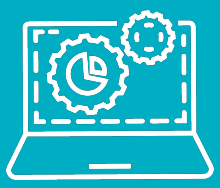
Prisma Access Cloud SWG

Advanced URL Filtering

Prisma Access Cloud SWG uses Palo Alto Networks Advanced URL Filtering to prevent today's unknown and sophisticated web-based threats in real time.

Using our Inline Deep Learning technology, Advanced URL Filtering is the industry's only web security solution that can prevent modern threats in real time to prevent patient zero, **stopping 40% more threats** than traditional web filtering databases.





What is Deep Learning?

Deep learning, which is a subset of machine learning, uses multi-layer artificial neural networks that do not require significant curation by data scientists, and is capable of learning from the security events they observe.

Analysis of Real Web Traffic

Analyze real web traffic as it enters the network instead of relying on after-the-fact analysis, stopping any malicious threats instantly.

Detect Evasive Threats

Increased detection of evasive and targeted attacks by inspecting real web traffic, not just web crawler data.

Protection

Prevent evasive known and unknown malicious web-based attacks in real time to prevent patient zero.

40%

more threat protection than traditional web filtering databases.

88%

of malicious URLs are blocked at least 48 hours before any other vendor.

11.5M

malicious URLs detected per day.

Enhance Your

Web Protection with paloalto® NETWORKS

Prisma Access Cloud SWG with Advanced URL Filtering not only stops the most evasive and sophisticated cyber attacks; it also streamlines operations and improves user experiences. Branches, home offices, and remote users can securely connect to the internet and all business-critical apps, irrespective of location, with the same level of access and uniform security as corporate headquarters.

Prisma Access Cloud SWG

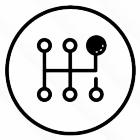
AI/ML-powered Internet and SaaS security

Visit Us

Cloud SWG vs Web Proxy Appliances

See a side-by-side comparison

Download Infographic



SASE Ultimate Test Drive

Experience it for yourself

Register Now

Modernize Your SWG with SASE

ESG white paper

Download

SOURCES:

- 90% of security incidents in 2021 involved phishing
- We as a population send 197.6 million emails, spend 1.6 million dollars online, and download almost 415,000 apps
- The average employee today spends more than 75% of their working day in a web browser
- Average cost of a phishing attack was $14.8M
- 93% of organizations were successfully phished in 2021
- 83% of phishing sites use SSL decryption
- 90% of today's phishing kits include evasive techniques
- 3.4 billion phishing emails are sent out each day

www.paloaltonetworks.com

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087