



News & Insights

News & Insights Home

Artificial Intelligence

Innovation

IT Careers & Skills

Cloud

Cyber Security

Future of Work

All Categories

Community

Community Home

Cloud

Collaboration

Hardware

Networking

Programming

Security

Software

Storage

Vendors

Virtualization

Windows

All Categories

Research

Research Home

State of IT 2025 Report

IT Spend Report

Customer Experience Report

Workplace Tech Report

IT Tools

Cloud Help Desk

Dark Web vs. Deep Web: 5 Key Differences

On the internet, the deep web is not indexed by web crawlers, while the dark web is intentionally kept hidden.



Hossein Ashtari Technical Writer

May 2, 2022

The deep web is defined as the internet section that is not indexed by web crawlers. The dark web, on the other hand, is defined as a subsegment of the deep web that can be accessed only with special tools. While the former is used chiefly for legitimate day-to-day online activities, the latter is more anonymous and known for illegal transactions. This article reveals the top five key differences between the dark web and the deep web.

Table of Contents

- Dark Web vs. Deep Web
- What Is the Dark Web?
- What Is the Deep Web?
- 5 Key Differences Between the Dark and Deep Web

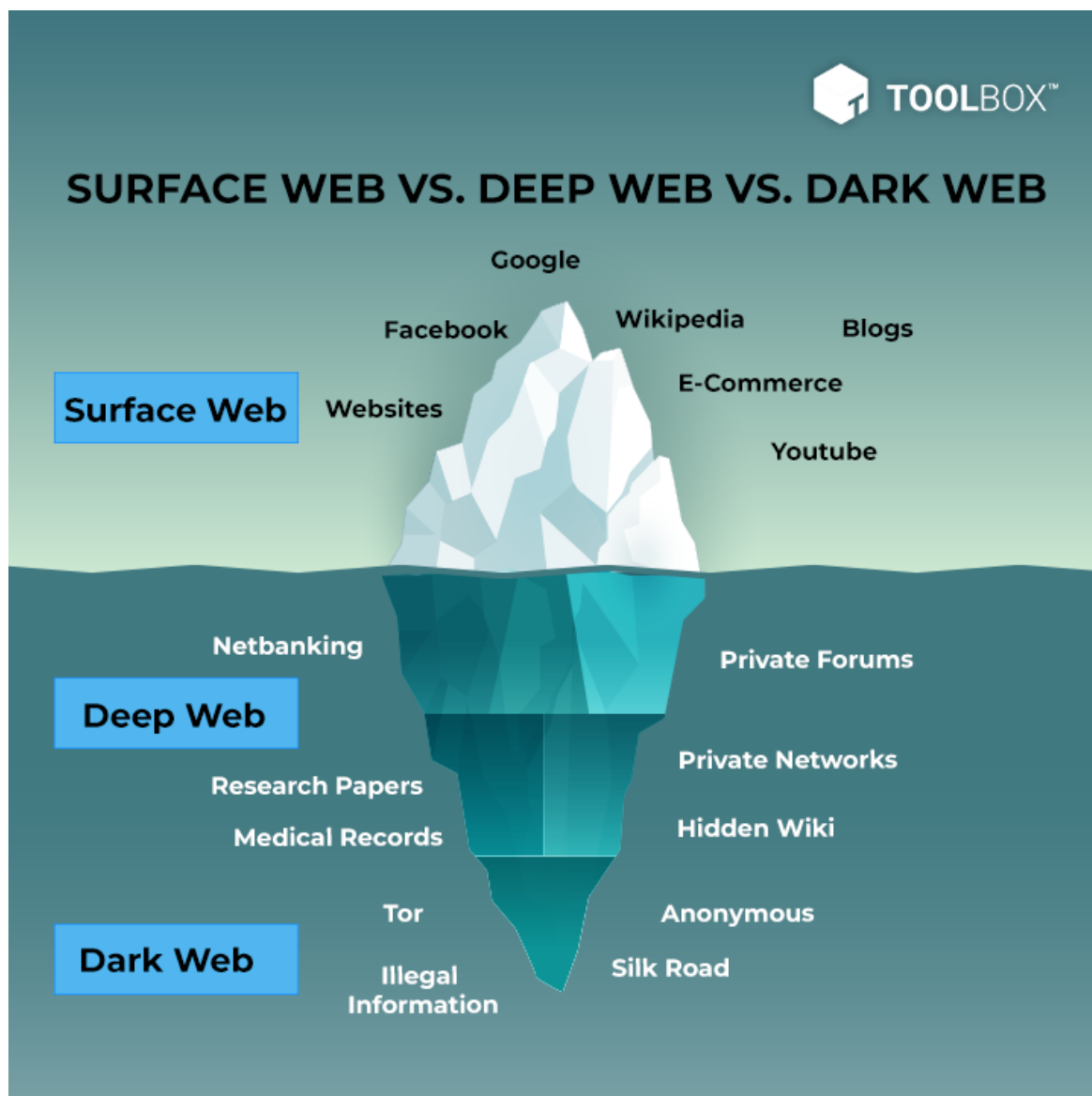
Spiceworks

Happy Sys
Ultimate IT
Spiceworks

Another ye
Friday, July
Administra

Dark Web vs. Deep Web

The deep web is a section of the internet that cannot be indexed by web crawlers. The dark web is a subsegment of the deep web that can only be accessed with special tools, such as the Tor browser.



Surface Web vs. Deep Web vs. Dark Web

While the deep web is chiefly used for legitimate day-to-day online activities, the dark web is mainly anonymous and known as a haven for conducting illegal transactions.

commonly

[How Are You
End-of-Sup](#)

With Micro
support in
your team
planning ...

[RDC forcin](#)

This has ju
last week.
in again lik
ch...

[Check c](#)

Adobe

**Flawl
in fev**

[Try nov](#)

Table of C

- [Dark W](#)
- [What Is](#)
- [What Is](#)
- [5 Key D](#)
[Deep W](#)

What Is the Dark Web?

The dark web is a subsection of the deep web including websites that one can only **access through purpose-built web browsers**. Some estimates mark the extent of the dark web as being much smaller than that of the surface web (which is the regular internet we use every day). However, it is challenging to measure how widespread the dark web is due to its decentralized and obscure nature.

Very few regular users will ever interact with the dark web. While the deep web usually requires just a [username and password](#) to be accessed (think of your email inbox), the dark web cannot be reached without the right software or hardware.

The architecture of the dark web features some **key elements** that make it an anonymous sanctuary for censored activities.

- Due to their unique registry operator, websites on the dark web are inaccessible by regular web browsers such as Google Chrome and Mozilla Firefox.
- Web crawlers cannot index the content hosted on the dark web. [Network security tools](#) such as encryption and firewalls prevent these search tools from discovering these websites.
- Access to dark web content is restricted with the help of virtual traffic tunnels through randomized network architecture.

The layman associates the dark web with illegal content and criminal activities such as trading illicit products and services. While this is mainly true, this online framework also has applications for legitimate entities. For instance, journalists in autocratic nations can use the dark web to pass information to their colleagues in other parts of the world.

The dark web was originally a domain exclusively used by cybercriminals and governments. Today, this is no longer true—[advanced encryption technologies](#) have made the anonymization of web surfing a hassle-free affair for regular users. The Tor browser is a popular tool for accessing the dark web.

Most enterprises do not have a direct use case for the dark web. However, cybersecurity organizations could benefit from indirect participation in discussions regarding hacking and exploit trading that regularly takes place on the dark web. This would give them insights into yet-unknown vulnerabilities and allow them to gain knowledge of exploits before they can turn into widespread cyber threats.

See More: [What Is a Secure Web Gateway? Definition, Benefits, and Best Practices](#)

What Is the Deep Web?

Unlike the dark web, which is deliberately obscured by layers of technology, the deep web exists just **below the surface web**. The majority of the deep web consists of regular websites that require users to create an account before they can be accessed.

If the surface web is the visible part of an iceberg above water, the deep web is the part submerged beneath – much larger but hidden from plain view. Some people use the terms ‘dark web’ and ‘deep web’ interchangeably; however, significant portions of the deep web are completely legal and safe to use.

A majority of the web consists of databases and intranets. The former includes privately protected file collections that one cannot access without the correct credentials. The latter includes internal networks for governments, educational facilities, and corporations. The ‘members only’ parts of public platforms are also a part of the deep web.

All web pages not indexed by web crawlers are considered to be a part of the deep web. The content is generally more secure and clean than that of the surface web. This is because deep web content is usually well-maintained. Security tools such as [firewalls](#) help in this endeavor.

Simple examples of deep web content include financial data, social security databases, email inboxes, social media, medical documentation, legal files, blog posts that are pending review and web page redesigns that are in progress. These pages are mostly obscured from the surface web to secure user data and privacy rather than any nefarious purpose.

However, the deep web is not entirely devoid of danger. Some portions of the deep

web allow users to overcome legal restrictions to access content that is not lawfully available in their geographical location. It is even possible to illegally download movies, music, and other digital media without paying for it. Naturally, these lawless segments of the deep web are rife with malware and other cyber threats.

While the content on the dark web has the potential to be more dangerous, this content is usually walled off from regular users. However, it is entirely possible for regular users to accidentally come across harmful content while browsing the deep web, which is much more easily accessible. This makes deep web security important for individuals and enterprises alike.

[See More: What Is Unified Threat Management \(UTM\)? Definition, Best Practices, and Top UTM Tools for 2021](#)

5 Key Differences Between the Dark and Deep Web

The terms dark web and deep web are perceived to be linked with illegal and otherwise suspicious activity; however, a vast difference exists between the two.

Outlined below are the top five differences between the dark and deep web.

1. Scope and Operations	
Dark Web	Deep Web
As a subsection of the deep web, the dark web cannot be indexed by web crawlers. However, there is an important difference: while the deep web content does not show up in the search results list, it is otherwise	The deep web is much broader in scope than the dark web. This umbrella term covers all the parts of the online world that are not accessible by web search engines such as Google, Yahoo, Bing, or DuckDuckGo. Unlike the dark web, which majorly hosts content that is illegal or otherwise restricted in nature, the deep web hosts a wide range

safe and can be accessed with

In nature, the deep web hosts a wide range

2. Size

Dark Web	Deep Web
<p>The dark web technically speaking, is a subsection of the deep web.</p> <p>However, there is no true way to gauge how vast and deep the dark web truly is.</p>	<p>It is easier to give an accurate estimate of the size of the deep web due to its public nature.</p> <p>More than 200,000 websites exist on the deep web.</p>
<p>Some experts peg the size of the dark web at approximately</p>	<p>The volume of public data on the deep web is 400 to 500 times greater than that of the surface web</p>

3. Access

Dark Web	Deep Web
----------	----------

Users **cannot ‘accidentally’ access** the dark web. Even if a cyberattack targets a user, it would be unlikely for the attack to have directly originated from the dark web. The tools to carry out the cyberattack may have been bought off a dark web marketplace, but the attacker would propagate the attack using mediums available on the standard web (such as email or chat).

No filters between users and the deep web. Any user with an internet-enabled device and the correct set of credentials **can access** a website on the deep web.

4. Applications

Dark Web	Deep Web
The main application of the dark web is to provide anonymity to both website owners and visitors. The dark web helps obscure websites that do not wish to be on the regular internet, where they could be monitored.	As discussed above, the deep web is visited regularly by most internet users. Listed below are three key applications of the deep web: Intranets , or internal networks used by companies and academic institutions, cannot be accessed by the public. They require access to a specific VPN service and credentials before they can be

5. Security

Dark Web	Deep Web
<p>The dark web is constantly evolving, with new marketplaces and forums for criminal activity cropping up frequently. Organizations are at risk of data theft by cybercriminals. Stolen data often ends up on the dark web for sale, giving cybercriminals the incentive to target organizations with sensitive customer data (such as financial institutions)</p>	<p>The deep web is largely secure and user-friendly. Accessing websites here is a safe, routine process. However, maintaining security procedures is critical even though these websites are legitimate.</p>

See More: [What Is Threat Modeling? Definition, Process, Examples, and Best Practices](#)

Takeaways

The dark web has numerous legitimate uses but is still home to various criminal activities. Conversely, the deep web is a regular part of the online experience for almost every internet user.

As a deep web subsection, the dark web shares many characteristics. However, noteworthy differences exist in operation, scope, size, access methodology, applications, and security.

Did this article help you understand the differences between the dark web and the deep web? Share your thoughts on [LinkedIn](#), [Twitter](#), or [Facebook](#)!

MORE ON SECURITY

- [What Is Phishing? Definition, Types, and Prevention Best Practices](#)
- [Top 10 Cyber Threat Intelligence Tools in 2022](#)
- [Top 10 Threat Intelligence Platforms in 2022](#)
- [What Is Security Information and Event Management \(SIEM\)? Definition, Architecture, Operational Process, and Best Practices](#)
- [Top 10 SIEM Solutions in 2022](#)

Cybersecurity

Share This Article:



Hossein Ashtari

Technical Writer

in f

Interested in cutting-edge tech from a young age, Hossein is passionate about staying up to date on the latest technologies in the market and writes about them regularly. He has worked with leaders in the cloud and IT domains, including Amazon—creating and analyzing content, and even helping set up and run tech content properties from scratch. When he's not working, you're likely to find him reading or gaming!