

# FAQ for Beazley Open Port & Vulnerability Assessments

**As your cyber insurer, Beazley continuously monitors the global threat landscape to proactively help clients mitigate cyber risk exposures.**

**When significant cyber-risks or vulnerabilities are identified, Beazley cross-references that data with publicly available information about servers and other devices on the internet and is then able to identify IP addresses and organisations that are potentially at risk.**



# FAQ for Beazley Open Port & Vulnerability Assessments

As your cyber insurer, Beazley continuously monitors the global threat landscape to proactively help clients mitigate cyber risk exposures.

When significant cyber-risks or vulnerabilities are identified, Beazley cross-references that data with publicly available information about servers and other devices on the internet and is then able to identify IP addresses and organisations that are potentially at risk.



## What is a port?

Computer applications and services usually communicate using numbered ports (in total there are 65,535 ports). Each port number is related to a specific application or service that allows computers to differentiate between the different kinds of traffic that may travel over a single network connection. As an example, web traffic generally travels over port 80 and email using the Internet Message Access Protocol (IMAP) protocol uses port 993. Microsoft's Remote Desktop Protocol (RDP) on port 3389.

[What is a port?](#)

[What is an open port?](#)

[What is a vulnerability?](#)

[Why is Beazley looking for open port and vulnerabilities?](#)

[How does Beazley discover my infrastructure?](#)

[What does Beazley do with my infrastructure?](#)

[Does Beazley track all open ports?](#)

[Does Beazley track all vulnerabilities?](#)

[What can I do?](#)



# FAQ for Beazley Open Port & Vulnerability Assessments

As your cyber insurer, Beazley continuously monitors the global threat landscape to proactively help clients mitigate cyber risk exposures.

When significant cyber-risks or vulnerabilities are identified, Beazley cross-references that data with publicly available information about servers and other devices on the internet and is then able to identify IP addresses and organisations that are potentially at risk.



## What is an open port?

An open port is a port that is configured to accept packets. For an open port to be visible on the internet (to Beazley or indeed anyone else), an organisation's firewall must be configured to allow connections from the public internet through that open port.

[What is a port?](#)

[What is an open port?](#)

[What is a vulnerability?](#)

[Why is Beazley looking for open port and vulnerabilities?](#)

[How does Beazley discover my infrastructure?](#)

[What does Beazley do with my infrastructure?](#)

[Does Beazley track all open ports?](#)

[Does Beazley track all vulnerabilities?](#)

[What can I do?](#)



# FAQ for Beazley Open Port & Vulnerability Assessments

As your cyber insurer, Beazley continuously monitors the global threat landscape to proactively help clients mitigate cyber risk exposures.

When significant cyber-risks or vulnerabilities are identified, Beazley cross-references that data with publicly available information about servers and other devices on the internet and is then able to identify IP addresses and organisations that are potentially at risk.



## What is a vulnerability?

A vulnerability is a weakness or flaw in computer software that could allow an attacker to use the software in a way not intended by its creator, usually in a malicious way to perform unauthorised actions in a computer system. When vulnerabilities are discovered they are usually added to a public list of Common Vulnerabilities and Exposures (CVE) and they are given a CVE ID or number (in the format CVE-2021-12345).

[What is a port?](#)

[What is an open port?](#)

[What is a vulnerability?](#)

[Why is Beazley looking for open port and vulnerabilities?](#)

[How does Beazley discover my infrastructure?](#)

[What does Beazley do with my infrastructure?](#)

[Does Beazley track all open ports?](#)

[Does Beazley track all vulnerabilities?](#)

[What can I do?](#)



# FAQ for Beazley Open Port & Vulnerability Assessments

As your cyber insurer, Beazley continuously monitors the global threat landscape to proactively help clients mitigate cyber risk exposures.

When significant cyber-risks or vulnerabilities are identified, Beazley cross-references that data with publicly available information about servers and other devices on the internet and is then able to identify IP addresses and organisations that are potentially at risk.



## Why is Beazley looking for open port and vulnerabilities?

Many cyber attackers conduct regular, automated scanning of the entire internet for computers that have open ports and whether or not a service (e.g. email, web, FTP, remote access) is listening on that port. When an organisation exposes certain services or ports to the internet, attackers will repeatedly query that port and attempt to exploit potential vulnerabilities in any services or software they find. These vulnerabilities may allow them to obtain access to the network behind that exposed port and conduct further malicious activity.

[What is a port?](#)

[What is an open port?](#)

[What is a vulnerability?](#)

[Why is Beazley looking for open port and vulnerabilities?](#)

[How does Beazley discover my infrastructure?](#)

[What does Beazley do with my infrastructure?](#)

[Does Beazley track all open ports?](#)

[Does Beazley track all vulnerabilities?](#)

[What can I do?](#)



# FAQ for Beazley Open Port & Vulnerability Assessments

As your cyber insurer, Beazley continuously monitors the global threat landscape to proactively help clients mitigate cyber risk exposures.

When significant cyber-risks or vulnerabilities are identified, Beazley cross-references that data with publicly available information about servers and other devices on the internet and is then able to identify IP addresses and organisations that are potentially at risk.



## How does Beazley discover my infrastructure?

Beazley and its professional advisers use an organisation's main domain name together with the WHOIS database, certificate data and passive Domain Name System (DNS) records to establish IP address ranges that we believe to be relevant to each of our insureds.

[What is a port?](#)

[What is an open port?](#)

[What is a vulnerability?](#)

[Why is Beazley looking for open port and vulnerabilities?](#)

[How does Beazley discover my infrastructure?](#)

[What does Beazley do with my infrastructure?](#)

[Does Beazley track all open ports?](#)

[Does Beazley track all vulnerabilities?](#)

[What can I do?](#)



# FAQ for Beazley Open Port & Vulnerability Assessments

As your cyber insurer, Beazley continuously monitors the global threat landscape to proactively help clients mitigate cyber risk exposures.

When significant cyber-risks or vulnerabilities are identified, Beazley cross-references that data with publicly available information about servers and other devices on the internet and is then able to identify IP addresses and organisations that are potentially at risk.



## What does Beazley do with my infrastructure?

Beazley does not scan your infrastructure. Beazley uses a variety of long-standing public services (e.g. Censys and Shodan) that track information on services exposed to the public internet and match that data to the IP ranges that we believe are relevant to our insureds' infrastructure.

[What is a port?](#)

[What is an open port?](#)

[What is a vulnerability?](#)

[Why is Beazley looking for open port and vulnerabilities?](#)

[How does Beazley discover my infrastructure?](#)

[What does Beazley do with my infrastructure?](#)

[Does Beazley track all open ports?](#)

[Does Beazley track all vulnerabilities?](#)

[What can I do?](#)



# FAQ for Beazley Open Port & Vulnerability Assessments

As your cyber insurer, Beazley continuously monitors the global threat landscape to proactively help clients mitigate cyber risk exposures.

When significant cyber-risks or vulnerabilities are identified, Beazley cross-references that data with publicly available information about servers and other devices on the internet and is then able to identify IP addresses and organisations that are potentially at risk.



## Does Beazley track all open ports?

Beazley does not track all 65,535 ports or services that might be open to the public internet.

Beazley is concerned about those ports or services that permit remote access into an environment, for example Virtual Network Computing (VNC) on port 5900 and Microsoft's Remote Desktop Protocol (RDP) on port 3389.

Beazley also tracks services that are legitimate within an organisation but are dangerous to expose to the public internet such as the Samba/SMB protocol (usually found on ports 139 and 445).

[What is a port?](#)

[What is an open port?](#)

[What is a vulnerability?](#)

[Why is Beazley looking for open port and vulnerabilities?](#)

[How does Beazley discover my infrastructure?](#)

[What does Beazley do with my infrastructure?](#)

[Does Beazley track all open ports?](#)

[Does Beazley track all vulnerabilities?](#)

[What can I do?](#)



# FAQ for Beazley Open Port & Vulnerability Assessments

As your cyber insurer, Beazley continuously monitors the global threat landscape to proactively help clients mitigate cyber risk exposures.

When significant cyber-risks or vulnerabilities are identified, Beazley cross-references that data with publicly available information about servers and other devices on the internet and is then able to identify IP addresses and organisations that are potentially at risk.



## Does Beazley track all vulnerabilities?

There are thousands of CVEs affecting hundreds of software platforms and Beazley does not track all of these. Beazley does track End of Life (EOL) software that is visible on the public internet because that is software that has stopped receiving critical updates and patches and is therefore highly susceptible to attack. Beazley also tracks unpatched firewalls, remote access gateways, virtual private networks (VPNs) and web servers that are frequent, and favourite, targets and are the causes of many recent and very high-profile compromises.

[What is a port?](#)

[What is an open port?](#)

[What is a vulnerability?](#)

[Why is Beazley looking for open port and vulnerabilities?](#)

[How does Beazley discover my infrastructure?](#)

[What does Beazley do with my infrastructure?](#)

[Does Beazley track all open ports?](#)

[Does Beazley track all vulnerabilities?](#)

[What can I do?](#)



# FAQ for Beazley Open Port & Vulnerability Assessments

As your cyber insurer, Beazley continuously monitors the global threat landscape to proactively help clients mitigate cyber risk exposures.

When significant cyber-risks or vulnerabilities are identified, Beazley cross-references that data with publicly available information about servers and other devices on the internet and is then able to identify IP addresses and organisations that are potentially at risk.



## What can I do?

Due to Beazley's market-leading position in the cyber insurance industry, we have a vast amount of incident data that demonstrates clearly the risks of exposing certain ports and/or un-patched software onto the public internet. We know that certain protocols and vulnerable software may provide an attacker with direct access to trusted devices within a network. Beazley therefore recommends that if remote access to services is required, this should be implemented via a secure gateway and/or secured behind a VPN such that these resources are not directly visible to attackers.

[What is a port?](#)

[What is an open port?](#)

[What is a vulnerability?](#)

[Why is Beazley looking for open port and vulnerabilities?](#)

[How does Beazley discover my infrastructure?](#)

[What does Beazley do with my infrastructure?](#)

[Does Beazley track all open ports?](#)

[Does Beazley track all vulnerabilities?](#)

[What can I do?](#)

