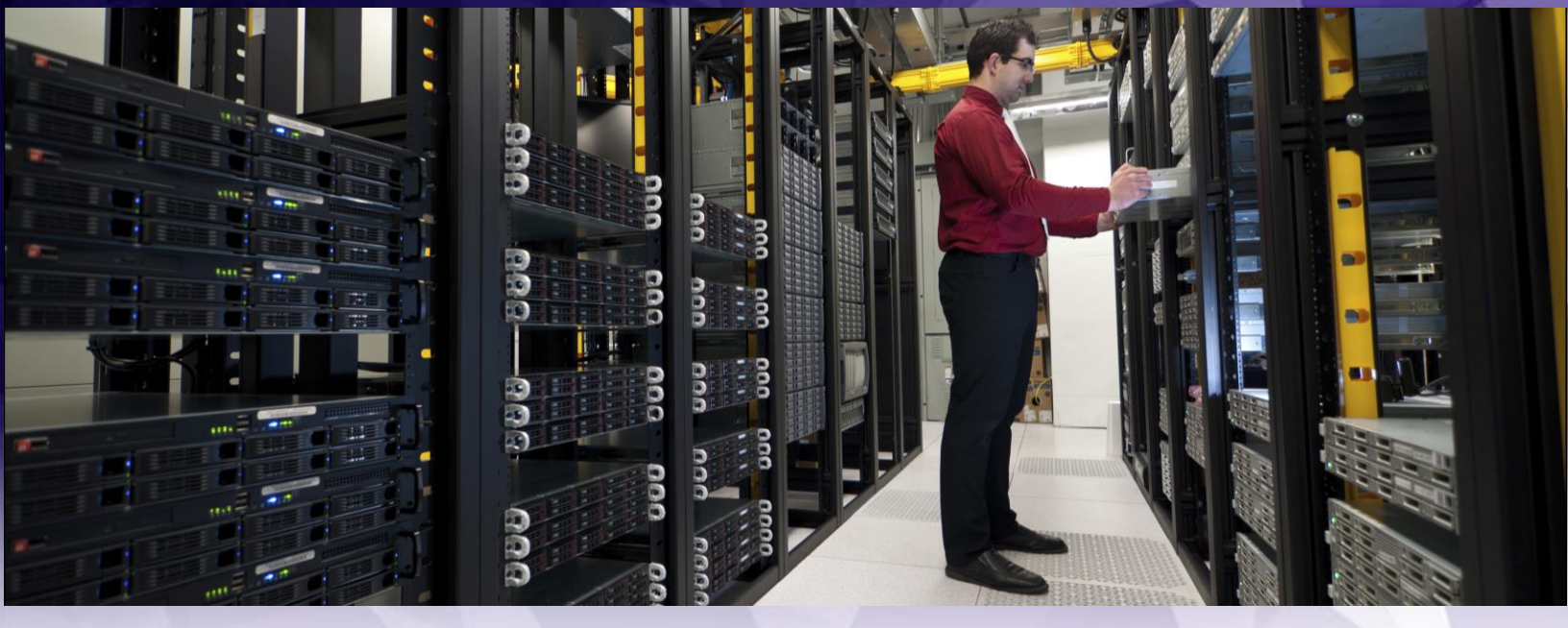
Datasheet.

Diamond IP DNS Firewall.

Protect your infrastructure from malware.



It all starts…and ends…with DNS.

Stop malware communications before they start. DNS is used by over 90% of malware according to Cisco. Our DNS firewall can help you shut down the initiation of malware communications.

Malware-infected devices typically rely on the domain name system (DNS) for communications. DNS helps malware locate the Internet address of its command center and can be used to exfiltrate sensitive information from your organization.

DNS ubiquity's double-edged sword.

Most enterprise networks freely permit DNS traffic through firewalls because DNS is the essential first step in Internet communications for every device, malware-infected or otherwise. Infected devices use DNS to lookup the IP address of the malware controller's command center, typically a file or webserver used to communicate instructions or software to distributed malware. The malware then serves as a remote "bot" implanted within your enterprise network to execute commands from the attacker's command center.

Cisco Security Research findings indicate that 68% of organizations don't monitor their recursive DNS. Monitor and protect your recursive DNS with the BT DNS firewall.
Source: Lystrup, Owen. Cisco Security Report, 21 January, 2016.

Advanced Persistent Threats.

DNS services are crucial to the simple navigation of the web in translating www addresses into IP addresses. But DNS is also useful for website administrators in that they can change their servers' IP addresses and simply update DNS to reflect the new name-to-address mapping.

Malware operators exploit these and other DNS capabilities to freely issue DNS queries to locate command centers, to exfiltrate information, and to change or "flux" their IP addresses to avoid shutdown through IP address filtering should they be detected. This and other evasive techniques enable malware to persist within networks and stealthily execute attacks on behalf of the attacker.

Actionable intelligence.

The BT Diamond IP DNS Firewall protects your network from the inception of malware communications attempts. It enables you to block or redirect queries for known malware and other undesirable domains to prevent infected devices from obtaining software or attack instructions. BT Diamond IP provides a continually updated firewall feed for your recursive DNS servers to enable you to protect your network and to identify and mitigate infected devices.

Datasheet.

Diamond IP DNS Firewall.

Multi-faceted filters.

BT Diamond IP DNS firewall enables you to not only protect your users from access to known malware domains and those of ill-repute. You can also customize rules to filter DNS responses for queries to other undesirable sites such as those known to contain adult, political or radical content. You have control for network protection and acceptable use policy governance.

Firewall policies.

BT Diamond IP provides a variety of triggers based on known bad actor domains and IP addresses from which you can enable or disable policies. You can select firewall policies to apply for each category you enable including:

- Drop the response to the client
- Respond with “not found” (NXDOMAIN)
- Respond with “no data received” (NODATA)
- Redirect to a given IP address, e.g., a captive portal
- Respond with the “truncated” header bit to trigger TCP
- Pass-through (“whitelist”)

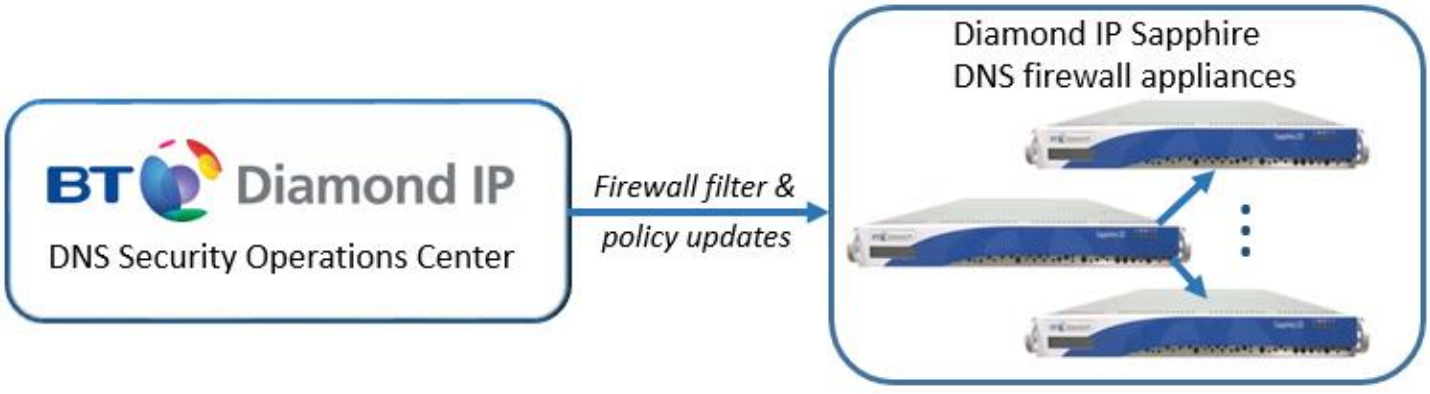
Actionable reporting.

Should a device querying your DNS server request a domain for which a policy exists, logging alerts notify you of the querier IP address. This enables you to track down the offending device to investigate malware infestation and to apply remediation tactics. Logging to our centralized facility also enables history reporting and tracking.

DNS firewall benefits.

The BT Diamond IP DNS Firewall includes a simple subscription service with frequent updates supporting the following benefits:

- Enhance your overall network security implementation. DNS is the first step in communications and serves as a prime opportunity to inhibit malicious communications.
- Timely firewall updates. Attackers move quickly to devise new attack vectors. Our firewall feed provides updates several times daily to keep your policies fresh.
- Prevent malware callbacks. With over 91% of malware using DNS in some manner, controlling access at the DNS layer can inhibit the effectiveness of such malware.
- Identify infected devices. With policy logging and reporting you can quickly identify devices issuing queries for which firewall policies apply for rapid remediation.
- Easily customize your firewall. Many firewall services offer a static feed over which you have no control. Our firewall service enables you to configure filters and associated policies to better secure your network.
- Simple implementation. Our subscription feed incorporates standard DNS protocol messages with digital signing to securely keep firewall information updated without requiring proprietary communications and associated Internet firewall configuration changes.



Find out more at:

+1 610 321 9000 www.bt.com/diamondip