tbl networks
technology. redefined.

# DNS PROTECTION

## Your First Line of Defense

As a secure internet gateway, **DNS Protection** provides the first line of defense against threats on the internet wherever users go.

## WHY DNS PROTECTION

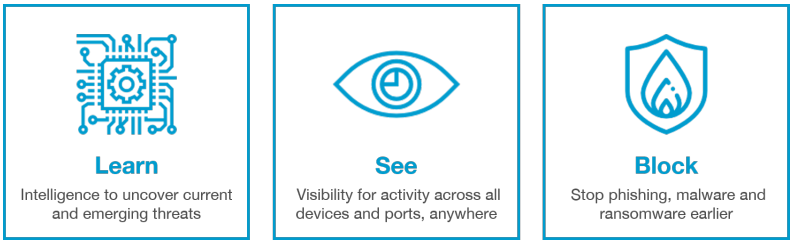
**DNS Protection** features deliver complete visibility into internet activity across all locations, devices, and users, and block threats before they ever reach your network or endpoints. As a cloud-delivered, open platform, **DNS Protection** solutions integrate easily with your existing security stack and deliver live threat intelligence about current and emerging threats.

By analyzing and learning from internet activity patterns, **DNS Protection** solutions automatically uncover attacker infrastructure staged for attacks and proactively block requests to malicious destinations before a connection is even established — without adding any latency for users. You can stop phishing and malware infections earlier, identify already infected devices faster, and prevent data exfiltration.

### Enforcement built into the foundation of the internet

When a DNS request is received, **DNS Protection** capabilities use intelligence to determine if the request is safe, malicious or risky — meaning the domain contains both malicious and legitimate content. Safe and malicious requests are routed as usual or blocked, respectively.

Risky requests are routed to our cloud-based proxy for deeper inspection where it's determined if a URL is malicious. Our proxy also inspects files attempted to be downloaded from those risky sites using anti-virus engines and Advanced Malware Protection. And, based on the outcome of this inspection, the connection is allowed or blocked.




## FEATURES & BENEFITS

### Mitigate remediation costs and breach damage

Because **DNS Protection** is the first line of defense, security teams will have fewer malware infections to remediate and threats will be stopped before they cause damage.

### Reduce the time to detect and contain threats

**DNS Protection** features contain command and control callbacks over any port or protocol and provide real-time reports on that activity.

### Increase visibility into internet activity across all locations and users

**DNS Protection** features provide crucial visibility for incident response and give you confidence that you're seeing everything.

### Identify cloud apps used across the business

**DNS Protection** features provide visibility into sanctioned and unsanctioned cloud services in use across the enterprise, so you can uncover new services being used, see who is using them, and identify potential risk.