CYREN

# Cyren DNS Security für öffentliche WLANs

Enterprise Security SaaS

## Schützen Sie Ihre Gäste, Kunden und Ihr Unternehmen.

CYREN DNS Security

**Schützen Sie Benutzer vor Bedrohungen und sperren Sie unangemessene Inhalte mithilfe eines Cloud-Dienstes, der einfach bereitzustellen und zu verwalten ist.**

Wenn öffentlicher Internetzugang bereitgestellt wird, ist es sehr wichtig, die Risiken zu berücksichtigen, denen Benutzer im Internet ausgesetzt sind, und Ihre Interessen bei der Durchsetzung akzeptabler Nutzungsrichtlinien zu wahren. Wenn Sie die potenzielle Anzeige unangemessener oder verletzender Inhalte an einem öffentlichen Ort oder auf Ihrem Betriebsgelände gestatten (und auch wenn solche Inhalte als Suchergebnisse angezeigt werden), können Sie rechtlich haftbar gemacht werden und Ihr Ruf kann darunter leiden.

Unternehmen müssen Ihrer Sorgfaltspflicht nachkommen, um illegale oder unerwünschte Handlungen über den von ihnen bereitgestellten Internetzugang zu stoppen. Bedrohungen wie Malware oder Phishing-Websites sind gefährlich, und zwar nicht nur für die Besucher, sondern evtl. auch für das Host-Unternehmen. Die Bereitstellung von Cyren DNS Security in einem öffentlichen Netzwerk lässt Sie ruhiger schlafen. Besucher und Ihre Organisation werden vor den schlimmsten Internetbedrohungen von heute geschützt. Dies umfasst die absolute Durchsetzung von Safe Search-Richtlinien und sowie Ihrer Richtlinien zur akzeptablen Nutzung („Acceptable Use Policy").

**Einhaltung von Acceptable Use Policies**—Anbieter von WLAN-basiertem Internetzugang für Gäste oder die Öffentlichkeit können mithilfe von Cyren DNS Security regulatorische, kundenorientierte oder Unternehmensrichtlinien für die akzeptable Nutzung des Internets durchsetzen.

**Einfache Integration**—Leiten Sie Ihre DNS-Abfragen an die Cyren-Cloud weiter, wo sie verarbeitet werden. Sie können die Richtlinien dadurch unmittelbar durchsetzen. Die Verwaltung von Hotspots und Richtlinien ist mit unserem intuitiven Web-Dashboard denkbar einfach.

**Mehrschichtige Sicherheit**—Cyren DNS Security wendet aktuelle Cyber-Intelligence an, um Benutzer vor neuen und kommenden Bedrohungen zu schützen. Dazu verwendet Cyren DNS-Filterung für HTTP/S und Cyber-Intelligence, die aus der Analyse von 25 Milliarden Internet-Transaktionen täglich von mehr als 1,3 Milliarden Benutzern in über 180 Ländern abgeleitet wird.

**„Best-of-Breed"-URL-Filterung**—Cyren ist weltweit führend bei der Echtzeit-URL-Filterung, klassifiziert kontinuierlich URLs und pflegt 64 URL-Kategorien in einer Echtzeit-Datenbank mit durchschnittlich mehr als 150 Millionen URLs. Mit Cyren WebSecurity können Netzwerkanbieter die Anwendung dieser Datenbank direkt in einfach zu konfigurierenden Richtlinien für öffentliche WLAN-Dienste und Netze verwalten.

**Optimieren Sie Ihre Bandbreitennutzung**—Cyren WebSecurity ermöglicht Netzwerkanbietern das Formen und Filtern des Internet-Datenverkehrs. Anbieter können die Netzwerknutzung optimieren und kontinuierlich eine hervorragende Benutzererfahrung bieten.

### Vorteile von Cyren DNS Security in der Cloud

- Pay-as-you-go-SaaS-Abonnementmodell mit flexiblen orts- oder benutzerbasierten Preisen.
- Schützen Sie Ihre Benutzer und Gäste mit der branchenweit größten Sicherheits-Cloud—Cyren verarbeitet täglich mehr als 25 Milliarden Transaktionen.
- Jedes mit Ihrem öffentlichen oder Gäste-Netzwerk verbundene Gerät ist vor unangemessenen Inhalten, Malware, Phishing und fortgeschrittenen Bedrohungen geschützt, egal, ob es sich um einen Desktop-Rechner handelt, der öffentlich verwendet werden kann, oder um Laptops, Smartphones und Tablets, die mit Ihrem Gäste-Netzwerk verbunden sind.
- Bereitstellung in wenigen Minuten—verweisen Sie einfach Ihr DNS und wählen Sie eine vorformatierte Richtlinienvorlage.
- Einfache Verwaltung mehrerer Standorte—unsere Cloud-Plattform wendet Ihre Richtlinien einheitlich über verschiedene Standorte an oder ermöglicht ihre einfache Anpassung.

www.Cyren.com

sales@cyren.com

**25 Mrd.**
Sicherheitsabfragen pro Tag

**1,3 Mrd.**
Geschützte Nutzer

**300 Mio.**
Abgewehrte Gefahren pro Tag

CYREN DNS Security

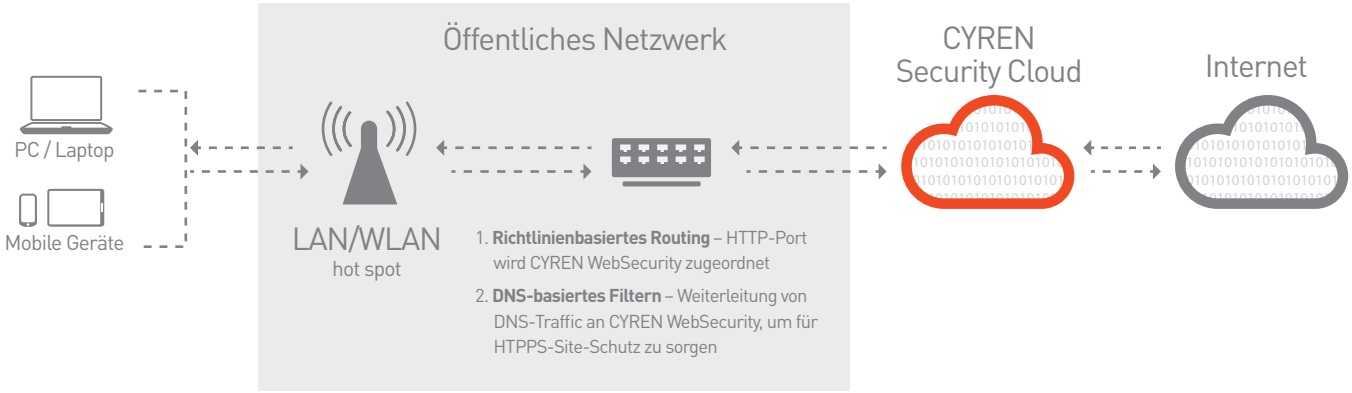
## Funktionen von Cyren DNS Security für öffentliche WLANs

**DNS-basierte Richtliniendurchsetzung**—Durch die Anwendung von Richtlinien auf Benutzer-Browsing-Aufforderungen auf DNS-Ebene sorgt Cyren DNS Security für einen strikten Datenschutz bei den Inhalten des Benutzer-Datenverkehrs. Wird die anfängliche Aufforderung zum Zugriff auf eine bestimmte URL genehmigt, gelangt der Benutzer direkt zur Ziel-Website. Sein Datenverkehr wird dann nicht weiter untersucht. Dieser Ansatz gewährleistet auch, dass der Benutzer keine Verzögerungen beim Ansteuern der gewählten Website erfährt, weil es bei der Transaktion keinen „Mittelsmann" gibt.

**Flexible URL-Filterung und Kategorisierung**—Cyren WebSecurity bietet standardmäßig 64 URL-Kategorien (einschließlich fortgeschrittener Bedrohungen), die so organisiert sind, dass eine optimale Analyse und Kontrolle gewährleistet wird. Wir bieten „Out-of-the-Box"-Benutzerrichtlinienvorlagen, um einen schnellen Start zu ermöglichen. Diese können Sie wie erforderlich mit Ihren eigenen Kategorien für White- und Blacklists anpassen und auf Wunsch nach Tageszeit und Ort variieren.

**Kontrollen anhand des Datei- und Datenverkehrstyps**—Bei Verwendung im Proxy-Bereitstellungsmodell für HTTP-Datenverkehr können Sie mit Cyren DNS Security die Hotspot-Bandbreite verwalten, indem Sie die Arten und Größen der Dateien steuern, die heruntergeladen werden können, sowie die URLs, die besucht werden können.

## Funktionsweise




Benutzer, die auf öffentliche Netzwerke zugreifen, werden durch Standard-Netzwerk-Konfigurationen zu Cyren WebSecurity Points-of-Presence in unserer globalen Sicherheits-Cloud geleitet. Die Dienstbereitstellung ist einfach und erfolgt fast sofort:

1. Verweisen Sie Ihr DNS auf die Cyren-Cloud.
2. Erstellen Sie in der Web-Admin-Konsole einen Ort und weisen Sie eine vorformatierte Benutzerrichtlinie zu. Sie können aber auch schnell verschiedene Kategorien kombinieren, um eine benutzerdefinierte Richtlinie zu erstellen.
3. Wahlweise können Sie Ihren HTTP-Port Cyren DNS Security zuordnen und Ihren Datenverkehr in die Cyren-Sicherheits-Cloud leiten.

Wenn Sie damit fertig sind, können Sie mithilfe der Administrationskonsole von Cyren DNS Security die öffentlichen IP-Adressen Ihrer Routing-Geräte in das System eingeben und die bevorzugte Acceptable Use Policy auswählen, die auf die jeweilige Adresse angewendet werden soll. Benutzer sind jetzt vor Cyberbedrohungen und einer unangemessenen Internet-Nutzung oder entsprechenden Inhalten geschützt.