UltraDNS Detection and Response (DDR)
The Protective DNS Resolution Service

It takes the most proactive security to effectively support the high speed of business. Vercara uses authoritative knowledge of attacker infrastructure and unrivaled domain-based intelligence to augment your existing security solutions, proactively protect your organization, and mitigate threats in real time.

Our combination of infrastructure expertise and communication pattern analysis gives you an instant and reliable source of truth to mitigate threats in real time and to enforce corporate internet usage policies. UltraDDR is a cloud-based DNS-layer cyber threat detection and response service that identifies and prevents attacks before they happen for devices inside and outside your network. Fast and flexible deployment support WFH/hybrid work models and protects devices of all kinds, including servers, mobile, IoT, and more.

BENEFITS

- Block bad domains, IP addresses and name servers with security, reliability, and performance

- Stop ransomware, phishing, and supply chain attacks before they start

- Global network of secure recursive servers

- Enforce corporate internet usage standards with category-based content web filtering and block/allow lists

- Deliver enterprise-wide protection at work, at home, and on the go

Block bad domains, IP addresses and name servers with security, reliability, and performance

VERCARA

Securing the Online Experience

A New Level of Protection

Uses years of historical domain data combined with real-time analysis of communication patterns to provide unrivaled threat mitigation by blocking command and control (C2) communication used by malware, ransomware, phishing, and supply chain attacks. UltraDDR works in concert with your existing endpoint and network controls to provide an additional layer of protection, correlation and management. Easy-to-use APIs allow you to seamlessly leverage SIEM, SOAR, firewalls, anti-malware, or other security solutions.

Zero-Day Detection

Adaptive policy engine that uses years of historical domain data combined with real-time analysis of communication patterns to identify and prevent attacks before they start. This ensures that users, devices, or servers don't communicate with adversary infrastructure.

Comply with Acceptable Use Policies

Customize and easily enforce company-wide policies at the user level to improve productivity and ensure global workforces aren't distracted by non-compliant sites.

Easy Deployment

Simply forward your recursive DNS traffic to the NSS platform to enforce corporate internet usage standards with a cloud-based, managed solution that ensures performance and security standards. There is no need for on-premise appliance deployments or additional configurations, saving time and money—all with the added benefits of a web-based portal, detailed reporting and industry leading SLAs.

DDoS Protection

UltraDDoS Protect provides built in DNS DDoS protection that quickly defends against attacks towards the UltraDDR network and ensures that DNS resolution availability is not compromised.

Fast Performance

Quickly resolves queries through a highly reliable, global DNS infrastructure. The UltraDDR nodes are deployed in 27 data centers worldwide providing near zero-latency of query response.

Support

24x7x365 support from a team of dedicated DNS experts.

ULTRADDR SUPPORTS:

- Blocking of harmful websites and C2 domains
- Category-based blocking
- Real-time decision policies
- DoT and DoH support
- IPv6 and DNSSEC support
- DDoS mitigation by UltraDDoS Protect

VERCARA *Securing the Online Experience*

Find more information at:

vercara.com

Call USA: +1 (844) 929 - 0808
Call EMEA: +44 808 175 1189