UltraDDR: UltraDNS detection and response

A cutting-edge protective DNS resolution service

Every online interaction starts with a DNS query. UltraDDR provides a critical line of defense at the DNS layer, ensuring the integrity of all online activity.

DigiCert UltraDDR takes a proactive approach to threat detection and response, helping stop attacks in real time while safeguarding users in even the most vulnerable situations.

Our combination of infrastructure expertise and communication pattern analysis offers an instant and reliable source of truth. Rather than relying on a static list of previously identified bad actors, UltraDDR uses artificial intelligence (AI) and machine learning (ML) to instantly capture and block new nefarious communication and behavior patterns.

Unlike traditional threat intel feeds, DNS firewalls, and DNS web filtering, our approach significantly reduces the burden of manual intervention and remediation of compromised devices. A fast and flexible deployment supports BYOD and WFH/hybrid models while protecting a wide range of devices, including servers, mobile and IoT devices, and POS systems.

For incident response and security teams:

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

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

Intercept malicious traffic before it breaches your environment, regardless of the device it originates from.

Enforce acceptable usage policies with category-based web filtering and customized block and allow lists.

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

Detect and block nefarious connections and threat actors the very first time they appear.

Product capabilities and features:

A new level of protection

ML and AI inform the decision engine that blocks DNS resolution of malicious domains during recursive DNS resolution, including domains that try to impersonate your own with similar symbols.

Real-time intelligence and notifications

A live audit of DNS logs offers full visibility into the activity on your network, as well as insights into exactly which device has been targeted. UltraDDR also creates a log entry every time a new hostname is blocked and can send notifications to users of the system.

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.

DDoS protection

Built-in DDoS protection quickly defends against attacks toward the UltraDDR network and ensures that DNS resolution availability is not compromised.

Easy deployment

Simply forward your recursive DNS traffic to the UltraDDR platform. Easy-to-use APIs allow you to seamlessly integrate with SIEM, SOAR, firewalls, antimalware, or other security solutions.

There's 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.

Enforce 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.

Support

24/7/365 support from a team of dedicated DNS experts.

Fast performance

Quickly resolve queries through a highly reliable, global DNS infrastructure.

UltraDDR nodes are deployed in 27 data centers worldwide, providing near zero-latency of query responses.

Protect employees wherever they are

Agent software is available for Windows and MacOS. The agents leverage DNS over HTTPS (DoH) connections, safeguarding all users and ensuring their data is kept safe.