NEUVYS
TECHNOLOGIES

Delta Detection & Response (∆DR)

Closing the Gaps XDR Leaves Behind

Modern threats evolve fast. ∆DR adapts faster—providing comprehensive protection that stops threats in just 6 minutes.

∆DR is a fully managed, unified Security-as-a-Service platform that fuses a curated, composable stack with a 24x7 team of security experts who deliver continuous incident response—without the overhead or vendor lock-in. Our platform-plus-people model gives you enterprise-grade protection, simplified.

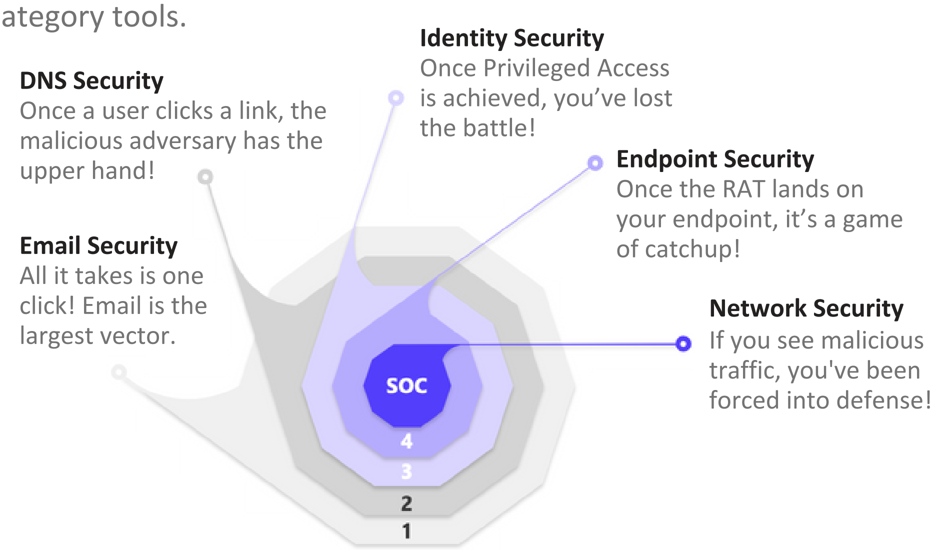
Next-Level Threat Detection & Response

∆DR eliminates the gaps caused by siloed tools and manual interpretation. It automatically collects and correlates data across your most critical attack surfaces—email, endpoints, servers, cloud workloads, and networks—giving our analysts the full context to detect, investigate, and respond faster and with greater precision.

By accelerating threat triangulation, ∆DR improves visibility, speeds response, and helps you stay ahead of attackers.

Adaptive, Evergreen Protection

Our modern, five-layered defense-in-depth approach delivers cyber resilience for today’s highly distributed world. Backed by a unified, composable tool stack—tested, curated, and managed by our experts—every layer and every threat vector is protected by best-in-category tools.



DNS Security
Once a user clicks a link, the malicious adversary has the upper hand!

Identity Security
Once Privileged Access is achieved, you’ve lost the battle!

Endpoint Security
Once the RAT lands on your endpoint, it’s a game of catchup!

Email Security
All it takes is one click! Email is the largest vector.

Network Security
If you see malicious traffic, you've been forced into defense!

KEY BENEFITS

- Adaptive protection that keeps pace with adversaries
- An evergreen tool stack—without the overhead
- Continuous Incident Response delivered by seasoned security experts
- Multi-layered defense that eliminates attackers’ time advantage
- Faster detection, response, and recovery across every threat vector
- Cross-layer correlation for faster, more accurate threat identification
- Enterprise-grade security—from 5 endpoints to 50,000
- Flexible adoption model—seamlessly integrate with your current tools and phase in as contracts expire
- 30-day onboarding
- 97% customer satisfaction

Editions

All ΔDR editions add value by ensuring that every threat is reviewed, acted upon, documented, responded to, and escalated as needed. Each product bundle builds on the previous edition.

ΔDR Essentials

Essentials is our foundational ΔDR edition with the core features to secure your environment across email, DNS, and endpoints. It is designed to meet the needs any sized organization that is ready to improve and modernize their distributed security posture.

ΔDR Essentials includes our world-class geo-redundant 24 x 7 x 365 Security Operations, eXtended Detection & Response with DNS security for cloud, on-prem and distributed workforces, post-gateway email security for advanced phishing protection, and includes Continuous Incident Response (CIR), Internal & External Posture Management, and Continuous Purple Teaming.

With the best threat intelligence in the industry, ΔDR Essentials sets up any organization to take the time advantage back from the bad actors.

Essentials edition features:

- **24 x 7 x 365 Security Operations**
- **eXtended Detection & Response** (XDR)
- **Autonomous EDR agents** apply real-time prevention and detection with or without cloud connectivity via Static AI
- **Fast recovery** gets users back and working in minutes without re-imaging and without writing scripts
- **Firewall & Device Policies** for network, USB, & Bluetooth device controls
- **Remote Shell** to connect to Windows, Mac, & Linux for support or troubleshooting
- **Endpoint Vulnerability Assessment** for OS & 3rd party apps
- **Rogue Device Visibility** for unmanaged endpoints or IoT devices
- **Breach & Attack Simulation** (BAS) leverage the simulated ATT&CKs to test your controls continuously
- **Dark Web Monitoring** for compromised passwords
- **DNS Security** on and off network for all endpoints
- **Selective Proxy** to block down bad domains and IPs
- **Web Filtering** can be performed by domain or category
- **Discover and block Shadow IT**
- Real-time defense against **Phishing** and **Spear Phishing**
- Real-time **Account Takeover/Impersonation** detection
- **BEC**, **CEO Fraud** prevention and **Domain Fraud** visibility
- **Identity Security Posture Management** (ISPM)

Stop ransomware and other fileless attacks with behavioral and strong autonomous remediation.

KEY FEATURES

- Unified platform integrates XDR, NDR, DNS, BEC, Internal/External & Cloud Posture security
- 24 x 7 x 365 Security Operations
- Supports a variety of form factors including physical, virtual, and VDI for both public and private clouds.
- Integrated threat intelligence and MITRE ATT&CK® threat indicators
- Continuous Incident Response
- Continuous Purple Teaming
- DNS & Email Security and threat detection/prevention
- Cloud storage security for M365 & GWS collaboration suites
- Multi-faceted telemetry for comprehensive and effective threat triangulation
- Global, multi-tenant SaaS platform. Highly available. Choice of locality (US, EU, APAC)
- Network sensors and endpoint agents are managed centrally by our SOC team
- Flexible administrative authentication and authorization (SSO, MFA, RBAC)
- Administration customizable to match your organizational structure
- Autonomous agents for Windows, Mac, Linux, and Kubernetes

∆DR Premium

Premium adds deeper DNS security and cloud storage protection for collaboration suites.

With the inclusion of **Cloud Storage Security** for M365 and GWS, we make sure there are no dormant threats in your cloud storage.

Premium edition includes all Essentials features, as well as:

- Block **C2 Callbacks** to malicious IPs/URLs
- **Distributed Proxy** of web traffic for inspection
- **DNS Threat Hunting** of suspicious web traffic
- Real-time **File Scanning** in cloud storage
- Commodity **Malware** detection
- Continuous **Data Risk Assessment** (DSPM)

∆DR Complete

Complete is tailored for organizations seeking advanced protection against identity-based threats, ensuring robust defense mechanisms for Active Directory (AD) and Microsoft Entra ID environments. This offering focuses on **real-time identity detection and response** to safeguard critical infrastructure and privileged accounts.

Complete edition includes all Premium features, as well as:

- **Real-Time AD & Entra ID Protection** provide continuous monitoring and defense against identity-based attacks
- **Identity Cloaking & Deception** to mislead attackers, protecting identity infrastructure
- **Privileged Account Protection**

∆DR Add-on SIEM

All ∆DR editions include 24 x 7 x 365 security operations with continuous incident response, attack surface management and full incident telemetry, but sometimes focusing on the endpoint, DNS, email and connected network telemetry is not enough.

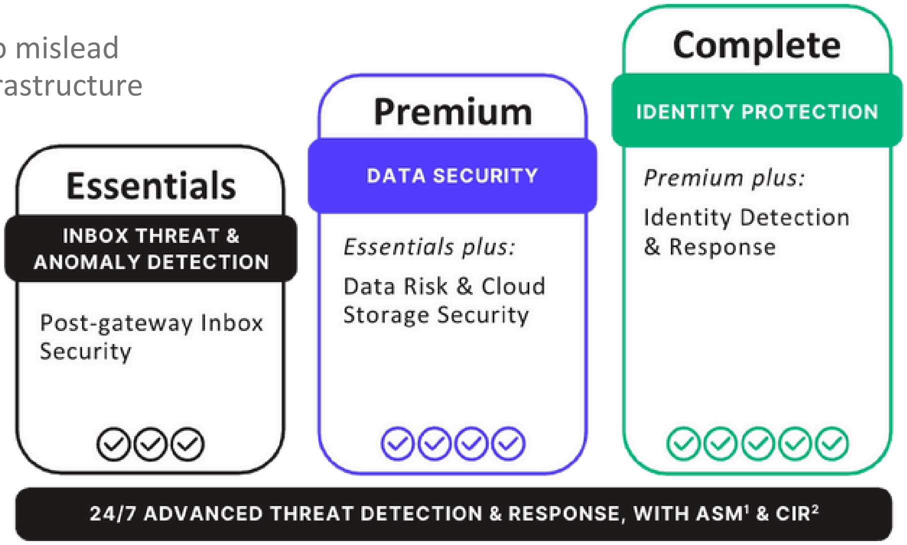
This is where our SIEM add-on for ∆DR shines. In addition to the deep visibility in our ∆DR platform, it never hurts to include telemetry and log sources from your infrastructure, cloud and SaaS applications.

The more telemetry we can integrate, the faster we can pinpoint and identify a bad actor in your network and root them out, reducing dwell time and potential risk of compromise.

Our optional SIEM add-on includes:

- Full featured **SIEM** to aggregate and correlate all of your log and API sources in one place
- **30-days** of **hot** storage for **raw data**, **1-year** of **hot** storage for **alerts** and **incidents, Sensors** and **Agents**
- **60MB**/day **data** volume is included for each **∆DR licensed node**, the SIEM Add-on is for **additional IPs & Users** (email addresses)

∆DR was built to eliminate the critical gaps between protection, detection, and response.



Essentials

INBOX THREAT & ANOMALY DETECTION

Post-gateway Inbox Security

✓✓✓

Premium

DATA SECURITY

Essentials plus:

Data Risk & Cloud Storage Security

✓✓✓✓

Complete

IDENTITY PROTECTION

Premium plus:

Identity Detection & Response

✓✓✓✓✓

24/7 ADVANCED THREAT DETECTION & RESPONSE, WITH ASM[1] & CIR[2]

[1] **Attack Surface Management (ASM)** includes Storage, DNS, Mailbox, Identity, Network and External Security Posture Management, and Breach & Attack Simulation (BAS).

[2] **Continuous Incident Response (CIR)** ensures threats are identified and neutralized before they escalate.

ΔDR Features	Essentials	Premium	Complete
Security Operations Center (24 x 7 x 365)			
Managed Detection & Response	✓	✓	✓
Active & Passive Asset Discovery (NTA)	✓	✓	✓
User & Entity Behavioral Analysis (UEBA)	✓	✓	✓
Continuous Network Vulnerability Scanning	✓	✓	✓
Breach & Attack Simulation (BAS) based on the MITRE ATT&CK® TTPs	✓	✓	✓
Dark Web & External Security Posture Management (ESPM)	✓	✓	✓
Identity Security Posture Management (ISPM)	✓	✓	✓
Continuous Incident Response (CIR)	✓	✓	✓
Endpoint Security			
Deep Visibility, Storylines, hunt by MITRE ATT&CK technique	✓	✓	✓
Manual / Auto file fetch (Windows, Mac, Linux)	✓	✓	✓
Deep Visibility Mark Benign finding as Threat for enforcement response	✓	✓	✓
Secure Remote Shell (Windows PowerShell, Mac & Linux bash)	✓	✓	✓
Autonomous Threat Response / Kill, Quarantine (Win, Mac, Linux)	✓	✓	✓
Static Behavioral AI for file-based / fileless attack detection & prevention	✓	✓	✓
Incident Analysis (MITRE ATT&CK, timeline, explorer, team annotations)	✓	✓	✓
Quarantine/Isolate device(s) from network	✓	✓	✓
OS & Third-party Application Inventory & Vulnerability (Win, Mac)			
DNS Security			
Block domains associated with phishing, malware, botnets, etc.	✓	✓	✓
Create custom block/allow lists	✓	✓	✓
Discover and block shadow IT, with App Discovery report	✓	✓	✓
Enable web filtering	✓	✓	✓
Proxy web traffic for inspection	✓	✓	✓
Inbox Security			
Real-time defense against business email compromise	✓	✓	✓
Protection against account takeover and insider risk	✓	✓	✓
Brand & Domain Fraud protection	✓	✓	✓
Account Takeover Protection	✓	✓	✓
SPF, DKIM, DMARC, BIMI Monitoring (DNSPM)	✓	✓	✓
Cloud Storage Security			
File Security for Google & Microsoft Collaboration Suites		✓	✓
Ransomware Risk Assessment		✓	✓
Data Security Posture Management (DSPM)		✓	✓
Identity Security			
Realtime AD & Entra ID Protection			✓
Identity Cloaking & Deception			✓
Privileged Account Protection			✓

Windows agents
All Windows workstation starting with 7 SP1 through Windows 11

All Windows Server starting with 2008 R2 SP1 through Server 2022

Mac agents
Big Sur, Monterey, Ventura, Sonoma

Windows Legacy agents
XP, Server 2003 & 2008, POS2009

Linux agents
Ubuntu, Redhat (RHEL), CentOS, Oracle, Amazon AMI, SUSE Linux Enterprise Server, Fedora, Debian, Virtuozzo, Scientific Linux

Container Support
Kubernetes self-managed v1.13+ [self-managed, AWS Kubernetes (EKS), Azure AKS]

Virtualization & VDI
Citrix XenApp, Citrix XenDesktop, Oracle VirtualBox, VMware vSphere, VMware Workstation, VMware Fusion, VMware Horizon, Microsoft Hyper-V