ISG-OPS

extended Detection & Response (XDR)

Platform Editions

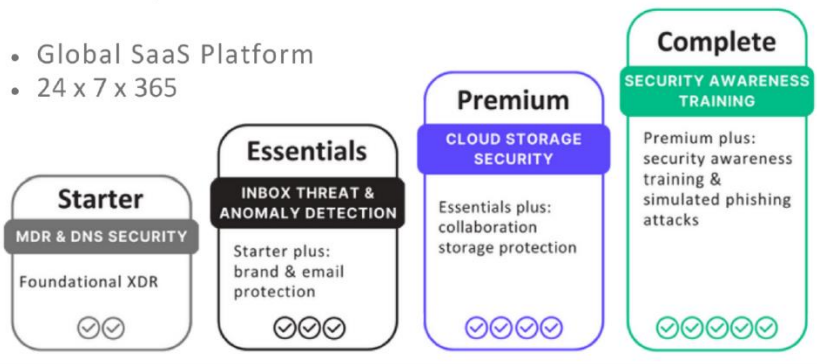
The first rule of a solid security posture: assume there's already a malicious adversary with a foothold in your environment. Our responsibility is to sniff out and eradicate that infiltrator.

XDR offers next-level threat detection and response, accelerating the ability to effectively "triangulate" threats. Instead of relying on analyst interpretation from disparate and siloed tools, XDR collects and automatically correlates data across multiple security layers and tools-email, endpoint, server, cloud workloads, and network-so threats can be detected faster, and security analysts can improve investigation and response times.

XDR is a fully managed service subscription designed to quickly elevate your security posture and back your security organization. XDR offers resource efficiency and autonomous agents for Windows, Mac, Linux, and Kubernetes. Network sensors and endpoint agents are managed centrally by our Security Operations team via our globally available multi-tenant SaaS platform. XDR supports a variety of form factors including physical, virtual, and VDI for both public and private clouds.

XDR Editions

All our XDR editions add value by ensuring that every threat is reviewed, acted upon, documented, responded to, and escalated as needed. We deliver what other XDR solutions aspire to be. Focused on capturing and correlating telemetry that matters, XDR takes time away from bad actors and empowers organizations to focus on what matters to their business. Each product bundle.



KEY BENEFITS

- Unified platform converges and integrates MDR, NDR, DNS, BEC, Internal/External & Cloud Posture security.
- Multi-layered cyber security protection takes the time advantage away from bad actors.
- Continuous Incident Response (CIR)
- Collects and automatically correlates data across multiple security layers and tools.
- Ransomware solved through superior behavioral AI
- Autonomous protective responses trigger instantly.
- Fully staffed and seasoned SOC backs your security organization 24 x 7 x 365.
- Time saving, fatigue-reducing forensic timeline for incident responders and threat hunters.
- Affordable data retention
- 97% customer support satisfaction
- 96% of customers recommend.

CONTACT US

XDR Starter

Starter is our foundational XDR edition, designed to meet the needs any sized organization that is ready to improve and modernize their distributed security posture.

XDR Starter includes our world-class 24 x 7 x 365 Security Operations, Managed Detection & Response with DNS security for cloud, on-prem and distributed workforces, including Continuous Incident Response (CIR), Internal & External Posture Management, and Continuous Purple Teaming.

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

Starter edition features:

- **24 x 7 x 365 Security Operations**
- **Autonomous 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
- **extended Security Controls Validations (eSCV)** 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**

XDR Essentials

Essentials enhances our Starter offering by adding frontline brand and business email compromise protection.

Gateway based email security is not cutting it, and Essentials advanced email security features are the answer! **Inbox Treat Analysis** (ITA) crawls through your M365 and GWS inboxes and finds dormant threats that got past your gateway defenses.

Essentials edition includes all Starter features, as well as:

- Real-time defense against **Phishing and Spear Phishing**
- Real-time **Account Takeover/Impersonation** detection
- **BEC, CEO Fraud** prevention and **Domain Fraud** visibility

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

KEY FEATURES

- 24 x 7 x 365 Security Operations
- Integrated threat intelligence and MITRE ATT&CK® threat indicators
- Continuous Incident Response (CIR)
- Continuous Purple Teaming
- DNS & Email Security and threat detection/prevention
- Cloud storage security for M365 & GWS collaboration suites
- End user security training & phishing simulation
- Multi-faceted telemetry for a more comprehensive and effective threat triangulation
- Global SaaS platform. Highly available. Choice of locality
- Flexible administrative authentication and authorization {SSO, MFA, RBAC)
- Administration customizable to match your organizational structure

XDR Premium

Premium adds deeper DNS security and cloud storage protection for M365 or GWS 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 **direct-to-IP** traffic for **C2 Callbacks**
- **Distributed Proxy** of web traffic for inspection
- **SSL Decryption** to inspect web traffic
- **DNS Threat Hunting** of suspicious web traffic
- Real-time **File Scanning** in cloud storage
- Commodity **Malware** detection

XDR Complete

Complete is for discerning organizations that want **comprehensive security** for all of their endpoint security, and want to ensure their users are trained and have **security awareness** when faced with threats.

Complete edition includes all Premium features, as well as:

- Monthly **Security Awareness Training**
- Advanced **Phishing/Threat Simulation**
- **Phish reporting** button
- Program **gamification**

XDR Add-on SIEM

All XDR editions include 24 x 7 x 365 security operations with continuous incident response and full incident telemetry, but sometimes focusing on the endpoint and connected network telemetry is not enough.

This is where our SIEM add-on for XDR shines. In addition to the deep visibility in our XDR 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.

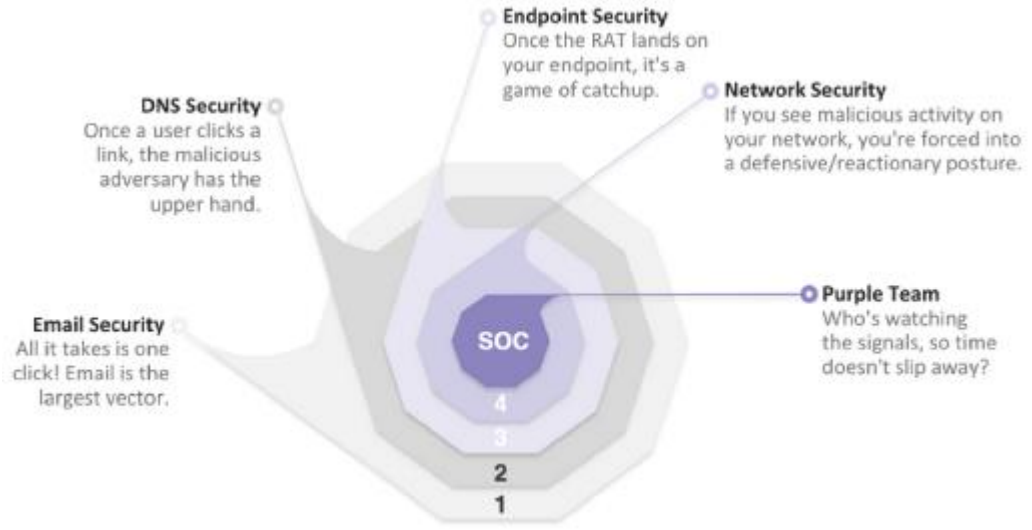
Our optional SIEM add-on includes:

- Full featured **SIEM** to aggregate and correlate all of your log and API sources in one place The base add-on includes **15-days* of live telemetry and up to 250G ** per month of** process data
- Network Vulnerability scans mapped to CVSS
- Host-based Intrusion Detection (HIDS) for domain controllers
- Network-based Intrusion Detection (NIDS) UEBA to baseline user and entity behavior for anomaly detection

* Live data retention options (15, 30, 90 or 180 days)

** Processed data per month can be upgraded to meet the demands of your environment

Our five-layered modern defense-in-depth approach to #cyberresilience in a highly distributed world.



XDR Editions Comparison

	Starter	Essentials	Premium	Complete
Security Operations Center (24 x 7 x 365)				
Managed Detection & Response	✓	✓	✓	✓
Active & Passive Asset Discovery (NTA)	✓	✓	✓	✓
Continuous Incident Response (CIR)	✓	✓	✓	✓
User & Entity Behavioral Analysis (UEBA)	✓	✓	✓	✓
Continuous Network Vulnerability Scanning	✓	✓	✓	✓
Internal Security Controls Validation based on the MITRE ATT&CK TTPs	✓	✓	✓	✓
Dark Web & External Vulnerability Assessment (Purple Teaming)	✓	✓	✓	✓
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 or 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	✓	✓	✓	✓
Block direct-to-IP traffic for C2 callbacks that bypass DNS		✓	✓	✓
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		✓	✓	✓
Cloud Storage Security				
File Security for Google & Microsoft Collaboration Suites			✓	✓
Security Awareness Training				
Monthly End User Training				✓
Advanced Phishing Simulation				✓
Advanced Threat Simulation				✓
Phish Reporting Button & Program Gamification				✓

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

All Windows Server starting with 2008 R2 SP1 through 2022

Mac agents
macOS Ventura, Monterey, Catalina, Mojave, High Sierra

Windows Legacy agents
XP, Server 2003 & 2008

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