Endpoint Detection & Response

EDR Platform Editions

Empower SOC & IT Operations Teams with a more efficient way to protect information assets against today's sophisticated threats.

Our Endpoint Detection and Response delivers differentiated endpoint protection including endpoint detection and response, IoT security, cloud security, and IT operations capabilities—consolidating multiple existing technologies into one solution.

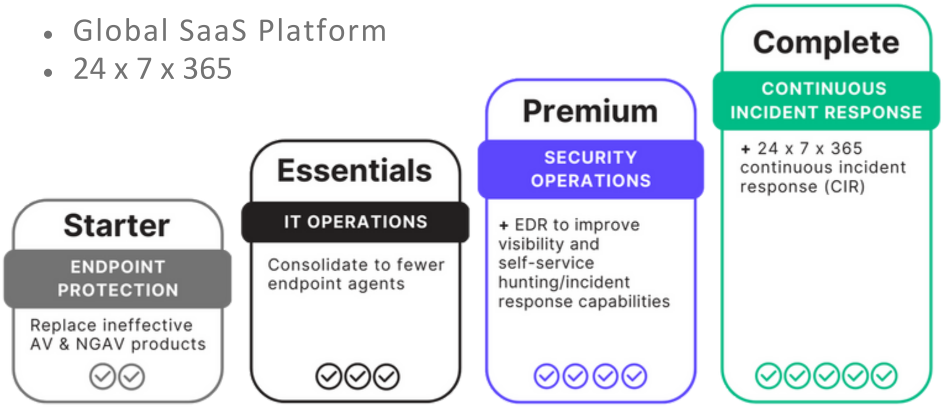
We offer EDR as a fully managed service or platform solution with resource efficient, autonomous agents for Windows, Mac, Linux, and Kubernetes and support a variety of form factors including physical, virtual, VDI, for both public and private cloud.

EDR Agents are managed via our globally available multi-tenant SaaS platform that meets your cost and security and requirements.

With four tiered offerings, EDR Starter, Essentials, Premium and Complete, you get the service—and protection level—that works for your organization.

EDR Editions

- Global SaaS Platform
- 24 x 7 x 365



Starter
ENDPOINT PROTECTION
Replace ineffective AV & NGAV products
✓✓

Essentials
IT OPERATIONS
Consolidate to fewer endpoint agents
✓✓✓

Premium
SECURITY OPERATIONS
+ EDR to improve visibility and self-service hunting/incident response capabilities
✓✓✓✓

Complete
CONTINUOUS INCIDENT RESPONSE
+ 24 x 7 x 365 continuous incident response (CIR)
✓✓✓✓✓

KEY BENEFITS

- Real-time detection and remediation of complex threats with no need for human intervention
- Accelerated triage and root cause analysis with incident insights and the best MITRE ATT&CK alignment on the market, with or without MDR
- Integrated threat intelligence for detection and enrichment from leading 3rd party feeds as well as our proprietary sources
- Autonomous protective responses trigger instantly, with 1-Click Remediation & Rollback
- Time saving, fatigue-reducing forensic timeline for incident responders and threat hunters
- Uncompromising protection across Windows, Linux, and macOS endpoints - physical, virtual, container - cloud or data center

CONTACT US

☎

🌐

✉

EDR Starter

Starter is the foundation of all our endpoint security offerings. It's our entry level endpoint security edition for organizations that want to replace legacy anti-virus or NGAV with an End Point Protection (EPP) that is effective and easy to manage.

This edition also offers basic EDR functions demonstrating the true merging of EPP+EDR capabilities. Threat intelligence is part of our standard offering and integrated through our AI functions.

Starter edition features:

- **Built-in Static AI and Behavioral AI analysis** prevent and detect a wide range of attacks in real time before they cause damage. Starter protects against known and unknown malware, Trojans, hacking tools, ransomware, memory exploits, script misuse, bad macros, and more.
- **Agents are autonomous** which means they apply prevention and detection technology with or without cloud connectivity and will trigger protective responses in real time.
- **Recovery is fast** and gets users back and working in minutes without re-imaging and without writing scripts. Any unauthorized changes that occur during an attack can be reversed with single click remediation and 1-Click Rollback for Windows.
- **Secure SaaS management access**. Choose from US, EU, APAC localities. Data-driven dashboards, policy management by site and group, incident analysis with MITRE ATT&CK integration, and more.

EDR Essentials

Essentials is made for organizations seeking the best-of- breed security found in EDR Starter with the addition of security suite features for endpoint management.

Essentials edition includes all Starter features plus:

- **Firewall Control** for control of network connectivity to and from devices including location awareness.
- **Device Control** for control of USB devices and Bluetooth/BLE peripherals.
- **Vulnerability Management,** in addition to application inventory, for insight into 3rd party apps that have known vulnerabilities mapped to the MITRE CVE database.

Stop ransomeware and other fileless attacks with behavioral AI and strong autonomous remediation.

KEY FEATURES

All editions include:

- Global SaaS implementation. Highly available. Choice of locality (US, EU, APAC)
- Flexible administrative authentication and authorization: SSO, MFA, RBAC
- Administration customizable to match your organizational structure
- 365 days threat incident history
- Integrated intelligence and MITRE ATT&CK® threat indicators
- Data-driven Dashboard Security Analytics
- Configurable notifications by email and syslog
- API-driven eXtended Detection & Response (XDR) integrations (SIEM, sandbox, Slack, 3rd party threat intelligence, etc.)
- Single API with 340+ functions

EDR Premium

Premium is made for enterprises that need modern endpoint protection and control plus advanced EDR features. Premium adds threat hunting with forensics that automatically contextualizes all OS process relationships (even across reboots) every second of every day and stores them for your future investigations. This saves analysts from tedious event correlation tasks and gets them to the root cause fast.

Premium is designed to lighten the load on security administrators, SOC analysts, threat hunters, and incident responders by automatically correlating telemetry and mapping it into the MITRE ATT&CK® framework. The most discerning global enterprises run Premium for their unyielding cybersecurity demands.

Premium edition includes Starter + Essentials features, as well as:

- **Forensic timeline tech** for fast RCA and easy pivots.
- **Integrated threat intelligence visibility** to both benign and malicious data.
- **14 - 365+ day historical EDR data** retention + usable query speeds at scale.
- **Hunt by MITRE ATT&CK®** Technique.
- **Mark benign storylines as threats** for enforcement by the EPP functions.
- **Automated Storyline™** Active Response (STAR) watchlist.

EDR Complete

Complete is a fully managed detection and response service subscription available to back your security organization 24x7 with a fully manned SOC and Continuous Incident and Response (CIR).

Complete is a service subscription designed to augment customer security organizations. Complete adds value by ensuring that every threat is reviewed, acted upon, documented, and escalated as needed.

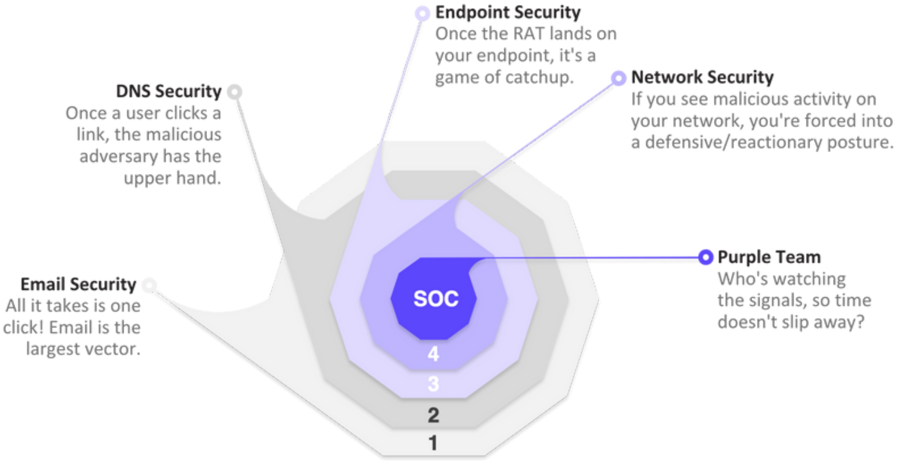
In most cases, we interpret and resolve threats in under 30 minutes—and only contact you about urgent matters.

EDR Complete empowers customers to focus only on the incidents that matter, making it the perfect endpoint add-on solution for overstretched IT/SOC Teams. Complete is a fully managed platform including agent updates, incident response, and remediation services.

Complete edition includes Starter + Essentials + Premium features, as well as:

- **Continuous Incident Response** (CIR)
- **24 x 7 x 365 Security Operations Center** (SOC). Seasoned SOC analysts:
  - **Active threat hunting**
  - **Identify and respond** to threats in real time.
  - **Resolve threats** and perform CIR
  - **Post Incident** support

EDR powers the endpoint security facet of our modern defense-in-depth approach to #cyberresilience in a highly distributed world.


Endpoint Security
Once the RAT lands on your endpoint, it's a game of catchup.
DNS Security
Once a user clicks a link, the malicious adversary has the upper hand.
Network Security
If you see malicious activity on your network, you're forced into a defensive/reactionary posture.
Purple Team
Who's watching the signals, so time doesn't slip away?
Email Security
All it takes is one click! Email is the largest vector.
SOC
4
3
2
1

EDR Editions Comparison

	Starter	Essentials	Premium	Complete
Managed Global SaaS Platform				
Secure Access, High Availability, EPP Policy Administration	✓	✓	✓	✓
EDR Incident Response & Threat Hunting	✓	✓	✓	✓
Complete Management & Monitoring	✓	✓	✓	✓
24 x 7 x 365 Security Operations Center and Subscription as a Service	✓	✓	✓	✓
Real time identification and response to threats by SOC	✓	✓	✓	✓
Post Action Reports	✓	✓	✓	✓
Base Endpoint Protection Features				
Autonomous agent Storyline™ engine	✓	✓	✓	✓
Static AI & Cloud file-based attack prevention	✓	✓	✓	✓
Behavioral AI fileless attack detection	✓	✓	✓	✓
Autonomous Threat Response / Kill, Quarantine (Win, Mac, Linux)	✓	✓	✓	✓
Autonomous Remediation Response / 1-Click, no scripting (Win, Mac)	✓	✓	✓	✓
Autonomous Rollback Response / 1-Click, no scripting (Win)	✓	✓	✓	✓
Quarantine device from network	✓	✓	✓	✓
Incident Analysis (MITRE ATT&CK®, timeline, explorer, team annotations)	✓	✓	✓	✓
Agent anti-tamper	✓	✓	✓	✓
App Inventory	✓	✓	✓	✓
IT OPS / Security Hygiene & Suite Features				
OS Firewall control with location awareness (Win, Mac, Linux)		✓	✓	✓
USB device control (Win, Mac)		✓	✓	✓
Bluetooth® / Bluetooth Low Energy® control (Win, Mac)		✓	✓	✓
App Vulnerability (Win, Mac)		✓	✓	✓
Security Operations EDR Features				
Deep Visibility ActiveEDR™			✓	✓
Deep Visibility StoryLine™ pivot			✓	✓
Deep Visibility hunt by MITRE ATT&CK technique			✓	✓
Automated Storyline™ Active Response (STAR) watchlist			✓	✓
Manual / Auto file fetch (Windows, Mac, Linux)			✓	✓
Deep Visibility Mark Benign finding as Threat for enforcement response			✓	✓
Extended EDR Historical Data Storage (available 14-365 days)			✓	✓
Secure Remote Shell (Windows Powershell, Mac & Linux bash)			✓	✓
Active threat hunting by SOC			✓	✓
Analytics, IoT Control (with Ranger option)				✓
Continuous Incident Response (CIR)				✓
Security Controls Validation				✓

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