FORENOVA

Nova MDR™

NovaMDR™

Cyber-Bedrohungen erkennen. Sicherheit stärken.

Herausforderungen lösen.

Anbieter im Gesundheitswesen stehen vor erheblichen Herausforderungen, wenn es darum geht, eine zuverlässige Cybersicherheit für sensible Patientendaten (Protected Health Information, PHI) sicherzustellen. Besonders der Schutz sensibler Gesundheitsdaten stellt hohe Anforderungen. Diese werden durch mehrere Faktoren zusätzlich erschwert.

Interoperabilität von Daten und IT-Systemen

Patientendaten, elektronische Gesundheitsakten, Diagnosen und Behandlungspläne werden in unterschiedlichsten Systemen gespeichert und übertragen. Jedes dieser Systeme erfordert eigene Sicherheitskontrollen, um den Schutz sensibler Informationen zu gewährleisten. Gleichzeitig vergrößert jedes zusätzliche medizinische Gerät, IoT-System, jeder Cloud-Dienst oder externe Anbieter die potenzielle Angriffsfläche. Viele dieser Systeme sind veraltet, erhalten keine regelmäßigen Sicherheitsupdates oder weisen teils gravierende Schwachstellen auf. Sie sind somit ideale Ziele für Cyberangriffe.

Einhaltung gesetzlicher Vorgaben und Branchenstandards

Gesetze wie das Krankenhauszukunftsgesetz (KHZG), das „Digitale-Versorgung-Gesetz“ sowie die Datenschutzanforderungen der DSGVO stellen hohe Anforderungen an den Schutz sensibler Gesundheitsdaten. Diese Vorgaben müssen nicht nur eingehalten, sondern auch regelmäßig überprüft und durch eine nachweisbare Sorgfaltspflicht belegt werden.

Zugang zu Cybersicherheitsexpertise

Während viele Klinikbereiche rund um die Uhr betrieben werden, steht häufig nur ein kleines IT-Team mit begrenzten Ressourcen zur Verfügung – meist ausschließlich zu Geschäftszeiten. Zuständigkeiten im Bereich Cybersicherheit sind oft nur einfach verteilt, sodass es an spezialisiertem Know-how fehlt, um die tatsächliche Bedrohungslage umfassend zu bewältigen.

24/7-Schutz für einen 24/7-Betrieb: Klinische Systeme müssen jederzeit verfügbar sein – Ausfälle sind keine Option. Gleichzeitig dürfen Sicherheitsmaßnahmen den operativen Betrieb nicht behindern, was nicht selten zu risikobehafteten Kompromissen führt. Der Ausfall digitaler Systeme kann im Ernstfall Menschenleben gefährden.

Für einzelne Praxen ist der Aufbau eines eigenen Security Operations Centers (SOC) kaum realisierbar. Selbst große Krankenhausverbünde stehen hier vor enormen Herausforderungen – personell, technisch und finanziell. Der Betrieb eines SOC erfordert hochqualifizierte Cybersicherheitsexperten, kontinuierliche Schulungen sowie leistungsfähige Erkennungs- und Reaktionssysteme.

NovaMDR™ schließt diese Lücke mit einem 24/7-Überwachungsdienst für Endgeräte und Netzwerke – unterstützt durch moderne Detection-&-Response-Technologien. So wird die Cyber-Resilienz Ihrer Einrichtung gezielt gestärkt.

Vermeiden Sie Reputationsschäden durch Datenpannen. Entlasten Sie Ihr IT-Team mit einem spezialisierten Sicherheitsdienst, der Ihre sensiblen Systeme rund um die Uhr im Blick hat – damit Sie sich ganz auf die Versorgung Ihrer Patientinnen und Patienten konzentrieren können.

Cybersicherheit als Service

Proaktive Abwehr für eine neue Bedrohungsrealität

Seien Sie Angreifern immer einen Schritt voraus.

- Angesichts immer ausgefeilterer Cyberbedrohungen und des rasanten Fortschritts in der KI reicht eine rein strategische Cyberabwehr nicht mehr aus.
- NovaMDR™ setzt auf proaktive Verteidigung: Unsere XDR-Plattform, GPT-Technologie und erfahrene Sicherheitsexperten reagieren in Echtzeit auf sich stetig wandelnde Bedrohungsszenarien.

Schließen Sie Ihre Sicherheitslücken

Stärken Sie Ihr Team mit unserer Expertise

- Profitieren Sie von einem echten Wettbewerbsvorteil durch NovaMDR™ – mit einem Team aus hochqualifizierten Cybersicherheitsexperten an Ihrer Seite.
- Wir liefern das Fachwissen, das Ihre Organisation braucht, um auch komplexe Bedrohungen souverän zu meistern – ganz ohne den Aufwand, intern teure Spezialisten einzusetzen.

Compliance nachweisen – Sicherheit gewinnen

Gesetzliche Vorgaben mühelos erfüllen

- Vorgaben wie NIS2, KRITIS oder ISO 27001 stellen hohe Anforderungen an Ihr Sicherheits- und Nachweissystem.
- NovaMDR™ unterstützt Sie gezielt dabei – mit professioneller Bedrohungsreaktion, vollständiger Abdeckung Ihrer digitalen Assets und automatisierten Compliance-Berichten, die den Nachweis der Einhaltung deutlich erleichtern.

FORENOVA

Funktionsübersicht

NovaMDR™ bietet eine Rund-um-die-Uhr-Überwachung Ihrer Endgeräte, Netzwerke, Cloud-Dienste und Firewalls und gewährleistet so umfassenden Schutz vor Cyber-Bedrohungen. Durch die Zusammenführung von Daten aus verschiedenen Quellen maximiert unser Expertenteam die Leistungsfähigkeit der KI-gestützten Analysen.

NovaMDR™ nutzt fortschrittliche GPT-KI und maschinelles Lernen, um Bedrohungen frühzeitig zu erkennen – und reduziert so die Zeit, die Angreifer zur Ausnutzung von Schwachstellen haben. Diese schnelle Erkennung sorgt dafür, dass Ihre Umgebung selbst vor hochentwickelten Angriffen geschützt bleibt.

Funktionen	NovaMDR™
Komplettlösung zur 24/7-Bedrohungserkennung	✔
Erweiterte Analysen durch menschliche Expertise und KI	✔
Schnelle Reaktion und effektive Eindämmung von Bedrohungen	✔
Proaktive Bedrohungssuche (Threat Hunting)	✔
Hohe Transparenz durch umfassende Berichterstattung	✔
Einfache und kostengünstige Lizensierung	✔

Wichtigste Funktionen und Vorteile von NovaMDR™

NovaMDR™ – Die wichtigsten Vorteile

Umfassende Cybersicherheit

Mehr sehen. Mehr erkennen.

- Umfassende Signalerfassung
- Endpunkte, Netzwerk, Cloud-Dienste, Firewall-Integrationen
- Normalisiert, aggregiert, korreliert
- Kontinuierlich verbesserte Playbooks
- Erkennen Sie ein breiteres Spektrum an Angriffen

Überwachung rund um die Uhr

- Jederzeit Zugang zu Experten
- Erweiterung Ihres Teams
- Echtzeit-Transparenz über das Portal und regelmäßige Berichte

Umfassender Schutz während des gesamten Angriffszyklus

- Vor dem Angriff: Risiken bewerten, bestehende Maßnahmen verstärken, Schwachstellen reduzieren
- Während des Angriffs: Experten werden durch GPT-KI unterstützt, um eine schnellere und präzisere Triage, Erkennung und gründliche Untersuchung zu ermöglichen
- Aktive, schnelle Reaktion und Eindämmung
- Nach dem Angriff: Unterstützung bei der Ursachenanalyse und Stärkung der Abwehrmaßnahmen

Sicherheit für jedes Szenario

Ransomware-Prävention

- Spezifische Algorithmen zur Erkennung von Ransomware
- Angewandte Ransomware-Intelligenz für gründliche Überprüfungen
- Umfassende Kill-Chain-Analyse
- Von Menschen überprüft und analysiert
- Schnelle Reaktion zur Verringerung erheblicher Auswirkungen

Verbesserter Microsoft 365-Schutz

- Spezifische Erkennung von Anwendungsfällen für Angriffe auf Arbeitsbereiche
- Umfassende Abdeckung von Bedrohungstaktiken für Benutzer- und Administratorkonten
- Erkennung kompromittierter Konten, potenzieller Social-Engineering-Angriffe
- Die Benutzer- und Ereignisverhaltensanalyse (UEBA) erkennt ungewöhnliche Aktivitäten

Proaktive Prävention

Turnkey-Lösung

- Enthält wichtige Sensoren für Endpunkt- und Netzwerktransparenz
- Zusatzsensoren für Transparenz der Cloud- und Firewall-Aktivitäten
- Die Sensoren werden mit den neuesten Bedrohungsinformationen und Erkennungsupdates gewartet

Kompetente strategische Beratung

- Wir sind Ihre Cybersicherheitsberater für:
- Strategische Verbesserungen, betriebliche Effizienz, taktische Erfolge
- Untersuchung von Vorfällen und Reaktion darauf

FORENOVA

Integration für schnelle Reaktionsmaßnahmen

NovaMDR™ bietet vorgefertigte Integrationen für Reaktionsmaßnahmen auf Basis führender Sicherheitslösungen und lässt sich dank moderner, flexibler API nahtlos in bestehende Systeme einbinden.

Warum entscheiden sich Gesundheitsdienstleister für ForeNova?

Minimale Auswirkungen auf bestehende Systeme

NovaMDR™ integriert sich nahtlos in Ihre bestehende Infrastruktur und erweitert deren Funktionen – ganz ohne zusätzliche Investitionen.

Die Lösung wurde gezielt entwickelt, um vorhandene Sicherheitsstrukturen zu ergänzen und zu stärken. So schöpfen Sie Ihre bisherigen Investitionen voll aus und profitieren ab dem ersten Tag von einem wirksamen Schutz.

Kosteneffizienz – ideal für begrenzte Budgets im Gesundheitswesen

Unsere Technologie optimiert den Betrieb Ihres SOCs, reduziert den Personalbedarf und ermöglicht es uns, erstklassige Cybersicherheitslösungen zu einem äußerst wettbewerbsfähigen Preis bereitzustellen.

Erweiterte Erkennung von Ransomware und kritischen Bedrohungen

Die Analyse-Engines von NovaMDR™ erfassen und korrelieren sicherheitsrelevante Daten deutlich effektiver als herkömmliche SIEM-Lösungen.

Durch die Kombination aus KI, maschinellem Lernen und menschlicher Expertise bieten wir eine präzise Überwachung Ihrer digitalen Umgebung – und erkennen selbst schwer fassbare Angriffe, bevor sie Schaden anrichten können.