FORENOVA

Angriffsfläche Blueprint

Stoppen Sie Ransomware, bevor es kein Zurück mehr gibt!
Erhalten Sie jetzt einen vollständigen Überblick über Ihr Netzwerk.

blueprint.forenova.com

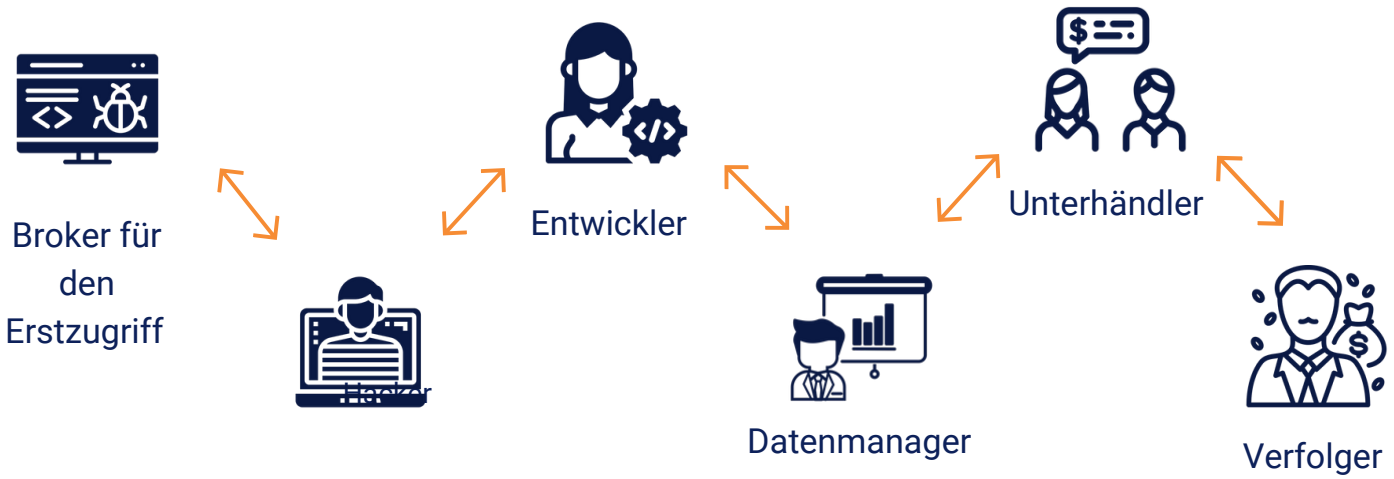
INHALTSVERZEICHNIS

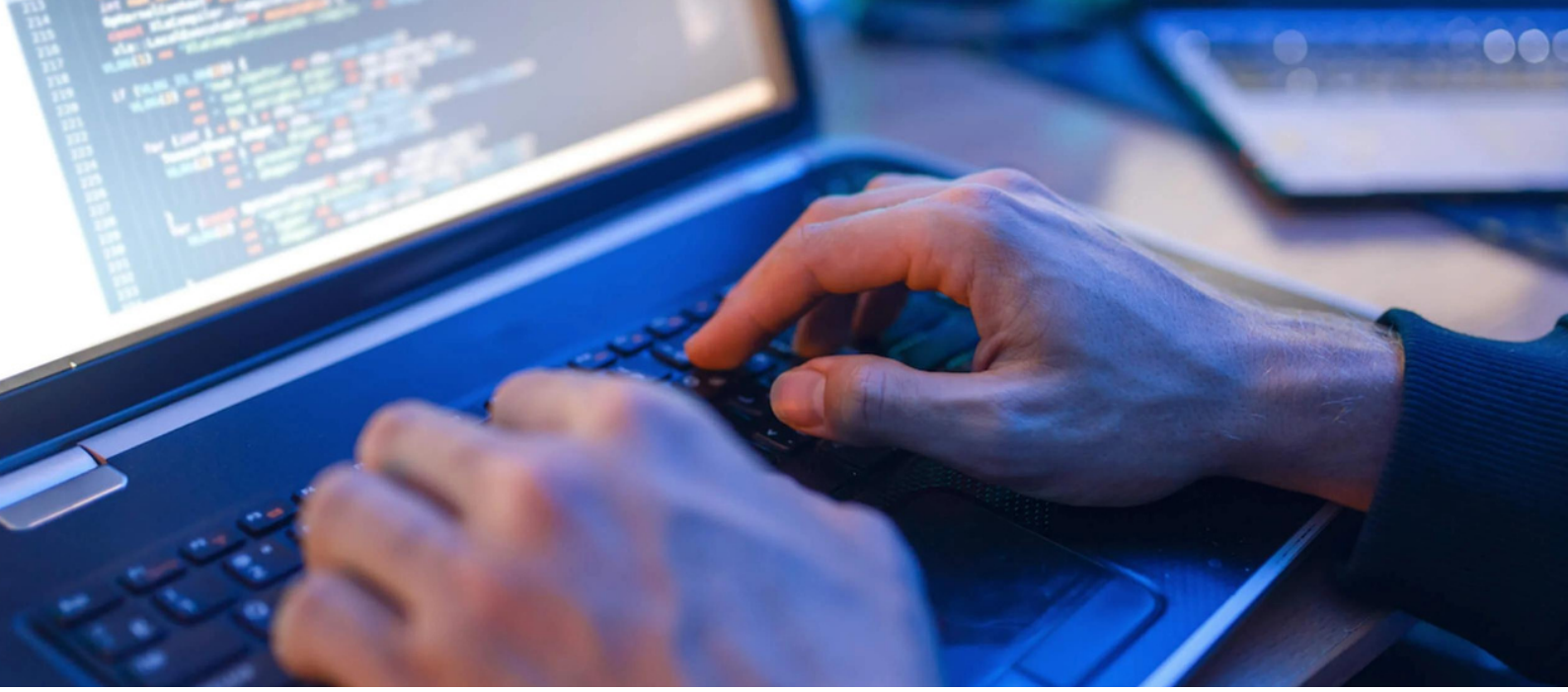
Eine neue Ära der Cybersicherheit

Cyberkriminelle haben Kapuzenpullis und dunkle Kellerräume gegen Geschäftsanzüge und Büros eingetauscht. Mittlerweile treten sie weltweit als professionelle Organisationen auf. Diese Ransomware Banden heuern die Besten der Branche an und schaffen eine ausgeklügelte und komplexe Kill Chain, die nur ein Ziel verfolgt: Daten zu verschlüsseln und das höchste Lösegeld zu erlangen.

Ransomware-Banden verfeinern kontinuierlich ihre Methoden. Erstzugriffsmakler, die erste Stufe in der Kill Chain, suchen mithilfe von maschinellem Lernen und KI nach gefährdeten Unternehmen mit hohem Wert. Mit diesen fortschrittlichen Technologien kann es für Teams schwierig sein, Angriffsmuster zu erkennen. Dadurch bemerken viele Teams die Netzwerkinfiltration erst, wenn ihre Dateien verschlüsselt sind. Darüber hinaus ist die steigende Popularität von Kryptowährungen ein großes Problem. Banden erhalten durch den Einsatz von Kryptowährungen einfacher Zahlungen und für Strafverfolgungsbehörden wird es immer schwieriger, Transaktionen zu verfolgen.

RANSOMWARE KILL CHAIN





Angesichts der zunehmenden Verbreitung von Ransomware - mit einem Anstieg von 151 % in den ersten sechs Monaten des Jahres 2021 - reicht eine Vorbeugung nicht mehr aus. Um Hacker mit ihren eigenen Waffen zu schlagen, müssen Sie genau das sehen, was sie sehen - einen vollständigen Überblick über die Netzwerkumgebung. Durch ForeNovas Attack Surface Blueprint ist das endlich möglich. So erfahren Sie, wie Ransomware Banden die Schwachstellen ihres Unternehmensnetzwerkes finden und versteckte Bedrohungen aufdecken. Handeln Sie jetzt schnell und sicher, um Ransomware zu erkennen und zu bekämpfen.

Auf den folgenden Seiten geben wir Ihnen einen Einblick in Funktionsweise der Attack Surface Blueprint, unterstützt durch ForeNovas Ansatz zur Netzwerkerkennung und -reaktion.

Denn man kann nicht etwas bekämpfen, das man nicht sieht - bis jetzt.

Ihr Attack Surface Blueprint

Unser Team von Ransomware-Experten erstellt Ihren individuellen Attack Surface Blueprint, basierend auf Daten und Analysen von Tausenden von Unternehmen, Ransomware-Angriffen und unentdeckten Bedrohungen. Anhand unserer Analysen haben wir die drei häufigsten Ransomware-Risiken für kleine und mittelständische Unternehmen identifiziert: IoT, Supply Chain und Insider-Bedrohungen.

INTERNET OF THINGS, IoT

Ransomware, die auf das Internet der Dinge abzielt, ist im Jahr 2021 mit mehr als 32 Millionen Angriffen sprunghaft angestiegen. Die größten Herausforderungen bei der Sicherung von IoT-Geräten sind ein schwacher Passwortschutz, das Fehlen regelmäßiger Patches und Updates sowie eine schlechte Geräteverwaltung.

SUPPLY CHAIN

Unternehmen, Branchen und die Gesellschaft sind immer stärker von komplizierten Lieferketten abhängig. Die Angriffe auf Supply Chains stiegen 2020 um 430 % und werden sich 2021 voraussichtlich noch einmal vervierfachen.

INSIDER THREATS

Mitarbeiter können das größte Kapital eines Unternehmens sein, aber mit Netzwerkzugang und ohne effiziente Schulungen und Kontrollen können sie es Ransomware-Banden leicht machen, in das Netzwerk einzudringen. Obwohl sie oft übersehen werden, machen Insider-Bedrohungen 60 % aller Datenschutzverletzungen aus.

DIE NovaCommand PLATTFORM

Die Erstellung eines Blueprints der Angriffsoberfläche ist ein schneller und nicht invasiver Prozess. Mit der gleichen Technologie, die NovaCommand, unserer Plattform zur Netzwerkerkennung und -reaktion nutzt, können wir in weniger als 4 Wochen einen Plan auf der Grundlage Ihres Netzwerkverkehrs erstellen.

Und so funktioniert es:

- Unser NovaSensor wird in Ihrem Netzwerk platziert, um die Basislinie Ihres Netzwerkverkehrs zu eruieren (dies ist auch als Port Mirror oder SPAN-Daten bekannt). Der Sensor sendet die Informationen basierend auf den Metadaten (nicht den Traffic selbst) an NovaCommand.
- NovaCommand analysiert den Datenverkehr und erstellt eine Momentaufnahme davon, **wer** in Ihrem Netzwerk kommuniziert (Assets), **worüber** sie sprechen (Logs, Anwendungen) und **wohin** der Datenverkehr geht (Ziele).
- NovaCommand korreliert und analysiert diese Daten, um anomalen Datenverkehr zu identifizieren. Dabei kann es sich um die Kommunikation mit "Command-and-Control-Servern", offene Ports in Ihrem Netzwerk und Anlagen handeln, auf denen "ältere" Softwareversionen mit bekannten Sicherheitslücken laufen.
- Unsere Erkenntnisse fassen wir dann im Attack Surface Blueprint zusammen und geben Ihnen so einen vollständigen Überblick über Ihre Netzwerkumgebung. Sie enthält eine Momentaufnahme des ein- und ausgehenden Datenverkehrs, Schwachstellen und Empfehlungen unseres Expertenteams, damit Ihr Unternehmen versteckte Bedrohungen schneller und präziser erkennen und darauf reagieren kann.

Sobald Sie Ihren Plan haben, wird unser Sales Engineering-Team einen Termin vereinbaren, um mit Ihnen Ihre Ergebnisse durchzugehen und Ihnen die nächsten Schritte und Maßnahmen basierend auf den Ergebnissen vorzuschlagen. Dies könnte beispielsweise die Anpassungen Ihrer aktuellen Sicherheitskontrollen und/oder die Erweiterung des Blueprint-Prozesses zu einem formalen Proof of Concept beinhalten.

FORENOVA

Attack Surface Blueprint

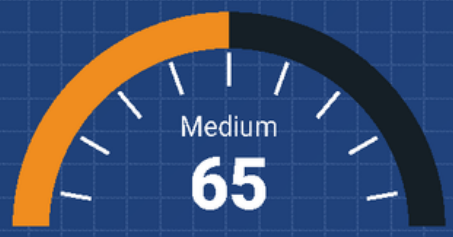
For Healthcare Providers

Network Security Overview

Stop ransomware by seeing what the attackers see, with a complete view of your IT network environment.

Stages of Attack

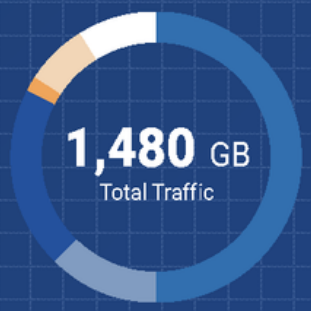
Overall Security Rating



Low Activity (7 Days)	Active Assets	Critical
66	968	6

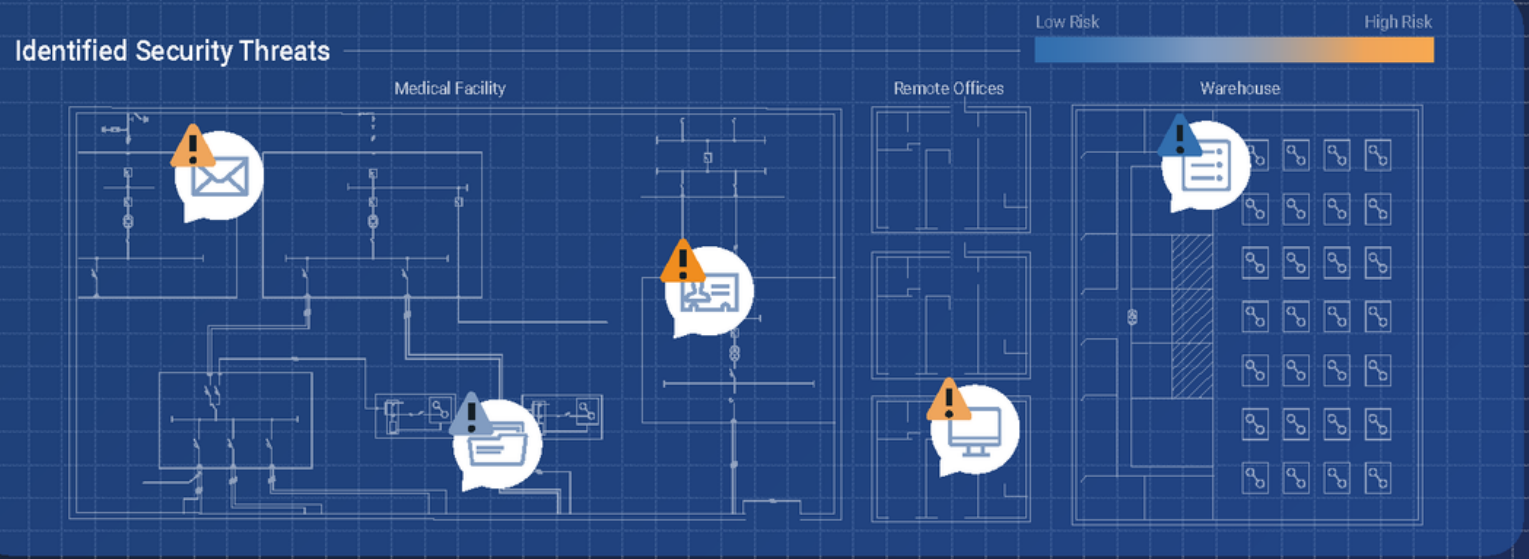
IoT	Servers	Hosts
350	310	308

Application Traffic



- Application Traffic: 740 GB
- File Transfer: 182 GB
- DNS: 1 GB
- SSL: 300 GB
- Remote Login: 2 GB
- RDP: 24 GB
- HTTP Application: 101 GB
- Streaming Media: 130 GB

Identified Security Threats



Get your custom ForeNova Attack Surface Blueprint.

Along with a detailed view of your network, it will include a snapshot of inbound and outbound traffic, vulnerabilities and weaknesses, and recommendations from our team of experts to help your business detect and respond to hidden threats with greater speed and precision.

**This Healthcare Attack Surface Blueprint is based on generalized data across mid-size healthcare organisations*

HOLEN SIE SICH JETZT IHREN INDIVIDUELLEN ATTACK SURFACE BLUEPRINT

Ihr individuelles Attack Surface Blueprint ist ein kostenloses 30-Tage-Pilotprojekt, zu dem Sie keinerlei Verpflichtung haben, sobald Sie es erhalten haben.

Sind Sie bereit loszulegen?

Holen Sie sich jetzt ihren Attack Surface Blueprint

ÜBER FORENOVA

ForeNova hilft kleinen und mittleren Unternehmen, sich aus den Unmengen der Warnmeldungen inklusive der False-Positive, der organisatorischen Silos und der ausufernden IT zu befreien und die Kontrolle über die ständigen Bedrohungen und Angriffe zu übernehmen. Ganz gleich, ob Sie Angriffe untersuchen, die Verfügbarkeit kritischer Anwendungen sicherstellen oder Ihre Investitionen in die Cloud sichern wollen, ForeNova erkennt Bedrohungen schnell und reagiert effizient.

Anfang 2021 wurde die ForeNova Technologies B.V. in den Niederlanden gegründet. Mit der Unterstützung von Hunderten von Entwicklern und Ingenieuren, die in Asien, Europa und den USA zusammenarbeiten, brachte das Unternehmen NovaCommand auf den Markt, eine benutzerfreundliche, erschwingliche NDR-Lösung, die moderne Sicherheit für kleine und mittelständische Unternehmen bietet. Heute arbeitet das Team in drei globalen Forschungs- und Entwicklungszentren weiter an der Innovation der KI-Engine der Plattform, um der Konkurrenz immer einen Schritt voraus zu sein und die EU-Zielmärkte zu bedienen. Die aktuelle Version von NovaCommand wird aus unserem GDPR-konformen europäischen Rechenzentrum in Frankfurt am Main ausgeliefert. Mehr Informationen unter: blueprint.forenova.com