WHITEPAPER

Digital Security
Progress. Protected.

Patient Krankenhaus: IT-Gesundheit beginnt mit starken Endpoints

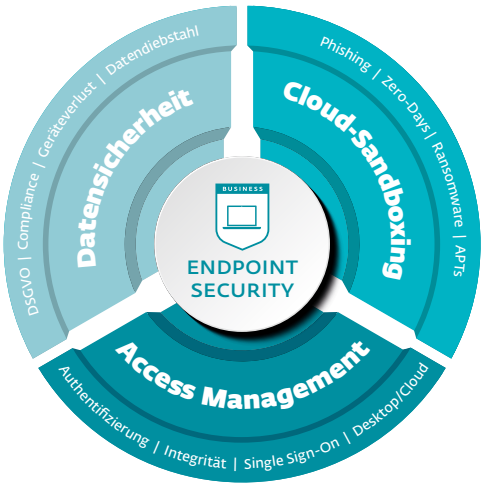
Patient Krankenhaus: **IT-Gesundheit beginnt mit starken Endpoints**

Sichere Rechner, sicheres Netzwerk: Die Erfolgsformel für malwarefreies Arbeiten in Krankenhäusern klingt einfach. Die Realisierung erfordert jedoch mehr als nur den Einsatz von Antivirenlösungen. Drei weitere Schutzmaßnahmen gelten bei Experten als zusätzliches Muss.

Manchmal braucht es leider besondere Umstände, die als Initialzünder längst überfällige Veränderungen vorantreiben. Ransomware-Vorfälle in Hospitälern und der Nachholbedarf in puncto Digitalisierung zeigen dies gerade in Bezug auf IT-Sicherheit in eindrucksvoller Weise auf. Klinik-Administratoren sollten jetzt die Chancen nutzen, die das Krankenhauszukunftsgesetz und die damit einhergehende Finanzspritze bieten. Durch die Erweiterung des vorhandenen Malwareschutzes mit Lösungen zur Festplattenverschlüsselung und Multi-Faktor-Authentifizierung sowie Cloud-Sandboxing verwandeln Administratoren und Laptops in den sogenannten Multi-Secured-Endpoint. Mit dieser Security-Vierer-kette sind sie überall perfekt gesichert: im Krankenhaus und im mobilen Einsatz gleichermaßen.

DATEN- UND NETZWERKZUGRIFF NUR MIT MULTI-FAKTOR-AUTHENTIFIZIERUNG

Für jeden Administrator ist es ein Albtraum, wenn sich jemand ins Netzwerk einloggt oder Daten aufruft, dessen Identität nicht eindeutig geklärt ist. Deshalb sollte eine Multi-Faktor-Authentifizierung als Mindestanforderung implementiert werden. Es befinden sich eine Reihe von Lösungen auf dem Markt, die einfach zu handhaben und kostengünstig in der Anschaffung sind. Beispielsweise ebnen professionelle Softwareprodukte den sicheren Zugang zu sensiblen Informationen und Netzwerkumgebungen. So lassen sich in weniger als einer Viertelstunde komplette Netzwerke mit tausenden von Rechnern ausstatten. Zusätzliche Hardware-Anschaffungen sind unnötig, bestehende Smartphones, FIDO-Sticks oder andere Token lassen sich leicht integrieren.



Die drei Kernbereiche des Multi-Secured-Endpoints

VERSCHLÜSSELUNG STOPPT DATENSCHNÜFFLER

Alle auf dem Endpoint gespeicherten Informationen sollten vor neugierigen Blicken oder im Verlustfall geschützt sein. Mit dem Einsatz einer Verschlüsselung schlagen Verantwortliche zwei Fliegen mit einer Klappe. Cyberkriminelle können mit den codierten Daten nichts anfangen und gleichzeitig kommt das Unternehmen Anforderungen aus der Datenschutzgrundverordnung nach. Voraussetzung für den Erfolg der Verschlüsselung ist die Akzeptanz des Anwenders. Deswegen sollte die Lösung bei ihrer täglichen Arbeit kaum „spürbar" und zuverlässig sein.

CLOUD-SANDBOXING HÄLT DAS POSTFACH SAUBER

Das Entdecken schädlicher E-Mails oder Downloads ist ein wichtiger Eckpfeiler für optimale Sicherheit. Gerade der Empfang von Office-Dokumenten, PDFs und zuweilen auch ausführbaren Dateien gehört zum Alltag im Krankenhaus. Nichts wäre schlimmer, als wenn durch dieses Schlupfloch beispielsweise Ransomware eindringt, die alle Daten verschlüsselt und unzugänglich macht. Abhilfe schaffen in diesem Fall Lösungen zur cloudbasierten Sandbox-Analyse. Suspekter und potenziell gefährlicher Binärcode wird in einer gesicherten Umgebung ausgeführt und erst bei negativem Befund in das Postfach übermittelt.

ESET PROTECT:
Impfstoff für die IT-Infrastruktur

In den vergangenen Jahren hat die Professionalisierung im eCrime Bereich nachweislich weiter zugenommen. Neben deutschen Mittelständlern geraten aber auch Krankenhäuser immer stärker in den Fokus von Cyber-Angreifern.

POSTFACH SAUBER

Die Unternehmensberatung Roland Berger stellte bereits 2017 fest, dass 64 Prozent der gut 2.000 Krankenhäuser in Deutschland Opfer eines Hackerangriffs wurden. Bund und Länder tragen dieser Entwicklung Rechnung und haben 2020 mit dem Krankenhauszukunftsgesetz die notwendigen Investitionsweichen gestellt: Von den insgesamt 4,3 Milliarden Euro zur Digitalisierung der Kliniken sollen mindestens 15 Prozent in die IT-Sicherheit der deutschen Kliniken gesteckt werden. Doch mit welchen Lösungen sind Krankenhäuser in der Lage, den Diebstahl von Patientendaten, Ransomware-Angriffe oder den unerlaubten Zugriff auf Rechner zu verhindern?

ANALYSIEREN UND HANDELN

Krankenhäuser müssen das Thema IT-Security als permanenten Prozess verstehen, der sich an verändernde Gefahrenpotenziale anpassen muss. Dafür ist es wichtig, die Ausgangslage und sich wandelnde Parameter genau zu erfassen. Konkret heißt das: Die eigene Situation sollte erst umfassend analysiert werden, um daraus den notwendigen Bedarf und das passgenaue Schutzniveau zu bestimmen. Das sollte idealerweise regelmäßig erfolgen, um neue Schwachstellen frühzeitig zu erkennen und sie mit entsprechenden Maßnahmen und IT-Security-Technologien und -Lösungen zu schließen. Doch vor welchen Herausforderungen stehen die Verantwortlichen? „In vielen Klinikbetrieben ist IT-Security noch immer nicht Chefsache. Das mangelnde Verständnis für ihre gewachsene Bedeutung zeigt sich darin, dass wir vielerorts noch klassischen Endpoint-Schutz als einzige Sicherheitsmaßnahme antreffen", so Maik Wetzel, Strategic Business Development Director DACH bei ESET. „Das ist in etwa so, als wenn Sie bei einem neuen Auto in puncto Sicherheit einzig und allein auf Ihre Stoßstange vertrauen. In modernen, digitalisierten Kliniken sind Cloud-Sandboxing, Endpoint Detection and Response, Multi-Faktor-Authentifizierung und Verschlüsselung unabdingbar. Es sind zudem dringend organisatorische und technische Maßnahmen notwendig, die dem heutigen Schutzbedarf angemessen sind. Ich denke hier insbesondere an die ISO 27001."

SINGLE VENDOR „MADE IN EU"

Eine der großen Herausforderungen stellen gerade im Gesundheitswesen Insellösungen dar, die nicht verzahnt in einander greifen. ESET hat dies frühzeitig erkannt und bietet Krankenhäusern mit seinem Multi-Secured-Endpoint-Ansatz ein am Markt einmaliges Lösungsportfolio an, das technologisch ausgereift ist und das nötige Schutzniveau gewährleistet. Der europäische Hersteller setzt dabei konsequent auf eigene Technologien – und das über alle gängigen Betriebssysteme hinweg, cloudbasiert oder On-premises. Vom Schutz der Clients, Server und Mobilgeräte über die Multi-Faktor-Authentifizierung bis hin zur Verschlüsselung können Kunden im Healthcare Sektor auf ESET vertrauen. Das sogenannte „Single Vendor Prinzip" vereinfacht es den Administratoren und reduziert zugleich den Kostenaufwand. Nahezu alle ESET Lösungen lassen sich über die Management-Konsole ESET PROTECT administrieren.

Secur IT y
made in EU
Trust Seal
www.teletrust.de/itsmie

ESET Sicherheit aus einem Guss basiert auf dem Bekenntnis zu Zero-Trust-Security, also dem vollumfänglichen Schutz aller Geräte, sowohl intern als auch extern. Damit geht ESET sogar einen Schritt weiter, als es das Bundesamt für Sicherheit in der Informationstechnik (BSI) fordert. Dies ist insbesondere für alle Krankenhäuser und Kliniken entscheidend, die als Kritische Infrastrukturen (KRITIS) eingestuft sind.

ESET PROTECT: PASSGENAUE SECURITY-BUNDLES FÜR JEDE ORGANISATIONSGRÖSSE

Das Herzstück der Lösungen ist die Management-Konsole **ESET PROTECT**, die sowohl cloudbasiert als auch On-Premises zur Verfügung steht. Die Konsole bietet einen kompletten Überblick über alle Endpoints in Echtzeit sowie die Verwaltung aller Geräte innerhalb und außerhalb einer Organisation.

ESET PROTECT Advanced wurde im Hinblick auf die stetig steigende Bedrohungslage, und daraus abgeleitet, auf die Bedürfnisse von mittleren Organisationsgrößen und MSPs optimiert. Das Bundle bietet Schutz für Clients, Mobilgeräte und Server, unter anderem auch vor Ransomware und Zero-Day-Bedrohungen, Sandboxing-Analyse sowie Datenschutz durch vollständige Festplattenverschlüsselung.

ESET PROTECT Complete beinhaltet zusätzlich Lösungen zum Schutz von Mailservern sowie genutzten Microsoft 365 Anwendungen..

ESET PROTECT Enterprise richtet sich an große Krankenhäuser und Klinikverbünde, für die eine umfassende Transparenz und strenge Sicherheitsanforderungen unerlässlich sind. Diese Variante bietet umfassenden Schutz für Unternehmenskunden mit einer der anpassungsfähigsten Endpoint Detection and Response Lösung auf dem Markt - dem ESET Inspect.

ESET PROTECT Mail Plus bietet einen dedizierten Schutz für Mailserver (bzw. die Absicherung des gesamten E-Mail-Verkehrs) in Verbindung mit Cloud-Sandboxing.

FLEXIBLE SICHERHEIT, DIE JEDERZEIT MITWÄCHST

Die ESET Bundles bieten eine hohe Flexibilität, denn sie eignen sich für den cloudbasierten oder On-premises Einsatz. Zudem können sie individuell erweitert werden, sowohl in der Anzahl der Lizenzen als auch mit weiteren Sicherheitslösungen. Ähnlich wie beim Autokauf kann der Kunde zum „Grundmodell" weitere Ausstattungen – wie beispielsweise Vollverschlüsselung oder Multi-Faktor-Authentifizierung – hinzubuchen. Die ESET PROTECT Bundles werden als klassische Lizenzvariante oder zum Teil auch als MSP-Modell angeboten.

PROTECT ENTRY	PROTECT ADVANCED	PROTECT COMPLETE	PROTECT ENTERPRISE	PROTECT MAIL PLUS
Zentrale Management-Konsole: ESET PROTECT (Cloud/ On-Premises) **Schutz von Clients, Mobilgeräten und Fileservern:** ESET Endpoint Security ESET Endpoint Antivirus ESET Server Security	**Enthält alle Komponenten von ESET PROTECT Entry sowie:** **Festplatten-verschlüsselung:** ESET Full Disk Encryption **Cloud-Sandboxing:** ESET LiveGuard Advanced	**Enthält alle Komponenten von ESET PROTECT Advanced sowie:** **Schutz von Mailservern:** ESET Mail Security **Schutz von MS 365 Anwendungen:** ESET Cloud Office Security (nur im Cloud-Bundle enthalten)	**Enthält alle Komponenten von ESET PROTECT Advanced sowie:** **Detection and Response:** ESET Inspect (Cloud/ On-Premises)	**Zentrale Management-Konsole:** ESET PROTECT (Cloud/ On-Premises) **Cloud-Sandboxing:** ESET LiveGuard Advanced **Schutz von Mailservern:** ESET Mail Security

Ergänzen Sie Ihr Bundle um weitere ESET Sicherheitslösungen:

MULTI-FAKTOR-AUTHENTIFIZIERUNG
(ESET SECURE AUTHENTICATION)

VOLLWERTIGE VERSCHLÜSSELUNG
(ESET ENDPOINT ENCRYPTION)

SCHUTZ VON MICROSOFT SHAREPOINT SERVERN
(ESET SECURITY FÜR MICROSOFT SHAREPOINT SERVER)

ESET SERVICES
(ESET SECURITY SERVICES & ESET PREMIUM SUPPORT SERVICES)

ESET PROTECT Bundles: Umfassendes Lösungsportfolio für den Gesundheitssektor.

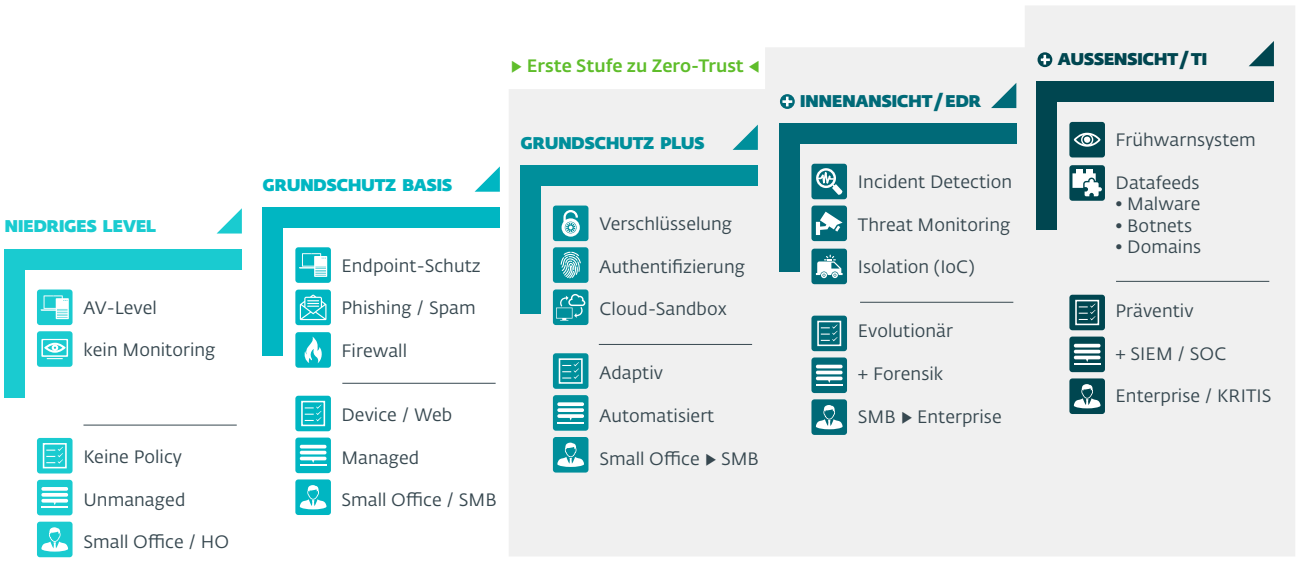
NEUER SICHERHEITSANSATZ ZERO-TRUST-SECURITY

ESETs Strategieansatz basiert auf dem von der Harvard Universität konzipierten Zero-Trust-Konzept zur IT-Sicherheit. Diese konzeptionelle Basis hat ESET aufgegriffen, weiterentwickelt und auf die Bedürfnisse unterschiedlicher Organisationsgrößen zugeschnitten. Kurz gesagt geht es darum, alle internen und externen Geräte, Prozesse und Personen grundsätzlich als potentiell gefährlich einzustufen. In Zeiten von Corona und Home-Office hat sich das als zwingend erforderlich erwiesen.

Der Zero-Trust-Security-Ansatz von ESET besteht aus einem dreistufigen, aufeinander aufbauenden Reifegradmodell. Je höher die Stufe ist, desto sicherer ist die Schutzwirkung – also „reifer". Das Modell startet mit der Basisstufe „Grundschutz Plus", die dem Prinzip des Multi-Secured-Endpoints folgt. Diese eignet sich unabhängig vom individuellen Schutzbedarf für jede Organisation im Gesundheitswesen. Daran schließen sich zwei Zero-Trust-Stufen mit weiter steigenden Security-Maßnahmen und -Diensten an.

Die ESET PROTECT Bundles sowie alle ergänzenden ESET Lösungen sind bei allen ESET-Fachhändlern in Deutschland verfügbar.

Weitere Informationen erhalten Sie auch unter www.eset.de.



Das ESET Reifegradmodell zeigt, was für die Umsetzung des Zero-Trust-Security-Konzepts wichtig ist.

Digital Security
Progress. Protected.

ÜBER ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Unternehmensgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihr Netzwerk mit Hilfe von Cloud-Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungsprodukte unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen.

Unsere XDR-Basis mit Endpoint Detection and Response Lösung, Frühwarnsysteme (bspw. Threat Intelligence) und dedizierte Services ergänzen das Angebot im Hinblick auf Forensik sowie den gezielten Schutz vor Cyberkriminalität und APTs. Dabei setzt ESET nicht nur allein auf Next-Gen-Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

ZUFRIEDENE KUNDEN

BVB 09 Champion Partner

Seit 2019 ein starkes Team
auf dem Feld und digital

Allianz Suisse

Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Secur|Ty made in EU
Trust Seal
www.teletrust.de/itsmie

ESET wurde das Vertrauenssiegel
„IT Security made in EU" verliehen

CERTIFIED ISO 9001:2015 COMPANY
CERTIFIED ISO 27001:2013 COMPANY

Unsere Lösungen sind nach
Qualitätsstandards zertifiziert

ESET IN ZAHLEN

110+ Mio.
Geschützte Nutzer weltweit

400k+
Geschützte Unternehmen

200+
Länder & Regionen

13
Forschungs- und Entwicklungs-zentren weltweit

welivesecurity by eset

ESET Deutschland GmbH | Spitzweidenweg 32 | 07743 Jena | Tel.:+49 3641 3114 200

ESET.DE | ESET.AT | ESET.CH