Lenovo
Health

# Allgegenwärtiger Gesundheitsdatenschutz

Ein **intelligenter** Ansatz zur Abwehr aufkommender Bedrohungen

ThinkShield

Windows 10

Smarter technology for all

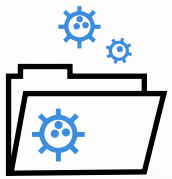
Lenovo

# Für die IT-Sicherheit im Gesundheitswesen wird es auch in der Zukunft nicht einfacher

Wenn Sie Führungskräfte danach fragen, was ihnen schlaflose Nächte bereitet, können Sie sicher sein, dass Cyberbedrohungen zu den Faktoren ganz oben auf der Liste gehören. Dies trifft insbesondere auf die Gesundheitsbranche zu, die am häufigsten von Hackern ins Visier genommen wird.

Patientenakten sind die wertvollsten Informationen, die im Darknet verfügbar sind, weil sie eine große Vielfalt an Informationen enthalten, darunter Geburtsdatum, Kreditkarteninformationen, Sozialversicherungsnummer, Wohnanschrift und E-Mail-Adresse. Eine einzelne Patientenakte kann bis zu 850 Euro einbringen.[1]

Bei einer solchen Summe ist es daher nicht weiter verwunderlich, dass die Angriffe auf Gesundheitsdaten von Jahr zu Jahr zunehmen.



Im Jahr 2019 wurden 41 Millionen Patientenakten gehackt – fast dreimal so viele wie 2018.[2]

**STEIGENDE KOSTEN DURCH GESUNDHEITSDATENMISSBRAUCH**

Die aus Datenmissbrauch resultierenden Kosten für Gesundheitseinrichtungen steigen weiter an. Datensicherheitsverletzungen kosten den Gesundheitssektor im Durchschnitt 5,5 Millionen Euro. Das ist über 60 Prozent mehr als in allen anderen Sektoren. Es handelt sich dabei um 365 Euro für jeden im Jahr 2019 verloren gegangenen oder gestohlenen Datensatz im Vergleich zu 348 Euro pro Datensatz im Jahr 2018.[3]

**MAAS (MALWARE-AS-A-SERVICE)**

Heute gibt es aufgrund der Verbreitung hochentwickelter Hackertools mehr Bedrohungen für die Gesundheits-IT. Cyberkriminelle müssen nicht mehr komplexen Code schreiben, um einen Angriff zu starten – die Ressourcen sind nur einen Klick entfernt. Websites bieten jetzt Malware-as-a-Service an.[4]

Lenovo Windows 10

# Eine zunehmend komplexe Landschaft

Die Veränderungen im Gesundheitswesen können die Abwehr von aufkommenden und zunehmenden Bedrohungen erschweren.

**Steigende Mobilität führt zu einer Zunahme der Angriffsmöglichkeiten**
Einer der deutlichsten Trends, der sich auf die Sicherheit auswirkt, ist der immense Zuwachs an Mobiltechnologie. Eine kürzliche Befragung von Führungskräften aus der Gesundheits-IT-Branche ergab, dass derzeit 90 Prozent ein Mobilitätsprogramm einführen oder dies planen.[5]

Mit zunehmender Anzahl von Endgeräten und dem steigenden Datenverkehr in immer mehr Netzwerken vergrößert sich der durch Bedrohungen gefährdete Bereich sehr schnell. Wie das National Institute of Standards and Technology (NIST) in seiner neuesten Publikation bekannt gab, sind Patientendaten, die gesammelt, gespeichert, verarbeitet oder auf Mobilgeräte übertragen werden, für Angriffe besonders anfällig.[6]

Dennoch haben laut der HIMSS Cybersecurity Survey weniger als fünf Prozent der Befragten Mobilgeräte in ihren Penetrationstest einbezogen.[7]

Die zunehmende Mobilität von Gesundheitsdienstleistern und Pflegediensten stellt eine bedeutende Herausforderung für Gesundheits-IT-Teams dar, von denen viele selbst remote arbeiten.

**Vorschriften und Konformität**
Jede Technologielösung muss anhand eines zusätzlichen Kriteriums bewertet werden, bevor sie für den Einsatz im Gesundheitswesen als nutzbringend betrachtet werden kann. Hilft diese Lösung dem Unternehmen, strengste regulatorische Standards einzuhalten?

Technologien, die Sicherheitsstandards in anderen Branchen erfüllen, entsprechen möglicherweise nicht den HIPAA-Standards zum Patientendatenschutz oder den Richtlinien für die elektronische Verschreibung kontrollierter Substanzen (EPCS).

**Sicherheit versus Zweckmäßigkeit**
Immer mehr Sicherheitsvorkehrungen werden in den Pflegeprozess eingebunden, während Mediziner weiterhin bestrebt sind, so schnell wie möglich lebensrettende Patientenfürsorge zu leisten. Sicherheitsebenen können Pflegeprozesse unterbrechen, erheblich verzögern und sich negativ auf die Behandlungsergebnisse auswirken. Mediziner vergeuden allein schon mit der An- und Abmeldung an Computersystemen 45 Minuten Arbeitszeit pro Schicht.8 Als Folge davon geben 41 % der Gesundheitseinrichtungen an, wissentlich die Sicherheit zugunsten der Zweckmäßigkeit oder Business Performance vernachlässigt zu haben.[9]

**Für die Sicherheit ist ein patientenorientierter Ansatz erforderlich**
Das IT-Sicherheitskonzept im Gesundheitswesen muss einerseits lückenlos sowie vollumfänglich sein, andererseits muss dieses Konzept auch der Arbeitsweise des Gesundheitspersonals entsprechen. Außerdem muss die IT-Sicherheit die Arbeitsprozesse der Fachkräfte im Gesundheitswesen unterstützen, ohne dass dadurch die Sicherheit der Unternehmensdaten gefährdet ist.

# Sicherheit durch Design

## Ein intelligenter Ansatz für IT-Sicherheit im Gesundheitswesen.

ThinkShield ist eine anpassbare Sicherheitslösung, die für einen umfassenden End-to-End-Schutz Ihrer wichtigen Daten und Geschäftstechnologien sorgt. Es handelt sich nicht um ein eigenständiges Produkt, sondern um eine einzigartige Kombination aus Hardware, Software, Services und Prozessen, die in Lenovo Geräte integriert sind. Auf diese Weise wird die IT im Gesundheitswesen in vier Schlüsselbereichen geschützt.

Die Sicherheit durch Design beginnt mit der Entwicklung von Standardsicherheitsanforderungen für jedes Gerät, um Schutz vor der aktuellen und sich ständig weiterentwickelnden Bedrohungslandschaft zu bieten.

Dieser Ansatz setzt sich mit dem Schutz unserer Lieferkette durch stabile und zuverlässige Richtlinien und Verfahren fort.

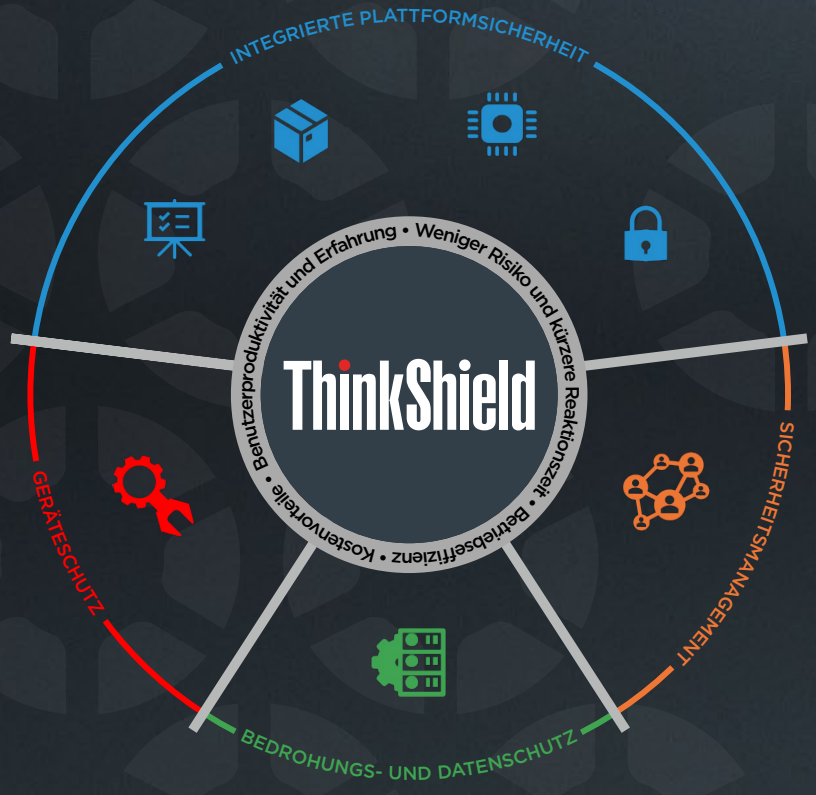
Unser Trusted Supplier Program ist ein strenger Prüfprozess, der sicherstellt, dass jeder Lieferant von Komponenten und Software für Lenovo die höchsten Sicherheitsstandards über die gesamte Lieferkette hinweg erfüllt. Zu den Anforderungen für Lieferanten zählen vierteljährliche Konformitätsbewertungen, Prüfungen des Bestandsschutzes vor Ort und die Umsetzung der bedarfsorientierten Kontrolle der Informationssicherheit und logistischer Prozesse.

ThinkShield hilft bei der Realisierung von Datenschutz und Sicherheit in der Gesundheits-IT-Umgebung.

# Sicherheitsfunktionen von Windows

## Einfache, flexible Verwaltung.

Windows 10 Pro vereinfacht die Verwaltung von Identitäten, Geräten und Anwendungen, sodass Sie sich auf Ihre Tätigkeit konzentrieren können. In einem sich schnell ändernden Umfeld wird der Geschäftserfolg dadurch bestimmt, wie gut Sie sich anpassen können, ohne an Tempo zu verlieren. Verbinden Sie sich ganz einfach mit vorhandenen Unternehmensnetzwerken sowie moderner cloudbasierter Verwaltung. Mit der intuitiven Kontrolle über Ihre IT-Infrastruktur ist Ihr Unternehmen auf alles vorbereitet.




**INTEGRIERTE PLATTFORMSICHERHEIT**
Unser ganzheitlicher Ansatz für Sicherheit beginnt mit integrierten ThinkShield Sicherheitslösungen, die standardmäßig im Lieferumfang unserer branchenführenden Think® Geräte enthalten sind.

**GERÄTESCHUTZ**
Hardwareschutzfunktionen und Serviceangebote bilden eine weitere Schicht des Geräteschutzes.

**BEDROHUNGS- UND DATENSCHUTZ**
Sicherheitslösungen, die sich nahtlos in Lenovo Geräte integrieren lassen, sorgen für den Schutz Ihrer kritischen Daten und Geschäftstechnologien.

**SICHERHEITSMANAGEMENT**
Lösungen, die Möglichkeiten zur Bereitstellung, Überwachung und Meldung von IT-Bestand bieten.

Lenovo Windows 10

# Datenschutz – Sicherheit für Patientendaten und im Klinikalltag

Die Gesundheitsfürsorge unterliegt einem ständigen Wandel, und Sicherheitsmaßnahmen müssen mit dieser Entwicklung Schritt halten. Es lässt sich nicht immer leicht feststellen, wer in einer Schicht auf einen Gerätebildschirm schaut. Aus diesem Grunde bieten wir PrivacyGuard und Schutz gegen Shoulder Surfing an.

**PrivacyGuard** bietet einen integrierten elektronischen Blickschutzfilter, der verhindert, dass andere Ihnen über die Schulter schauen, um so an wertvolle Informationen zu gelangen. Dadurch werden keine Blickschutzfilter von Drittanbietern mehr benötigt, die häufig verloren gehen oder weggeworfen werden und ersetzt werden müssen. Ein vorinstallierter elektronischer Blickschutzfilter ist sicherer und sorgt dafür, dass sich das IT-Team und die Benutzer um eine Sache weniger kümmern müssen.

**Schutz gegen Shoulder Surfing** enthält Blickerkennungstechnologie, die den Benutzer benachrichtigt, wenn eine andere Person auf den Bildschirm schaut. Außerdem wird erkannt, von welcher Seite aus die Person den Bildschirm im Blick hat. Dank der Blickerkennung wird der Bildschirm unscharf, sobald der Benutzer wegschaut.

Der Schutz gegen Shoulder Surfing enthält eine integrierte Anwesenheitserkennung, die das Gerät sperrt, um für Sicherheit zu sorgen, wenn der Benutzer seinen Arbeitsplatz verlässt.

**Zur integrierten ThinkShield Plattformsicherheit** gehört außerdem eine Webcam-Kameraabdeckung für sowohl normale als auch IR-Kameras. Diese mechanische Kameraabdeckung gibt Patienten und Benutzern die Gewissheit, dass die Kamera nicht eingeschaltet und vor Hackern sicher ist.

Der Datenschutzansatz von ThinkShield umfasst den gesamten Gerätelebenszyklus und schließt mehrere Optionen zur sicheren Entsorgung ein, um die Privatsphäre des Patienten zu schützen.

**Die sichere Löschfunktion** im BIOS entfernt zuverlässig alle Daten aus einem Datenträger, ohne dass externe Tools erforderlich sind.

**„Keep Your Drive"** -Service (Einbehalten der Festplatte) erlaubt Kunden im Falle eines Geräteausfalls die Festplatte zu behalten und macht die Nachverfolgung des Versandwegs von Festplatten überflüssig.

**THE THINKPAD® T14i HEALTHCARE EDITION**
All diese ThinkShield Funktionen finden Sie in der ThinkPad T14i Healthcare Edition. Der auf die Bedürfnisse im Medizinbereich zugeschnittene Funktionsumfang dieses leistungsstarken Notebooks hat die ThinkPad® Produktfamilie auf globaler Ebene zur ersten Wahl bei Beschäftigten im Gesundheitswesen gemacht.

Lenovo Windows 10

# Sicherheit – Gewährleistung der Sicherheit von Patienten durch Minimierung von Infektionsgefahren

Die Einhaltung der Vorschriften zur Infektionsprävention ist heute wichtiger als je zuvor. Schließlich verweist die wachsende Anzahl von Veröffentlichungen darauf, dass der Grad der bakteriellen Verunreinigung der Mobilgeräte, die von Beschäftigten im Gesundheitswesen verwendet werden, von 40 bis fast 100 Prozent reicht – daher ist es höchst erstaunlich, dass 90 Prozent der Gesundheitsdienstleister, die mit Patienten in Kontakt kommen, nie ihre Mobiltelefone reinigen.[10]

Es gibt aber auch gute Nachrichten. Die Kontamination mit Krankenhauskeimen kann bereits mit relativ geringem Aufwand reduziert werden. Laut einer Untersuchung kann eine Kontamination innerhalb von fünf Minuten durch einfache Verwendung eines antibakteriellen feuchten Reinigungstuchs um 36 bis 100 Prozent verringert werden.11 Eine andere Untersuchung belegte eine Keimreduktion um 50 % durch 70-prozentiges Isopropanol und 15 Sekunden Reibung.[12]

In einer in einem Krankenhaus durchgeführten Untersuchung wurden Krankheitserreger nachgewiesen, die sich auf 80 Prozent der dort verwendeten Mobiltelefone und auf 81 Prozent der Hände der Mediziner befanden, die diese Telefone benutzten.[13]

Lenovo nimmt den Schutz der Gesundheit und Sicherheit von Krankenhauspersonal und Patienten sehr ernst. Aus diesem Grunde weisen unsere Notebooks für den Gesundheitsbereich u. a. folgende spezielle Merkmale auf:

- antimikrobielle Oberflächenbehandlung, die mit ISO 22196 konform ist
- umfangreiche Prüfung nach CDC-Standards auf Festigkeit gegen intensive Reinigung über die Dauer eines Tages mit anerkannten Markenprodukten wie Virox Accel Wipes, PDI Germicidal Wipes und B. Braun Meliseptol
- Beständigkeit bei einem Abwischen von bis zu 10.000 Mal während der Lebensdauer des Geräts
- Lenovo Quick Clean Funktion ermöglicht die vorübergehende Deaktivierung der Benutzereingaben, damit rasches Abwischen möglich ist, ohne das Gerät abzuschalten
- Lenovo Quick Clean Timer kann dabei so eingestellt werden, um für eine angemessene Zeitdauer zur ordnungsgemäßen Reinigung und Desinfektion zu sorgen
- nach Militärstandards auf Haltbarkeit getestet und übersteht hohe Luftfeuchtigkeit, niedrige/hohe Temperaturen, Staub, Vibrationen und Schimmel

Krankenhausbedingte Infektionen betreffen In den USA einen von 25 hospitalisierten Patienten und führen zum Verlust von zehntausenden Leben sowie Kosten von Milliarden von Dollar für das Gesundheitswesen. Verfahren zur Infektionsverhinderung wie diese können krankenhausbedingte Infektionen jedoch um bis zu 70 Prozent verringern.[14]

Lenovo Windows 10

# Sicherheit – Authentifizierung und Daten

Die Beschränkung des Datenzugriffs auf autorisierte Benutzer ist ein Meilenstein auf dem Weg zu mehr Schutz personenbezogener Daten im Gesundheitswesen. ThinkShield bietet dabei mehrere Möglichkeiten zur Verifizierung der Identität eines Benutzers, einschließlich ganzheitlicher Multifaktor-Authentifizierung.

**NETZWERKSICHERHEIT**
auf der Basis der IP-Adresse des Geräts

**GPS-SICHERHEIT**
auf der Basis des geografischen Standorts

**GESICHTSERKENNUNG**
Infrarotkameras, die Windows Hello unterstützen

**BLUETOOTH**
Authentifizierung über die Bluetooth-Umgebung von Smartphones

**PASSWÖRTER UND PINS**
Intel Authenticate Secure PIN, PINs für Windows 10 und visuelle PINs

**„MATCH ON CHIP"-FINGERABDRUCKSENSOR**
enthält Anti-Spoofing-Technologie mit Quantum Matcher

**FIPS 201-KONFORMITÄT**
übertrifft die Anforderungen für EPCS

**NFC**
sichere NFC-Anmeldung durch Antippen, unterstützt von allen bekannten Single Sign-on-Anbietern, einschließlich Imprivata®

Die Integration all dieser Funktionen bedeutet, dass durch ThinkShield geschützte Geräte ohne zusätzliche Hardware nahtlos in bestehende Sicherheitsverfahren eingebunden werden können.

Lenovo Windows 10

**ZEITERSPARNIS DURCH UMSTELLUNG AUF EINMALANMELDUNG**

Eine kürzlich durchgeführte Untersuchung zeigte, dass ein Krankenhaus die durchschnittliche Anmeldezeit von Medizinern mit einer einmaligen Anmeldung (SSO) von 29,3 auf 8,9 Sekunden senken konnte – auf diese Weise wurde eine Zeitersparnis von 69 Prozent erzielt. Im Laufe einer Woche kommen so 49,7 Stunden oder etwa vier 12-Stunden-Schichten zusammen.[15]

# Sicherheit – Endpoint Protection in Echtzeit

ThinkShield bietet Funktionen, die speziell für Endpunktsicherheit in Echtzeit für Gesundheitseinrichtungen entwickelt wurden.

**SentinelOne – autonome Endpunktsicherheit**
SentinelOne bietet Virenschutz der nächsten Generation durch patentierte verhaltensorientierte künstliche Intelligenz. Diese hochentwickelte autonome Bedrohungserkennung bietet vollständigen Ersatz für eine Virenschutzlösung und kann eine aktive Erkennung und Abwehr von Bedrohungen an Endpunkten (EDR) integrieren, wodurch die Geräte nach breit angelegten Angriffen die erforderlichen Maßnahmen umgehend einleiten.

**WinMagic – Laufwerksverschlüsselung**
Eine in hohem Maße konfigurierbare, umfassende Verschlüsselung für die Unternehmensumgebung zum Schutz von vertraulichen Informationen, die auf Geräten gespeichert sind. Die zentrale Verschlüsselungsverwaltung eignet sich für Geräte auf allen Plattformen, z. B. SecureDoc-Laufwerksverschlüsselung, FileVault 2, BitLocker, dm-crypt und selbstverschlüsselnde Laufwerke. Einfache Verfolgung der Verschlüsselung und Verwaltung von Schlüsseln für SecureDoc-Geräte und Anwendungen, Plattformen sowie Einheiten von Drittanbietern über eine einzige Konsole.

**Absolute® – Sichtbarkeit und Kontrolle von Endpunkten**
Absolute ist eine in die Geräte-Firmware direkt eingebundene Lösung für die Sichtbarkeit und Kontrolle von Endpunkten, die ein zuverlässiges Sicherheitsmanagement ermöglicht. Durch automatisierte Endpunkt-Widerstandsfähigkeit werden die Möglichkeiten zur Selbstreparatur unterstützt. Die in Echtzeit gesteuerte Wiederherstellung erlaubt die Fernuntersuchung von potenziellen Bedrohungen und die Einleitung von Maßnahmen, wenn ein sicherheitsrelevanter Vorfall eintritt.

**Lenovo WiFi Security – Datenschutz innerhalb und außerhalb des Unternehmens**
Lenovo WiFi Security erkennt automatisch verdächtige Aktivitäten und schützt Geräte vor Angriffen über WLAN-Netzwerke. Wenn ein Benutzer sich nicht auf dem Firmengelände befindet, prüft der lokale Agent die Einzelheiten des Zugangspunks auf Schwachstellen, führt eine lokale Risikoanalyse durch und warnt Benutzer vor verdächtigen Aktivitäten am Zugangspunkt.


**LENOVO VIRTUAL ROUNDING**

Erfahren Sie, wie die von Lenovo bereitgestellte Lösung Virtual Rounding für eine sichere persönliche Kommunikation im Medizinbereich sorgt und gleichzeitig dabei hilft, die Ausbreitung von krankenhausbedingten Infektionen einzudämmen.

# Perfekte Kombination aus Schutz und Produktivität

Der Schutz von Patientendaten vor externen Bedrohungen und interner Offenlegung ist eine nie endende Herausforderung. Gleichzeitig müssen Sicherheitsmaßnahmen die dynamischen Arbeitsabläufe unterstützen, die im heutigen Medizinbereich zu finden sind und bei Bedarf den rechtzeitigen Zugriff auf Patientendaten ermöglichen.

Die durch ThinkShield geschützten Lenovo Notebooks für den Gesundheitsbereich tragen dazu bei, diese Balance zu erreichen – wobei leistungsstarke Funktionen für Datenschutz und Sicherheit im modernen Gesundheitswesen sorgen.

Weitere Informationen finden Sie unter
**techtoday.lenovo.com/de/de/solutions/healthcare**

Lenovo Windows 10

# Smartere Gesundheitsdienstleistungen mit Lenovo Health

Windows 10

Setzen Sie auf Lenovo Health. Wir unterstützen Sie dabei, Hindernisse zu überwinden und intelligente Lösungen bereitzustellen. Sind Sie bereit, loszulegen? Wir stehen Ihnen gerne zur Seite.

Weitere Informationen erhalten Sie bei Ihrem Lenovo Ansprechpartner oder Ihrem Business Partner vor Ort

Weitere Informationen finden Sie unter **www.lenovo.com/health**


**QUELLEN**

1 https://www.beckershospitalreview.com/cybersecurity/patient-medical-records-sell-for-1k-on-dark-web.html

2 https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats

3 https://healthitsecurity.com/news/data-breaches-cost-healthcare-6.5m-or-429-per-patient-record

4 https://www.itprotoday.com/cloud-security/malware-taking-new-shape-malware-service

5 https://healthitsecurity.com/news/mobile-devices-in-healthcare-increase-as-do-security-challenges

6 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-1.pdf

7 https://www.healthcareitnews.com/news/protecting-endpoints

8 Von Imprivata bereitgestellte Statistik zum Webinar „Shielding Healthcare Data from Cyberthreats: Tools You Can Use from A to V“, Mai 2019.

9 Von Imprivata bereitgestellte Statistik zum Webinar „Shielding Healthcare Data from Cyberthreats: Tools You Can Use from A to V“, Mai 2019.

10 https://orb.binghamton.edu/cgi/viewcontent.cgi?article=1001&context=alpenglowjournal

11 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6210060/

12 https://www.myamericannurse.com/mobile-devices-healthcare-associatedinfections/

13 https://www.healthcareitnews.com/news/ensuring-computers-notebooks-andmobile-devices-are-included-disinfection-mix

14 https://www.healthypeople.gov/2020/topics-objectives/topic/healthcareassociated-Infections

15 https://www.beckershospitalreview.com/healthcare-information-technology/how-single-sign-on-within-ehrs-can-save-clinicians-time-reduce-hospital-costs-improve-patient-care.html




Lenovo