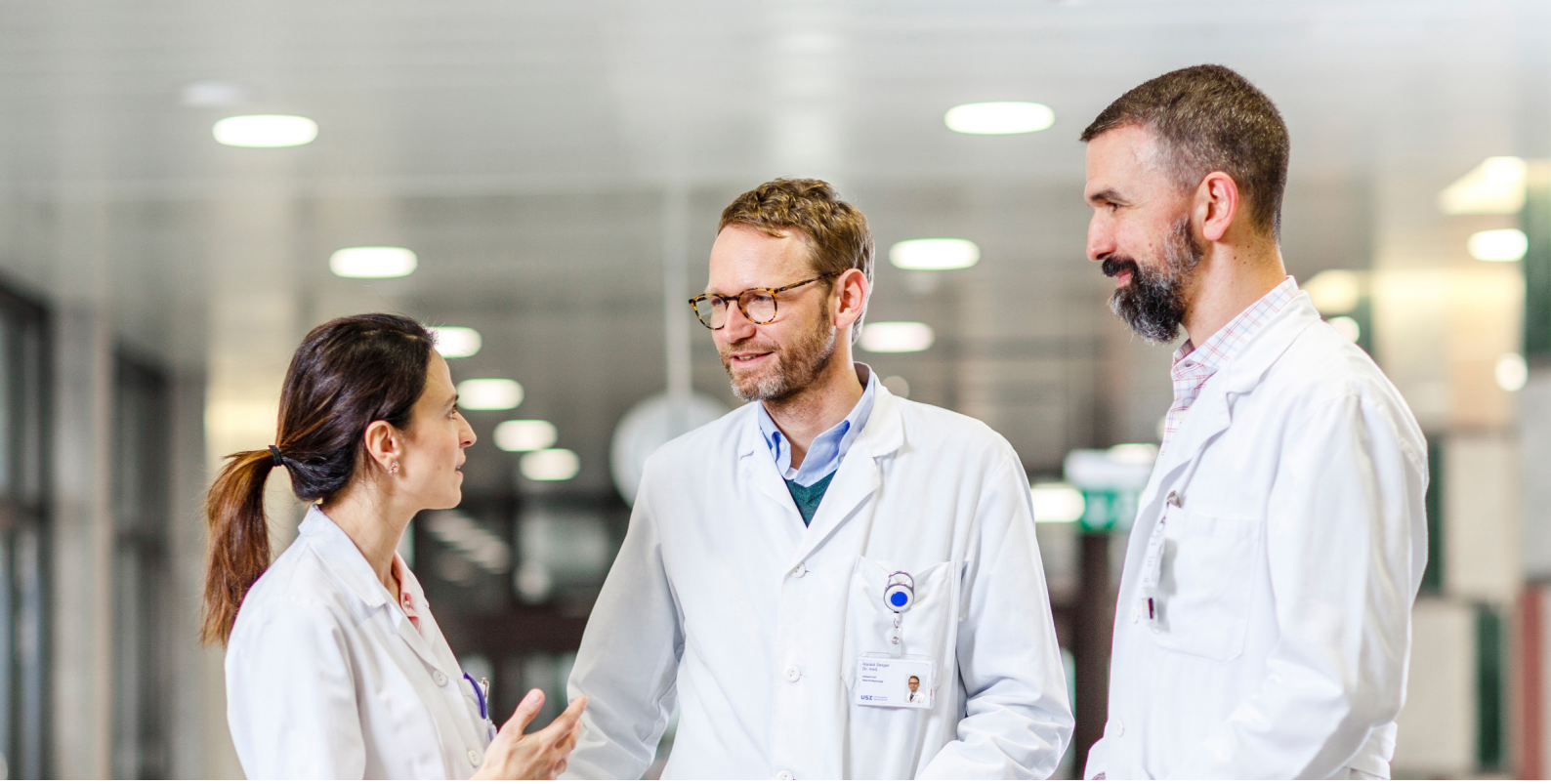


Quelle: Universitätsspital Zürich

FALLSTUDIE

100% Threat Protection für eine sicherere und umfangreicherere medizinische Versorgung

Seit dem Wechsel zur Endpoint Security Lösung von Palo Alto Networks werden erheblich mehr Malwarebedrohungen erkannt und blockiert – das 2,5-fache der zuvor eingesetzten Lösung. So kann eine erstklassige medizinische Versorgung gewährleistet werden, im Wissen, vor Malwareangriffen bestmöglich nach state-of-the-art geschützt zu sein.

paloalto NETWORKS

IN KÜRZE

Kunde

Universitätsspital Zürich

Produkte und Dienstleistungen

Kritische medizinische Versorgung

Partner

Omicron AG

Branche

Gesundheitswesen

Unternehmensgrösse

8.400+ Mitarbeiter

Land

Schweiz

Herausforderung

Das Universitätsspital Zürich benötigte eine konsistentere Sicherheit, um Patienten, Mitarbeiter und 13.000 verteilte Endpunkte effektiv zu schützen.

Anforderungen

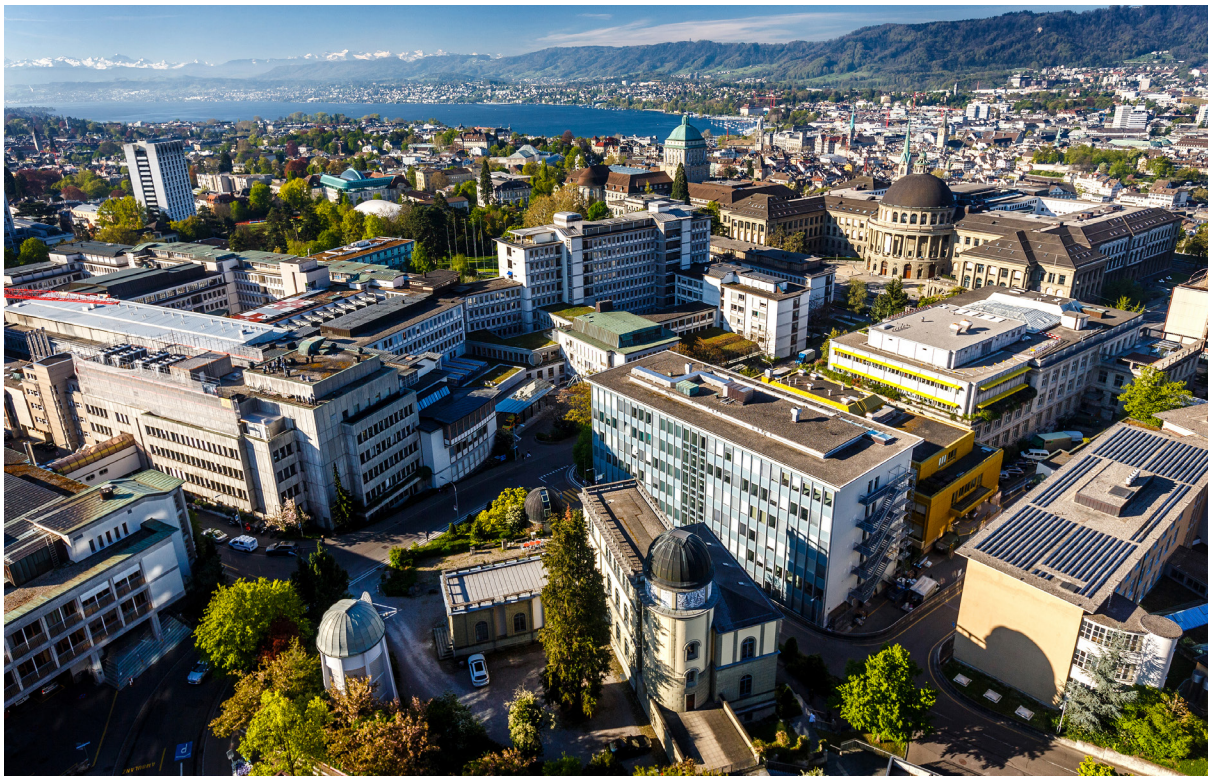
+ Effektiverer Schutz vor modernen Bedrohungen
+ Unterstützung virtueller Umgebungen
+ Geringere CPU-Auslastung

Lösung

Durch die Migration zunächst zu Palo Alto Networks Traps™ und später zu Cortex® XDR™ wurde modernste Sicherheit erreicht, um das Risiko für die sensiblen Daten des USZ zu minimieren.

Kritischer Schutz für 13.000 verteilte Endpunkte

Einrichtungen des Gesundheitswesens müssen heute ihre kritischen Daten und Infrastrukturen vor einer ständig wachsenden Zahl automatisierter, ausgeklügelter Angriffe schützen. Da bei fast jedem Malwareangriff mindestens ein Endpunkt infiltriert wird, ist es unverzichtbar, allen Benutzern und Endpunkten den bestmöglichen Schutz zu bieten, ganz gleich, wo sie sich befinden. Das USZ ist ein hervorragendes Beispiel dafür, wie dies mit der richtigen Technologie und den richtigen Partnern einfach und effektiv möglich ist.

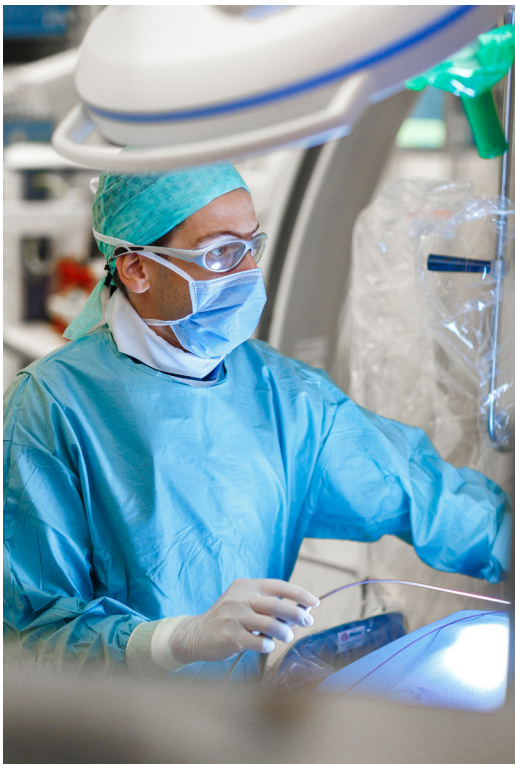


Quelle: Universitätsspital Zürich

Als eines der ältesten und angesehensten Krankenhäuser Europas behandelt das USZ jährlich hunderttausende Patienten.

HERAUSFORDERUNG

Erweiterung des modernen Endpunktschutzes für moderne medizinische Versorgung, überall



Quelle: Universitätsspital Zürich

Jedes Jahr behandelt das USZ fast 650.000 Patienten in seinen medizinischen Einrichtungen, Kliniken und Instituten. Es beschäftigt mehr als 8.400 medizinische und administrative Mitarbeiter und nutzt über 13.000 Desktopcomputer, mobile Geräte und andere Endpunkte. Als Verantwortlicher für Endpoint Security des USZ hat Tom Schütt die Aufgabe, seine Mitarbeiter und Endgeräte vor Angriffen zu schützen.

„Wir müssen unbedingt das gesamte Netzwerk sichern“, erklärt Schütt. „Es ist daher unerlässlich, dass unsere Endpunkt Sicherheitslösung auf dem neuesten Stand der Technologie ist, um Risiken zu minimieren.“

Im Jahr 2018 erkannte Schütts Team, dass es eine effektivere Endpunkt Sicherheitslösung benötigte, als seine bestehende On-Premises-Lösung bieten konnte.

Durch die Omicron AG erfuhr Tom Schütt von der ausgefeilten Endpoint Security Lösung Traps und führte daraufhin einen Proof of Concept (PoC) durch. „Bei unserer Softwareevaluierung war Traps der klare Sieger“, erinnert sich Schütt. „Der wichtigste Faktor bei einer solchen Lösung ist ihre Fähigkeit, Malware zu erkennen, und das kann Traps wirklich gut.“ Um die spezifischen Anforderungen zu optimieren, wurden wir von der Omicron AG tatkräftig unterstützt.

> Es ist unerlässlich, dass unsere Endpunkt Sicherheitslösung auf dem neuesten technologischen Stand ist, um Risiken zu minimieren. Bei unserer Softwareevaluierung war Traps der klare Sieger.
>
> **– Tom Schütt, Verantwortlicher für Endpoint Security**

ANFORDERUNGEN

Abwehr von Malware mit hervorragender Skalierbarkeit und minimaler Bandbreitenbelastung

Das USZ verglich beim PoC anhand einer umfassenden Auswahl der neuesten Malware die Leistung seiner bestehenden Endpunkt Sicherheitslösung mit derjenigen von Traps. Das Ergebnis: Traps erkannte und blockierte erfolgreich 100% der Bedrohungen, die bestehende Lösung hingegen nur 40%. Mit anderen Worten: Traps erkannte und blockierte 2,5mal so viele bösartige Dateien. Der PoC zeigte auch die Stärke der Sicherheitslösung von Palo Alto Networks gegenüber Metasploit-Penetrationtests auf isolierten Systemen.

Im Jahr 2019 brachte Palo Alto Networks Cortex® XDR™ auf den Markt, eine neue Generation des Endpunktschutzes, der Erkennung wie auch Reaktionslösung, welche auf der Technologie von Traps aufbaut und eine KI- und ML-basierte Abwehr einschliesslich Verhaltensanalysen umfasst. Das USZ wusste, dass dies die richtige Lösung war, um sich vor immer komplexeren Bedrohungen zu schützen. Mit der Installation von Cortex XDR war das USZ besser gegen alle Malwareherausforderungen gewappnet, beginnend mit der COVID-19-Pandemie.

LÖSUNG

Cortex XDR bietet einen bahnbrechenden Schutz

Wie viele andere IT-Abteilungen auf der ganzen Welt musste das USZ Anfang 2020 plötzlich Tausende von Mitarbeitern schützen, die wegen der Pandemie ins Homeoffice wechselten.

„Die Endpunktsicherheit ist während der COVID-19-Pandemie natürlich noch wichtiger geworden – zum einen, weil das USZ kritische Infrastrukturen betreibt, und zum anderen, weil seit Beginn des Lockdowns im Frühjahr 2020 viele Mitarbeiter, vor allem in der Verwaltung, von zu Hause aus arbeiten."

Mithilfe von maschinellem Lernen analysiert Cortex XDR kontinuierlich das Verhalten von Endpunkten, Netzwerken und Benutzern, um auch die unauffälligsten Angriffe aufzudecken. Als Cloud-Technologie bot Cortex XDR Schütt und seinem Team die besten Voraussetzungen, um mehr als 3.000 mobile Mitarbeiter umgehend zu schützen.

> Die Endpunkt Sicherheit ist während der COVID-19-Pandemie natürlich noch wichtiger geworden.
>
> **– Tom Schütt, Verantwortlicher für Endpoint Security**

VORTEILE

KI- und ML-gestützte Erkennung blockierte effektiv 100% der getesteten Malware

Für medizinische Zentren wie das USZ ist Malware eine ständige Herausforderung. Schütt erklärt: „Palo Alto Networks war besonders effektiv bei der Erkennung von Malware – die meiner Meinung nach die grösste Bedrohung darstellt. In keinem anderen getesteten Produkt war der verhaltensbasierte Ansatz so gut umgesetzt wie in diesem. Und wir haben gesehen, dass er sich im praktischen Einsatz bewährt, vor allem seit dem Upgrade auf Cortex XDR."

Extrem geringer Ressourcenverbrauch plus einfache Skalierung

Cortex XDR bietet unvergleichlichen Schutz, mit minimalem Ressourcenaufwand. Dies ist in virtuellen Clientumgebungen entscheidend, um für maximale Sicherheit zu sorgen, ohne die Produktivität zu beeinträchtigen.

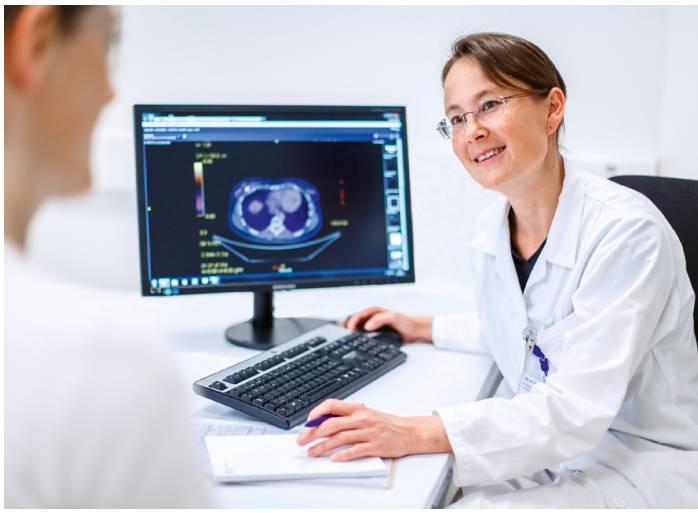
„Aber das Wichtigste für uns ist, dass Cortex XDR uns sehr effektiv vor Bedrohungen schützt", betont Schütt. Als das USZ Team erkannte, dass Cortex XDR schnell erweitert werden musste, um zusätzliche 2.500 Clients zu schützen, war dies mit der Cloud-Lösung glücklicherweise fast mühelos möglich. „Auch diese Clients sind jetzt bestmöglich vor Angriffen geschützt", ist er sich sicher.

Cortex XDR hat die Malwareabwehr des USZ deutlich verbessert und bietet:

- Höhere Effektivität mit 100% blockierter Malware im Test
- Geringere Ressourcennutzung auf virtuellen Desktops
- Vereinfachten Endpunktschutz mit einfacher Verwaltung von überall aus

Cloudbasierter Schutz kann von überall aus verwaltet werden

Schütt und die meisten Verwaltungsmitarbeiter des Krankenhauses verbrachten einen Grossteil des Jahres 2020 im Homeoffice. „Dass wir Cortex XDR als Cloud-Lösung und im Security-as-a-Service-Modell einsetzen, hat sich als grosser Vorteil erwiesen."



Quelle: Universitätsspital Zürich

Einzigartige Integration für das SOC von morgen

Das USZ baut derzeit ein Security Operations Center (SOC) auf. „Eine Kombination der SIEM Lösung mit Cortex XDR und der Cortex XSOAR-Plattform wird uns eine umfassende Lösung für die Sicherheitsorchestrierung, -automatisierung und -reaktion bieten", so Schütt.

Verbesserte Malwareerkennung minimiert Ausfallzeiten

Seit der Bereitstellung von Traps und später Cortex XDR profitiert das USZ von einer deutlich verbesserten Malware-Erkennung. Die Mitarbeiter sind jetzt unabhängig von ihrem Arbeitsort besser geschützt, sodass sie sich auf die kritische medizinische Versorgung und die Betreuung ihrer Patienten konzentrieren können.

Weitere Informationen finden Sie unter paloaltonetworks.de/cortex/cortex-xdr.

Omicron Seit 1995

Omicron AG
Industriestrasse 50b
Postfach
8304 Wallisellen

Telefon +41 44 839 11 11
E-Mail mail@omicron.ch
Web www.omicron.ch

paloalto NETWORKS

Oval Tower, De Entrée 99–197
1101 HE Amsterdam
Niederlande

+31 20 888 1883

www.paloaltonetworks.de