

Anwenderbericht ZAE Bayern

Endpoint Security

”

Das Produkt Endpoint Detection Response (powered by enSilo) aus der Matrix42 Security Suite hat am besten abgeschnitten, da es in allen Aspekten unserer Tests durchweg gute Ergebnisse gezeigt hat.

Christian Hilgers, IT-Gruppenleiter, ZAE Bayern

Kurzüberblick ZAE Bayern

Das ZAE Bayern ist ein außeruniversitäres Forschungsinstitut für angewandte Energieforschung mit ca. 240 Mitarbeitern, das vom Bayerischen Staatsministerium für Wirtschaft, Energie und Technologie institutionell gefördert wird. In seinen zentralen Kompetenzbereichen Erneuerbare Energien, Energiespeicherung und Energieeffizienz verbindet das ZAE Bayern in einem interdisziplinären Forschungsansatz Materialforschung, Komponentenentwicklung und Systemoptimierung. Die Forscher am ZAE Bayern arbeiten unter anderem an thermischen und elektrochemischen Energiespeichern, energieeffizienten Prozessen, energieoptimierten Gebäuden, Photovoltaik, Nanomaterialien, Smart Grids und sektorenübergreifenden Energiesystemen (Strom und Wärme/Kälte).

Mit seinen drei Hauptstandorten in Erlangen, Garching bei München und Würzburg sowie zwei Außenstellen in Hof und Nürnberg ist das ZAE Bayern landesweit präsent und bietet seinen Kunden komplette Innovationspakete im Bereich effiziente und nachhaltige Energiesysteme. Weitere Informationen finden Sie unter www.zae-bayern.de.

Die Herausforderung

Im Jahr 2017 hat das IT-Team des ZAE Bayern entschieden, dass es an der Zeit war, das vorhandene System zum Schutz seiner PCs und Laptops vor den immer häufigeren und ausgefeilteren Cyber-Angriffen zu modernisieren. Das Institut benötigte eine Lösung, die mehr als 300 Geräte vor einer großen Bandbreite an Malware und Ransomware schützen konnte. Die Lösung musste außerdem schnell und einfach in Betrieb zu nehmen sein und einen sehr guten, zentralen Überblick über den Gerätestatus in Echtzeit ermöglichen. Als Non-Profit-Organisation mit einem kleinen IT-Team musste die Lösung für das ZAE Bayern außerdem einfach zu nutzen und zu verwalten sein. Auf einem TAP.DE-Event in München erfuhr das ZAE-Team vom Matrix42 Portfolio und den Möglichkeiten, die es bietet. Aufgrund der vertrauensvollen Beziehung zwischen dem ZAE und TAP.DE wurde entschieden, Matrix42 Endpoint Detection Response (powered by enSilo) in die laufende Auswertung einzubeziehen. Zusammen mit Matrix42 hat TAP.DE Solutions die gesamte Auswertungsphase begleitet.

Lösung

Nachdem acht Lösungen detaillierten Tests unterzogen wurden, wurde Matrix42 EDR wegen seiner allgemeinen guten Performance ausgewählt. Die gute Erreichbarkeit des Vorverkaufsteams und der leitenden Angestellten sowie das Hinzufügen attraktiver neuer Features während des Auswahlprozesses waren ebenfalls Schlüsselfaktoren.

Die EDRSoftware wurde Mitte 2018 schnell und einfach auf allen Geräten des ZAE Bayern installiert. Auch auf den zwanzig Servern des Instituts wird sie bis Ende des Jahres laufen.

Mehr zum **Anwenderbericht** unter:
www.matrix42.com/de/hvc-overview





Unternehmen ZAE Bayern

Eine moderne Endpoint Security Solution, die den elaborierten IT-Sicherheitsbedrohungen des 21. Jahrhunderts gewachsen ist.

Als eine Non-Profit-Organisation hat das ZAE Bayern mehr Gründe als die meisten anderen Organisationen, bei jeder Investition auf maximale Kosteneffizienz zu achten, auch bei der IT. Gleichzeitig erfordert die Aufgabe, die Industrie mit Innovationen zu versorgen, dass auch das ZAE Bayern selbst modernste Technik einsetzt. Daher beschlossen die IT-Führungskräfte des Forschungsinstituts Anfang 2017, eine moderne, gewerbliche Lösung zu finden, nachdem viele Jahre lang signaturbasierte Antiviren-Software genutzt worden war. Christian Hilgers, IT-Gruppenleiter beim ZAE Bayern, erklärt: „Wir haben festgestellt, dass die potenziellen Bedrohungen für unsere ca. 300 PCs und Laptops mit Windows 7 und Windows 10 zahlreicher und ausgefeilter geworden sind. Wir haben ebenfalls ermittelt, dass die Lösung, die wir genutzt haben, um diese Endpoints vor Viren und Malware zu schützen, der heutigen Situation nicht gerecht wird. Zum Beispiel bot sie keinen Schutz vor Exploits, und wir hatten keinen detaillierten Einblick in das, was auf unseren Endgeräten geschah.“

Auswahlkriterien festlegen

Zum Auswahlprozess der neuen Lösung sagt Hilgers: „Im Sommer 2017 haben wir angefangen, ernsthaft darüber nachzudenken, und daraufhin mit den tatsächlichen Tests im Oktober/November begonnen. Zuerst haben wir uns 14 unterschiedliche Produkte angesehen und dann acht davon in die engere Auswahl genommen.“ Die Schlüssel-Auswahlkriterien, auf die sich Hilgers und seine Kollegen konzentrierten, waren:

- **Umfangreicher Schutz:** Abdecken einer großen Bandbreite an Bedrohungen, darunter auch Ransomware
- **Eine hohe Erkennungsrate:** Die Fähigkeit der Software, Malware zu erkennen
- **Die Ermittlung von Exploits:** Die Fähigkeit, das Eindringen von Bedrohungen zu erkennen, wurde hauptsächlich mit dem Metasploit Framework für Penetrationstests geprüft
- **Schnelle Bereitstellung:** Die Lösung konnte auf allen Geräten mit nur einem Installationsagenten bereitgestellt werden
- **Einfache Nutzung:** Vor allem in der mobilen Umgebung sollte es selbstverständlich sein, dass Nutzer auch sicher sind, ohne sich in einen VPN-Tunnel einzuloggen
- **Einfache Verwaltung:** Da eine kleine Organisation wie das ZAE Bayern nicht die Ressourcen für eine große Verwaltung hat
- **Hohe Transparenz:** Die Möglichkeit, zu sehen, was an bestimmten Endpoints geschieht und sofort reagieren zu können
- **Ereignisgraphen:** Zur bildlichen Darstellung, was blockiert wurde und warum
- **Hohe Verfügbarkeit:** Die Lösung sollte auch funktionieren, wenn die Cloud aus irgendeinem Grund nicht verfügbar ist

Matrix42 EDR überzeugt

Am Ende des Auswahlprozesses war das Ergebnis eindeutig, wie Hilgers bestätigt: „Matrix42 EDR hat am besten abgeschnitten, da es in allen Aspekten unserer Tests durchweg gute Ergebnisse gezeigt hat.“ Dies war jedoch nicht der einzige Grund für die Entscheidung. „Wir hatten bereits lange vorher Matrix42 Enterprise Management und den Service Store im Einsatz. Daher war es auch ein wichtiger Faktor, dass enSilo einer der neuen, wichtigen Technologiepartner von Matrix42 ist. Wir waren auch von der guten Erreichbarkeit des Matrix42 Partners enSilo beeindruckt. Wir hatten persönlichen Kontakt zum CTO, was bei den anderen Anbietern, mit denen wir gesprochen haben, niemals möglich gewesen wäre, da unser Unternehmen relativ klein ist. Dies gab uns großes Vertrauen in die Beziehung und den Strategieplan. Auch wenn Matrix42 EDR ein junges Produkt ist, haben wir großes Potenzial gesehen. Dass einige Features, die wir brauchten, während des Vorverkaufsprozesses hinzugefügt wurden, hat Matrix42 EDR zu einer noch attraktiveren Lösung für uns gemacht.“

Reibungsloser Rollout, zufriedener Kunde

Matrix42 EDR wurde im Januar 2018 auf ca. 50 Geräten installiert, um festzustellen, wie sie mit falsch positiven Ergebnissen umgeht. Nach hervorragender Arbeit des Vorverkaufsteams zur Klärung technischer Fragen ist das ZAE Bayern im April von einer Probelizenz zu einer gewerblichen Lizenz gewechselt. Die vollständig agentengesteuerte Installation wurde schnell fertiggestellt und wird bis Ende des Jahres 2018 um 20 Server erweitert.

„Nach drei Tagen wurden bereits rund 70 % der für die wissenschaftliche Arbeit genutzten Computer durch die neue Software geschützt. Die Installation auf Geräten, die nicht immer laufen, dauerte insgesamt ungefähr einen Monat. Generell ist der Prozess schnell und einfach vonstattengegangen, und es waren keine Neustarts der Geräte nötig, was ein wichtiger Punkt war. Ich bin sehr glücklich mit der EDR-Lösung von Matrix42 und bin bereits gespannt darauf, wie die Funktionalitäten weiterhin entwickelt werden, um uns in den nächsten Jahren noch bessere Endpoint Security zu gewährleisten“, erklärt Hilgers abschließend.

”

Wir waren auch beeindruckt von der guten Erreichbarkeit des Matrix42 Partners enSilo. Wir hatten persönlichen Kontakt zum CTO, was bei den anderen Anbietern, mit denen wir gesprochen haben, niemals möglich gewesen wäre.

Christian Hilgers, IT-Gruppenleiter,
ZAE Bayern

Standorte

Hauptsitz Deutschland

Matrix42 AG
Elbinger Straße 7
60487 Frankfurt am Main
Deutschland
Telefon: +49 69 66773-8220
Fax: +49 69 66778-8657
info@matrix42.com

Niederlassung Schweiz und Österreich

Matrix42 Helvetia AG
Grabenstrasse 32
6300 Zug
Schweiz
Telefon: +41 41 720-4220
info@matrix42.ch

Weitere Niederlassungen im Ausland

finden Sie auf unserer Website:
www.matrix42.com

Über Matrix42

Matrix42 unterstützt Organisationen dabei, die Arbeitsumgebung ihrer Mitarbeiter zu digitalisieren. Die Softwarelösungen für Unified Endpoint Management, Software Asset- und Service Management sowie Endpoint Security verwalten Geräte, Anwendungen, Prozesse und Services einfach, sicher und richtlinienkonform.

Die Matrix42 AG hat ihren Hauptsitz in Frankfurt am Main, Deutschland, und vertreibt und implementiert Softwarelösungen weltweit mit lokalen und globalen Partnern.

Unser Partner TAP.DE



Die TAP.DE Unternehmensgruppe betreut mittelständische Unternehmen, Konzerne und öffentliche Einrichtungen bei der Entwicklung und Optimierung von Business Prozessen sowie dem nachhaltigen Betrieb von IT Arbeitsumgebungen. Die Spezialisten von TAP.DE entwickeln strategische Konzepte für die Bereiche Workplace Automatisierung, Endpoint Security, IT Service Management und Compliance. Praxistauglichkeit, Quickwins sowie die Verbesserung interner Abläufe und Services stehen stets im Vordergrund stehen.