FALLSTUDIE – FORTIS BY SENTINEL

MAGNET IGNITE™

Fortis beschleunigt die Endpunkt-Durchsuchung um 70 % und leitet damit den Weg zu einer schnelleren Wiederherstellung ein

> Mit IGNITE führen wir sehr schnell eine erste Triage mit der Durchsuchung von Endpunkten durch. Verglichen mit traditioneller Forensik mit skriptgesteuerten Tools sparen wir 70 % Zeit bei der Datenerfassung und der ersten Durchsuchung von Endpunkten.
>
> **— Ted Joffs, National Incident Response Manager, Fortis by Sentinel**

Die Herausforderung

Langsame und komplizierte Tools

Als National Incident Response Manager bei Fortis by Sentinel muss Ted Joffs oft Menschen helfen, die ihren schlimmsten Arbeitstag erleben. Von Ransomware oder sonstigen Malware-Angriffen betroffene Unternehmen sind verletzlich und verzweifelt. Sie benötigen schnelle Hilfe.

Fortis kümmert sich mit einem Team von Spezialisten um die Bekämpfung der Sicherheitsverletzung. Da eine gründliche Analyse jedes potenziell betroffenen Endpunkts viel Zeit und Geld erfordert, muss der Forensik-Anbieter die Bedrohung zunächst eingrenzen. In der Vergangenheit wurden skriptbasierte Tools zur Datenerfassung für die erste Überprüfung verwendet. Diese Produkte erwiesen sich jedoch als mangelhaft.

„Skriptbasierte Datenerfassungstools sind in der Regel langsam und kompliziert“, bemerkt Joffs. „Sie benötigen oft die richtigen Tools als Basis, je nach Art der Plattform.“

Fortis suchte nach einem schnelleren, zuverlässigen Tool zum Durchsuchen von Endpunkten und zur Minimierung der Gesamtzahl von Endpunkten, die eine gründliche Untersuchung erfordern.

FORTIS by Sentinel
Advancing Your Protection

Fortis by Sentinel bietet umfassenden Schutz und Wiederherstellung, der Risiken reduziert und Schwachstellen eliminiert

ZENTRALE

- Downers Grove, IL

GRÖSSE

- Über 450 Fachkräfte

EXPERTISE

- Penetrationstests
- Vorfallsreaktion
- Einschätzung von Sicherheit und Gefährdung

ERGEBNISSE

- Eliminiert die Kosten und den Aufwand für überflüssige tiefgreifende forensische Untersuchungen
- Trägt dazu bei, dass die Umgebung des Kunden in der Hälfte der Zeit im Vergleich zu Wettbewerbern wiederhergestellt wird
- Fördert die Entwicklung langfristiger Beziehungen

Wie Magnet IGNITE hilft

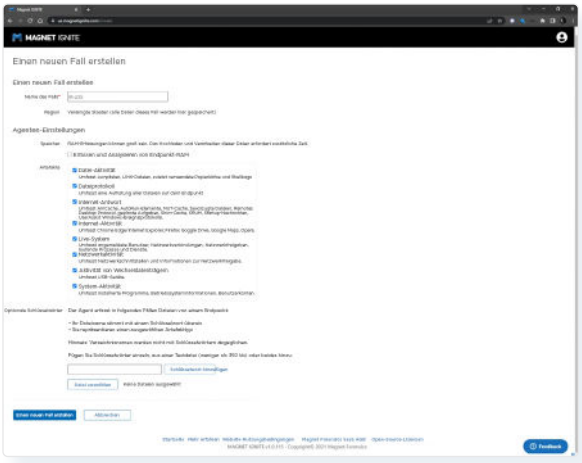
Beschleunigte Reaktion

Fortis, die Magnet AXIOM Cyber bereits ausgiebig für Untersuchungen einsetzten, vertrauen auf Magnet Forensics' Liebe zum Detail und kontinuierlichen Innovationen. Auf Empfehlung eines Teammitglieds, das das Triage-Tool bei seiner früheren Arbeit verwendet hatte, setzte das Unternehmen Magnet IGNITE schon früh ein.

„Unsere Teams für digitale Forensik- und Vorfallsreaktion verwenden IGNITE, um schnelle Ergebnisse zu erhalten, ... die eine umfangreiche forensische Untersuchung überflüssig machen", sagt Joffs.

Da IGNITE laut Joffs „weiß, wo man suchen muss", dient es als Startschuss für die Reaktion und Wiederherstellung, sodass die Kunden im Vergleich zu einigen Wettbewerbern nur die Hälfte der Zeit für die Wiederherstellung benötigen.

„Jedes Mal, wenn man den forensischen Prozess beschleunigen kann, hat man definitiv einen Vorteil", sagt er. „IGNITE liefert diesen Vorteil."



Schnelle Zielerfassung

In den Händen von Fortis-Spezialisten sorgt IGNITE dafür, dass Fachkräfte Zeit und Energie schnell und präzise einsetzen können.

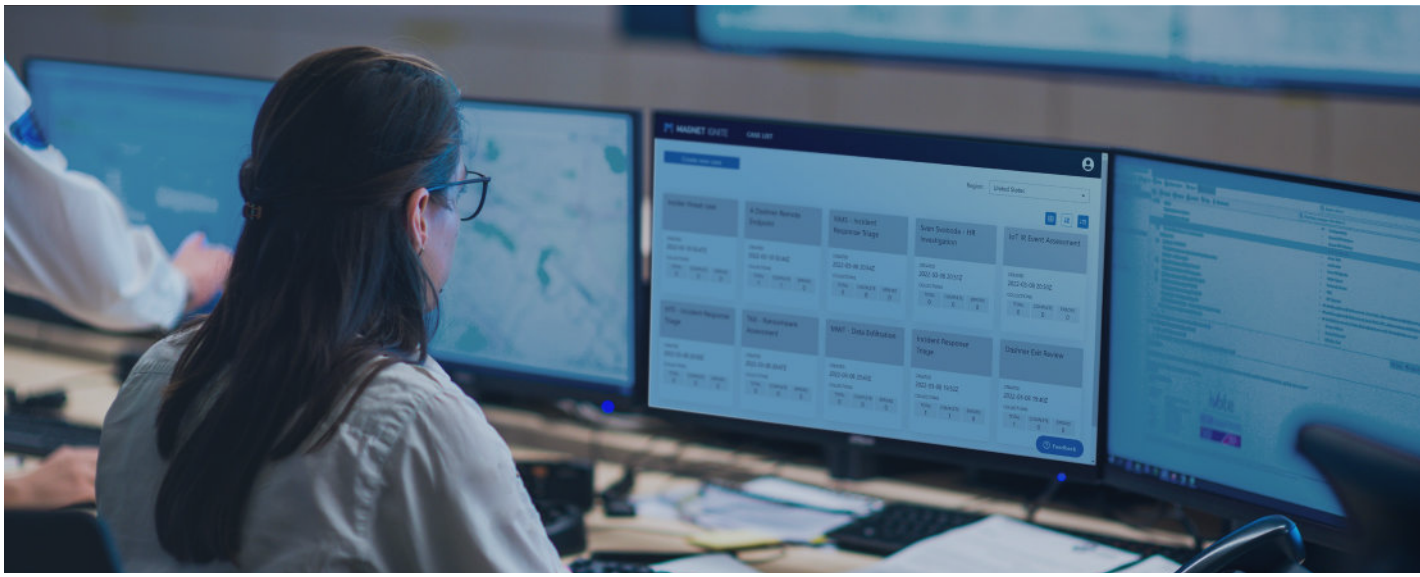
„Mit IGNITE führen wir sehr schnell eine erste Triage mit der Durchsuchung von Endpunkten durch", erklärt Joffs. „Verglichen mit traditioneller Forensik mit skriptbasierten Tools sparen wir 70 % Zeit bei der Datenerfassung und der ersten Durchsuchung von Endpunkten."

Bei Fortis-Untersuchungen im Zusammenhang mit Ransomware-Aktivitäten identifiziert IGNITE Indikatoren für eine Kompromittierung und die Aktivitäten von Bedrohungsakteuren schneller als frühere Methoden, sodass die Analysten zielgerichtet vorgehen können.

> Wenn wir Daten von 100 Systemen wiederherstellen und IGNITE schnell feststellt, dass nur zwei davon eine vollständige forensische Analyse benötigen, können wir etliche Stunden Reaktionszeit sparen", sagt Joffs.

Fortis und seine Kunden sparen auch die damit verbundenen Kosten für forensische Tiefenanalyse von nicht betroffenen Systemen. Kompromittierte Endpunkte können mit AXIOM Cyber einfach für eine Untersuchung exportiert werden.

„Für viele Leute sind Vorfallsreaktion und digitale Forensik zwei getrennte Dinge", sagt Joffs. „Wenn jedoch die Endpunktsuche mit einer einzigen Kontrollinstanz einhergeht, kann man schnell alle kompromittierten Objekte identifizieren und so Umfang der Wiederherstellung und des Wiederaufbaus eingrenzen."



Cloudbasierte Triage

Im Vergleich zur wartungsintensiven skriptbasierten Datenerfassung ist IGNITE sofort einsatzbereit und ermöglicht eine schnelle Ferntriage von Endpunkten. Anstelle von Methoden, die ein manuelles FTP und eine Überprüfung erfordern, ermöglicht IGNITE den Analysten eine sofortige Überprüfung der Ergebnisse. Fortis-Experten investieren ihre Zeit in die Gewinnung von Erkenntnissen, nicht in die Konfiguration von Tools.

Darüber hinaus können Analysten und Kunden eine cloudbasierte Triage direkt am jeweiligen Standort durchführen. Die meisten Fortis-Kunden sind zwar US-amerikanische Unternehmen, aber große Organisationen haben oft mehrere regionale und globale Niederlassungen und ein Großteil der Mitarbeiter arbeitet dezentral. Das Gleiche gilt für das DFIR-Team von Fortis, das die Kunden bei der Reaktion und Wiederherstellung begleitet und sich gleichzeitig mit standort- und branchenspezifischen Vorschriften und Berichten auseinandersetzt.

„Alle arbeiten jetzt dezentral", sagt Joffs. „Die Möglichkeit, dezentral und gemeinschaftlich zu arbeiten, ist wichtig."

Eine cloudbasierte Verarbeitung unterstützt auch die Skalierbarkeit. Es spielt keine Rolle, ob es sich um ein hohes oder niedriges Volumen handelt, alle Kundenbedürfnisse werden erfüllt, so Joffs:

„IGNITE lässt sich gut skalieren, weil es mit der Cloud kommuniziert und über eine gute Infrastruktur für eine schnelle Datenerfassung verfügt."

Fallerstellung und Konformität

Durch Effizienz gewinnt Fortis das Vertrauen von Kunden, Rechtsteams und Versicherungsanbietern. Die Analysten verlassen sich darauf, dass IGNITE nur die gefährdeten Objekte erfasst und leiten die Ergebnisse dann an AXIOM Cyber weiter, um die für den Aufbau eines Falls wichtigen Untersuchungen durchzuführen. „Jedes Mal, wenn es zu einem Vorfall kommt, möchten die Rechtsabteilungen die Daten so schnell wie möglich haben," erklärt Joffs.

> Die Schnelligkeit der Erfassung und Lieferung der Ergebnisse an eine Rechtsabteilung ist ein wesentlicher Wettbewerbsvorteil."

Die Berichterstattung von IGNITE und AXIOM wird laufend an die immer weiter wachsenden Anforderungen angepasst. Das ermöglicht den Analysten von Fortis die Einhaltung gesetzlicher Vorschriften und die Ursachenermittlung eines Vorfalls. „Die Lösungen von Magnet geben uns die Möglichkeit, vollständige Zeitachsen zu erstellen", bemerkt Joffs. „Es ist wirklich wichtig, dass wir diese Daten erfassen und dann in leicht lesbaren Formaten anzeigen können."

Auswirkungen

Ausfallsicherheit für Kunden

Mit der Ferntriage von IGNITE und der Analyse von AXIOM stellt Fortis sicher, dass sich Unternehmen wieder auf ihre Kernaufgaben konzentrieren können. Dabei spielt es keine Rolle, ob das Gesundheitsversorgung, Investitionsschutz oder sonstige wichtige Dienstleistungen betrifft.

Unternehmenswachstum

Neben der Befriedigung, Kunden bei der Fortsetzung des Geschäftsbetriebs helfen zu können, pflegen Joffs und sein Team Verbindungen, die das Wachstum von Fortis fördern. Tatsächlich dienen Transaktionsfälle, die fast ein Drittel der gesamten Kundenarbeit ausmachen, oft als erste Kontakte, die zu dauerhaften Partnerschaften führen.

> “Wenn man eine Umgebung wiederhergestellt hat, weiß man, dass man einem Kunden durch den schwersten Tag seiner beruflichen Laufbahn geholfen haben", schließt Joffs. „Das schafft Vertrauen und führt zu langfristigen Beziehungen.“

Magnet IGNITE selbst in Aktion sehen

Erfahren Sie mehr über Magnet IGNITE und fordern Sie eine kostenlose Testversion an unter **magnetforensics.com/magnet-ignite**.

MAGNET FORENSICS®