ÉTUDE DE CAS – FORTIS BY SENTINEL

MAGNET IGNITE™

Fortis accélère de 70 % le balayage des terminaux et permet une récupération plus rapide.

> Avec IGNITE, nous effectuons très vite un triage initial avec balayage des terminaux. Par rapport à la criminalistique classique qui utilise des outils de script, nous constatons un gain de temps de 70 % sur la collecte des données et le balayage initial des terminaux.
>
> — **Ted Joffs, responsable national des interventions en cas d'incidents, Fortis by Sentinel**

Le défi

Des outils « lents et difficiles à utiliser »

En tant que responsable national des interventions en cas d'incidents pour Fortis by Sentinel, Ted Joffs est souvent appelé à intervenir auprès de personnes qui vivent leur pire journée de travail. Frappées par des ransomwares ou d'autres attaques de logiciels malveillants, de nombreuses entreprises victimes sont vulnérables et affolées. Elles ont besoin d'aide, rapidement.

Fortis intervient en envoyant une équipe de spécialistes pour contrer l'attaque. Étant donné que l'analyse approfondie de chaque terminal potentiellement touché nécessite énormément de temps et d'argent, le fournisseur de services de criminalistique doit d'abord évaluer la menace. Auparavant, il utilisait des outils de collecte de données scénarisés pour l'examen initial. Toutefois, ces outils se sont révélés insuffisants.

« Les outils de collecte de données scriptés sont généralement lents et difficiles à utiliser », note Joffs. « Ils dépendent souvent de la présence des bons outils en dessous, en fonction du type de plateforme. »

Fortis avait besoin d'un outil plus rapide et plus fiable pour balayer les terminaux et réduire le nombre total de terminaux nécessitant une analyse approfondie.

FORTIS by Sentinel
Advancing Your Protection

Fortis by Sentinel offre une protection et une récupération de bout en bout qui réduisent les risques et éliminent les vulnérabilités.

SIÈGE SOCIAL

- Downers Grove, IL

TAILLE

- Plus de 450 professionnels

SPÉCIALITÉS

- Tests de pénétration
- Intervention en cas d'incident
- Évaluations de la sécurité et de la compromission

RÉSULTATS

- Élimine les coûts et les efforts liés à des recherches approfondies superflues.
- Contribue à la reprise d'activités des clients en deux fois moins de temps que les concurrents
- Favorise le développement de relations à long terme

Utilité de Magnet IGNITE

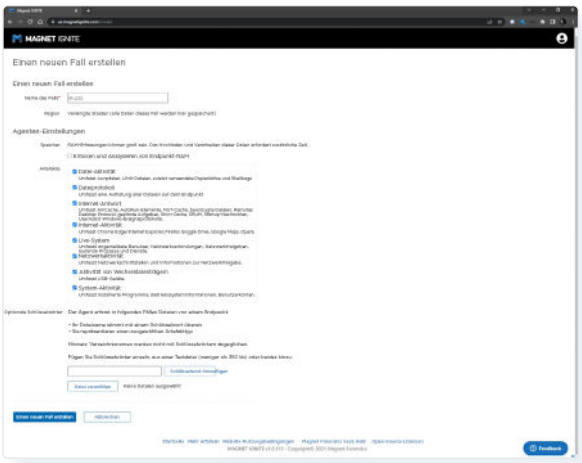
Accélérer l'intervention

En tant que grand utilisateur de Magnet AXIOM Cyber pour ses enquêtes, Fortis fait confiance à l'attention portée aux détails et à l'innovation continue de Magnet Forensics. L'entreprise a ensuite adopté rapidement Magnet IGNITE sur la recommandation d'un membre de l'équipe qui avait utilisé l'outil de triage dans son travail précédent.

« Nos équipes de criminalistique numérique et d'intervention en cas d'incidents utilisent IGNITE pour obtenir des résultats rapides... qui éliminent le besoin de criminalistique approfondie inutile », déclare Joffs.

En fait, en « sachant ce qu'il faut faire », selon Joffs, IGNITE sert de coup d'envoi à l'intervention et à la récupération qui aide les clients à reprendre leurs activités en deux fois moins de temps que certains concurrents.

« Chaque fois que l'on peut accélérer le processus de criminalistique, on a un avantage certain », explique-t-il. « IGNITE offre cet avantage. »



Ciblage rapide

Entre les mains des spécialistes de Fortis, IGNITE garantit que le temps et l'énergie des personnes qualifiées sont alloués avec rapidité et précision.

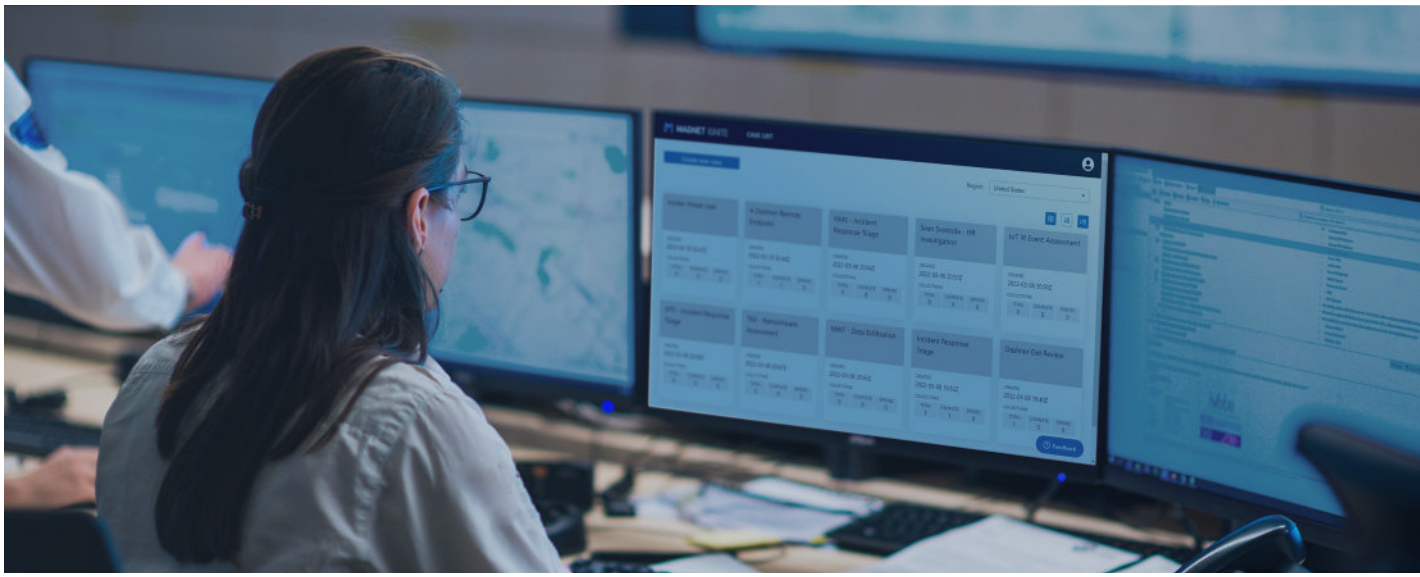
« Grâce à IGNITE, nous procédons à un triage initial très rapide en balayant les terminaux », explique Joffs. « Contrairement à la criminalistique traditionnelle avec des outils scriptés, nous réalisons un gain de temps de 70 % sur la collecte des données et le balayage initial des terminaux. »

Dans les investigations de Fortis liées à l'activité des ransomwares, IGNITE identifie les indicateurs de compromission et l'activité des acteurs de la menace plus rapidement que les méthodes précédentes, ce qui permet aux analystes de progresser avec une confiance ciblée.

> Si nous récupérons les données de 100 systèmes et qu'IGNITE identifie rapidement que seuls deux d'entre eux nécessitent une analyse judiciaire complète, nous pouvons gagner des heures de temps de réponse », explique Joffs.

Fortis et ses clients réduisent également les coûts liés à la criminalistique approfondie des systèmes non affectés, les terminaux compromis pouvant être facilement exportés pour investigation avec AXIOM Cyber.

« De nombreuses personnes considèrent que l'intervention en cas d'incident et la criminalistique numérique sont deux choses distinctes », déclare Joffs. « Mais lorsque le balayage des terminaux est lié à un contrôle unique, vous pouvez rapidement identifier tous les actifs qui ont été touchés afin de limiter l'étendue de la récupération et de la reconstruction. »



Triage basé sur le cloud

Contrairement à la collecte de données par script, qui nécessite beaucoup de maintenance, IGNITE est prêt à l'emploi et permet d'effectuer un triage rapide et à distance des terminaux. En outre, au lieu d'utiliser des méthodes qui nécessitent un FTP et un examen manuels, IGNITE permet aux analystes d'examiner les résultats immédiatement. Les experts de Fortis passent leur temps à recueillir des informations, et non à configurer des outils.

En outre, le triage basé sur le cloud sert les analystes et les clients là où ils se trouvent. Bien que la majorité des clients de Fortis soient des entreprises américaines, les grandes organisations disposent souvent de plusieurs bureaux régionaux et mondiaux, la majorité des employés travaillant à distance. Il en va de même pour l'équipe DFIR de Fortis, qui guide les clients dans leur intervention et leur reprise d'activités, tout en gérant les réglementations et les rapports spécifiques au lieu et au secteur d'activité.

« Aujourd'hui, tout le monde travaille à distance », explique Joffs. « Il est essentiel de pouvoir travailler à distance et en collaboration. »

Le traitement basé sur le cloud favorise également l'évolutivité : qu'il s'agisse d'un volume élevé ou faible, tous les besoins des clients sont satisfaits, selon Joffs :

« IGNITE s'adapte bien parce qu'il communique avec le cloud et qu'il dispose d'une bonne infrastructure pour ingérer rapidement les données ».

Constitution de dossiers et respect des règles

Grâce à son efficacité, Fortis gagne la confiance des clients, des équipes juridiques et des assureurs. Les analystes s'appuient sur IGNITE pour cibler uniquement les actifs exposés, puis ils transmettent les résultats à AXIOM Cyber pour des investigations essentielles à la constitution d'un dossier. « Chaque fois qu'un incident survient, les équipes juridiques veulent obtenir les données le plus rapidement possible », explique Joffs.

> « La rapidité de la collecte et de la transmission des résultats à l'équipe juridique constitue un avantage concurrentiel majeur ».

Les capacités en matière de rapports d'IGNITE et d'AXIOM permettent aux analystes de Fortis de démontrer leur conformité aux réglementations et leur compréhension de la cause première d'un incident. « Les solutions magnétiques nous permettent d'établir des calendriers complets », note Joffs. « Il est très important de pouvoir collecter ces données et de les présenter dans des formats facilement lisibles. »

L'impact

La résilience des clients

Grâce au triage à distance IGNITE et à la cyberanalyse AXIOM, Fortis permet aux organisations de reprendre leurs missions principales, qu'il s'agisse de fournir des soins de santé, de protéger des investissements ou d'autres services vitaux.

Croissance de l'entreprise

Outre la satisfaction d'aider les clients à reprendre leurs activités, Joffs et son équipe entretiennent des relations qui contribuent à la croissance de Fortis. En fait, les affaires transactionnelles, qui représentent près d'un tiers de l'ensemble du travail des clients, constituent souvent les premières interactions qui débouchent sur des partenariats durables.

> « Une fois que vous avez récupéré un environnement, vous savez que vous avez aidé un client à surmonter la journée la plus difficile de sa carrière », conclut Joffs. « Ensuite, la confiance s'installe et permet de construire une relation à long terme. »

Voir Magnet IGNITE en action par vous-même

Pour en savoir plus sur Magnet IGNITE et bénéficier d'un essai gratuit, veuillez consulter le site Web **magnetforensics.com/magnet-ignite**.

MAGNET FORENSICS®