LÖSUNGSÜBERSICHT

InfiniSafe® Cyber Detection

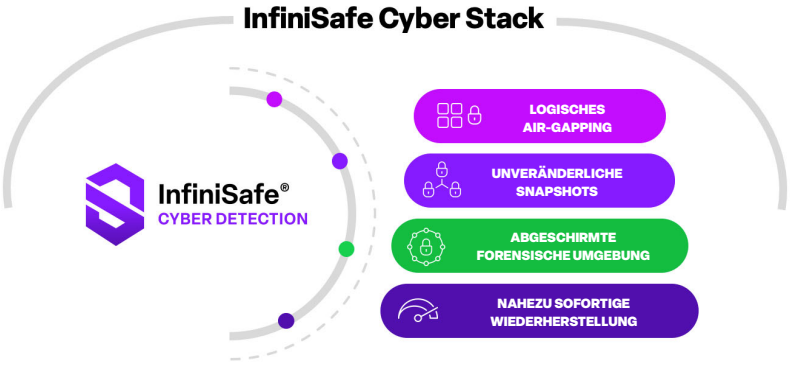
Es wird erwartet, dass die Auswirkungen der Cyberkriminalität die Unternehmen jährlich 8 Billionen USD kosten.[1] Alle 39 Sekunden gibt es irgendwo im Internet einen neuen Angriff.[2] Die Kosten für ein Unternehmen umfassen die Beschädigung und Zerstörung von Daten, Produktivitätsverlust, Diebstahl von geistigem Eigentum, Diebstahl von persönlichen und finanziellen Daten, Veruntreuung usw. Neben der Unterbrechung des Geschäftsbetriebs nach einem Angriff kommen forensische Untersuchungen, das Auffinden und Wiederherstellen gehackter Daten und Systeme sowie der Verlust von Vertrauen und gutem Ruf hinzu. Die meisten Sicherheits- und IT-Teams haben das Gefühl, dass es nur eine Frage der Zeit ist, bis es zu einem Cyberangriff kommt. Sind Sie vorbereitet?

Die InfiniSafe-Technologie bietet einen mehrschichtigen Cyber-Stack zur Erstellung von Cyber-Storage-resilienten Umgebungen mit den Plattformen InfiniBox® und InfiniBox™ SSA.

Die Einführung von InfiniSafe Cyber Detection verbessert die Cyber-Storage-Resilienz und die Reaktionsfähigkeit von Infinidat, weil Sicherheits- und IT-Teams damit Ransomware- und Malware-Angriffe mit einer Genauigkeit von bis zu 99,5 % erkennen und eine nahezu sofortige Wiederherstellung von Daten aus sauberen, nachweislich vertrauenswürdigen Kopien auf der InfiniBox- und der InfiniBox SSA-Plattform ermöglichen.

InfiniSafe Cyber Detection fügt dem InfiniSafe Cyber-Stack eine Datenerkennungsebene um die vier Hauptschichten des Stacks hinzu und vertieft die Fähigkeit von InfiniSafe, Cyber-Vorfälle zu erkennen. InfiniSafe Cyber Detection scannt Block-, Datei- und Datenbankspeicher, indem leistungsstarke KI-basierte Scan-Engines von InfiniBox und InfiniBox SSA unveränderliche Snapshots erhalten, um deren Integrität zu validieren und durch maschinelles Lernen alle bösartigen Änderungen zu identifizieren, die auf einen Cyberangriff hindeuten könnten.

Bei Erkennung eines Angriffs liefert InfiniSafe Cyber Detection forensische Berichte, um zu diagnostizieren, welche Daten wie kompromittiert wurden und liefert wichtige Erkenntnisse über die Herkunft der kompromittierten Daten. Mit der InfiniSafe-Technologie kann dann zügig der normale Geschäftsbetrieb wiederhergestellt werden, sobald eine nachweislich vertrauenswürdige Kopie der Daten identifiziert wurde.



InfiniSafe Cyber Detection verwendet eine Kombination aus über 200 vollständig inhaltsbasierten Analysen, die den Inhalt von Dateien und Daten, und nicht nur Metadaten, untersuchen. Leistungsstarke Algorithmen für maschinelles Lernen ermitteln mit einer Genauigkeit von 99,5 % die Art der Variante, mit der die Daten beschädigt wurden, damit geschäftskritische Infrastruktur und Inhalte geschützt werden, ohne dass es zu einer Flut von Fehlalarmen kommt. So können Sie sich auf die wirklichen Problembereiche konzentrieren und Probleme schnell beheben.

Wird eine Datenbeschädigung festgestellt, bietet InfiniSafe Cyber Detection die erforderlichen forensischen Tools zur Diagnose, Identifizierung und Wiederherstellung der betroffenen Ressourcen. InfiniSafe Cyber Detection erstellt Berichte über die betroffenen Dateien, und die forensischen Ergebnisse können von Ihren Sicherheits- und Softwareteams untersucht werden, sodass alle Probleme nach Bedarf mit den entsprechenden Tools behoben werden können. Dann können alle kompromittierten Daten einfach durch die letzte nachweislich vertrauenswürdige Version ersetzt werden, um den Geschäftsbetrieb mit minimaler Ausfallzeit wieder aufzunehmen. InfiniSafe Cyber Detection ist eine Zusatzoption zu unserer InfiniSafe-Kerntechnologie und als Lizenz auf Abonnementbasis erhältlich.

> „**79 %** der Unternehmen geben an, dass **Ransomware-Bereitschaft** in den Augen ihres Führungsteams bzw. Vorstands eine der fünf wichtigsten **Geschäftsprioritäten** ist.“
>
> Enterprise Strategy Group Research Report, The Long Road Ahead to Ransomware Preparedness, Juni 2022

Erkennung

Analytik und Erkennung durch maschinelles Lernen

Forensik

Forensische Berichte zur Diagnose und Identifizierung der Angriffsursache

Wiederherstellung

Berichte zur letzten nachweislich vertrauenswürdigen Version von Dateien, um die Wiederherstellung zu optimieren

Bei Feststellung einer Datenbeschädigung bietet InfiniSafe Cyber Detection die notwendigen forensischen Tools zur Diagnose, Identifizierung und Wiederherstellung der betroffenen Daten. InfiniSafe Cyber Detection erstellt Berichte über die betroffenen Dateien, und die forensischen Ergebnisse können von Ihren Sicherheits- und Softwareteams untersucht werden, sodass alle Probleme nach Bedarf mit den entsprechenden Tools behoben werden können. Dann können alle kompromittierten Daten einfach durch die letzte nachweislich vertrauenswürdige Version ersetzt werden, um den Geschäftsbetrieb mit minimaler Ausfallzeit wieder aufzunehmen. InfiniSafe Cyber Detection ist eine Zusatzoption zu unserer InfiniSafe-Kerntechnologie und eine Lizenz auf Abonnementbasis. InfiniSafe Cyber Detection deckt die Zeit nach einem Angriff ab und konzentriert sich auf die Datenresilienz im InfiniSafe Cyber-Stack. Es ersetzt keine bewährten Methoden für Ransomware- und Malware-Prävention oder herkömmliche Bedrohungsmanagementprodukte für den Server-, Anwendungs- und Netzwerkbereich als Teil einer Cyber-Sicherheitsstrategie.

Erkennung

InfiniSafe Cyber Detection nutzt die vollständige inhaltsbasierte Analyse aller geschützten Daten. Nur so können Sie sicher sein, dass Ihre Daten integer sind und dass Cyberkriminelle Ihre Datenanalysetools nicht umgehen, Spuren verwischen und Ihre Daten heimlich beschädigen.

Ähnlich wie unser neuronaler Cache für maschinelles Lernen ist InfiniSafe Cyber Detection mit leistungsstarkem und deterministischem maschinellem Lernen ausgestattet. Das Tool kombiniert über 200 Analysen – mehr als 20 Mal so viele wie bei Mitbewerbern – mit Datenbeobachtungen, die mit der Zeit durch mehr Beobachtungen intelligenter werden. Das maschinelle Lernen wurde an Tausenden von Ransomware-, Malware- und Trojaner-Infektionen trainiert, um ungewöhnliche Verhaltensmuster zu erkennen und Benutzeraktivitäten von Ransomware zu unterscheiden, während falsch positive und falsch negative Ergebnisse minimiert werden.

Forensik

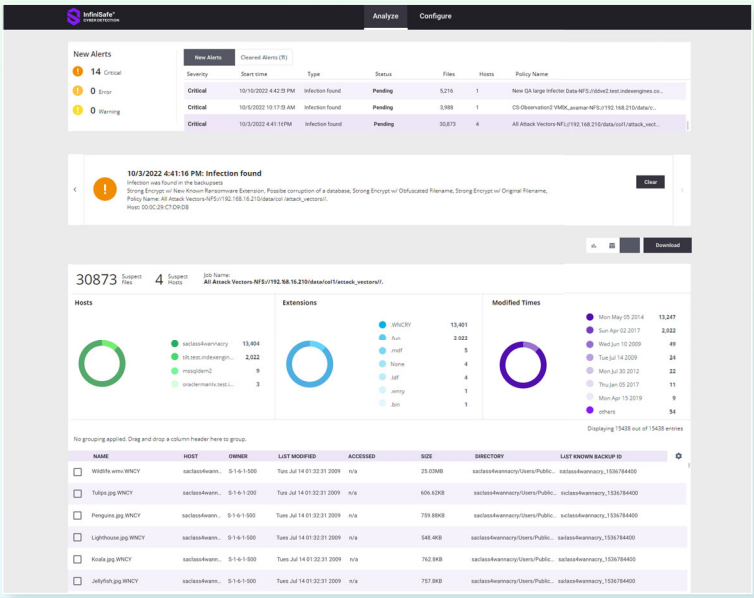
Bei Datenbeschädigung erstellt InfiniSafe Cyber Detection eine Liste der betroffenen Dateien. Beschädigte Dateien werden markiert und forensische Berichte erstellt, um die Auswirkungen des Angriffs zu diagnostizieren und zu identifizieren sowie die zur Wiederherstellung erforderlichen Informationen zu liefern.

Nach Schweregrad geordnete Warnmeldungen

Neue Einzelheiten zu verdächtigen Beschädigungen

Anpassbare, dynamische Diagramme, die Einzelheiten des Angriffs aufschlüsseln

Liste der beschädigten Dateien, die heruntergeladen werden können

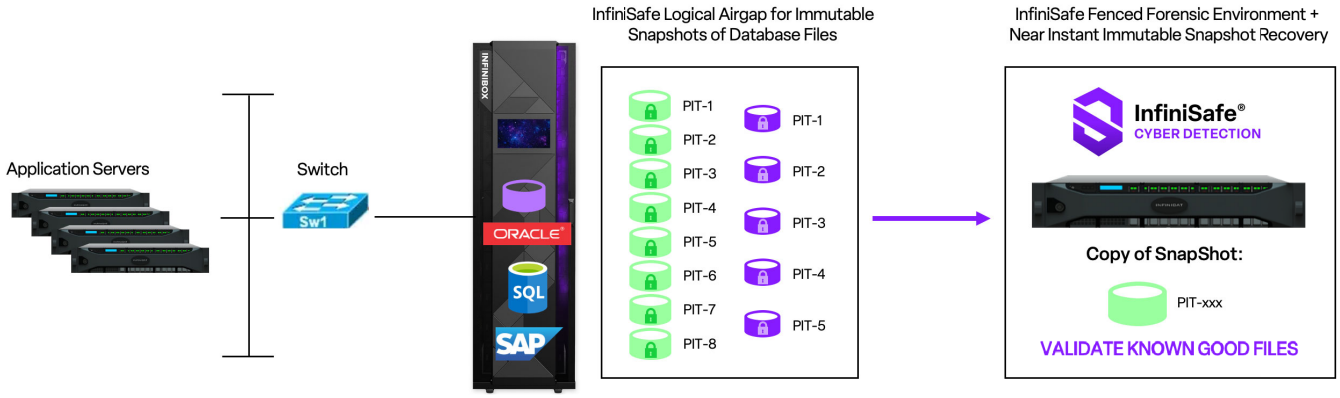


Das Post-Attack-Dashboard: verbesserte Benutzerfreundlichkeit, mehr Einblicke in die Daten, intuitiver Post-Attack-Workflow.

Wiederherstellung

Schließlich meldet InfiniSafe Cyber Detection die letzte nachweislich vertrauenswürdige Kopie einer Datei oder einer Sicherungskopie, wenn sich die Sicherungskopie auf einer InfiniBox oder InfiniBox SSA befindet. Die Plattform weiß, wo sich die beschädigten Daten und die letzte nachweislich vertrauenswürdige Version der Daten befinden sowie in welchen Snapshots oder Sicherungskopiesätzen sich die Daten befanden, um den Wiederherstellungsprozess zu optimieren.

Anwendungsfälle: Cyber-Erkennung in Blöcken, Dateien und Datenbanken



Unternehmen, die InfiniBox oder InfiniBox SSA für geschäftskritische Datenbankanwendungen einsetzen, können bei Verwendung der InfiniSafe Cyber-Stack-Technologie mit Cyber Detection sicher sein, dass sie regelmäßig unveränderliche Snapshots erstellen können, um deren Integrität zu überprüfen und durch maschinelles Lernen alle Änderungen zu erkennen, die auf einen Cyberangriff hindeuten. InfiniSafe Cyber Detection ermittelt alle Probleme und meldet nachweislich vertrauenswürdige Kopien der Daten zur nahezu sofortigen Wiederherstellung mit InfiniSafe.

Cyber Detection Array

Unternehmen, die mehrere InfiniBoxen oder InfiniBox SSAs einsetzen, können Daten mithilfe der nativen Infinidat-Replikationstools auf ein bestimmtes Cyber Detection Array in einer abgeschirmten forensischen Umgebung replizieren. Das Cyber Detection Array scannt alle Datendateien, markiert beschädigte Dateien und erstellt einen forensischen Bericht. Diese Konfiguration bietet Unternehmen die Möglichkeit, einen Cyberangriff zu erkennen.

Bösartige Ransomware- und Malware-Vorfälle stören auch weiterhin kritische Dienste und Unternehmen, von Energieversorgungsunternehmen über Schulen bis hin zu Krankenhäusern. Der wirtschaftliche Gesamtschaden durch Ransomware- und Malware-Angriffe steigt weiter an. Die Umsetzung einer wirksamen Strategie zur Aufdeckung von Cyberangriffen kann Ihr Unternehmen schützen und schnelle Wiederherstellung gewährleisten.

[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/
[2] https://techjury.net/blog/how-many-cyber-attacks-per-day/

dach@infinidat.com

INFINIDAT