INFINIDAT

SOLUTION BRIEF

Автоматизированная киберзащита InfiniSafe®: снижение угроз

Сейчас как никогда важно сократить окно угроз, чтобы избежать или попытаться предотвратить кибератаки. Ни одно решение не способно устранить все уязвимости, но наличие гибкого набора возможностей и опций защиты критически важных информационных активов компании является важным элементом сложной задачи. **Помните: вопрос не в том, нанесут ли киберзлоумышленники удар, а в том, когда это произойдет.**

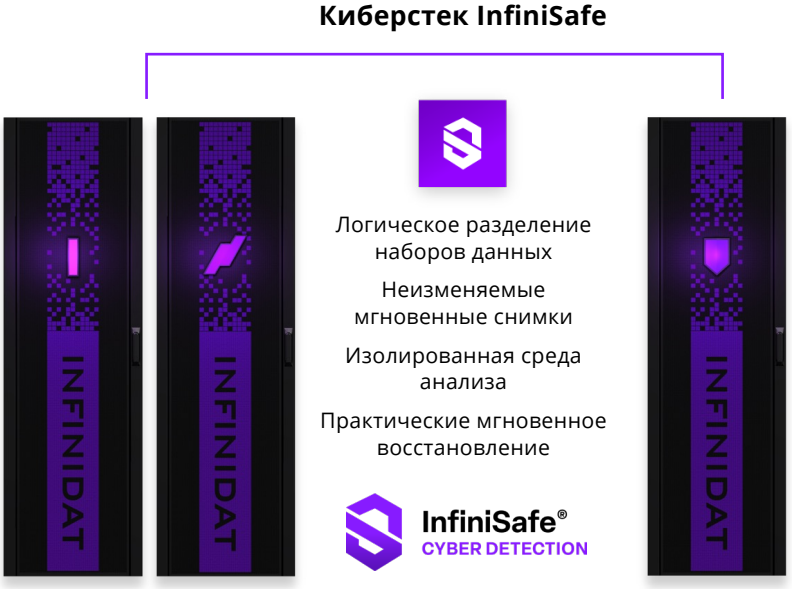
Подготовьтесь

В настоящее время большинство организаций защищают данные с помощью традиционных методов резервного копирования и восстановления, включая удаляемые моментальные снимки. Если дополнить эти методы запланированными, блокируемыми на определенный срок неизменяемыми моментальными снимками, то можно добиться постепенного прогресса в защите данных. К сожалению, запланированные события создают большие разрывы во времени, во время которых данные уязвимы. Промежуток времени между этими моментами обычно определяется целевой точкой восстановления (RPO) – мерой того, сколько данных предприятие может позволить себе потерять за определенное время. Если неизменяемые снимки выполняются четыре раза в день, это означает, что RPO составляет до 6 часов. Сегодня объем данных, который может быть скомпрометирован за это время, может погубить бизнес.

В результате для защиты данных в случае возникновения подозрений в атаке необходим более проактивный процесс. Команды мониторинга безопасности не могут реагировать достаточно быстро, чтобы защитить данные во время киберинцидентов, которые происходят со скоростью вычислений и сетей. Автоматизированная киберзащита InfiniSafe решает эту проблему. Используя мониторинг в реальном времени, существующий во многих операционных центрах безопасности компаний, команда безопасности может определить триггер для автоматического и немедленного создания неизменяемых снимков в среде хранения Infinidat, что снижает риск повреждения, удаления, шифрования данных и так далее.

Любая атака – это получение информации и рычагов влияния. Шифрование данных, повреждение резервных копий и кража информации создают рычаги влияния. Когда у злоумышленников есть рычаги влияния, они знают, что, скорее всего, смогут получить от вас деньги.

Время – это деньги, причем большие деньги, когда речь идет о киберинцидентах. Компании впадают в хаос, когда происходит киберпроисшествие такого масштаба. Чем быстрее вы сможете убедиться в том, что у вас есть данные и что они находятся в заведомо хорошем состоянии, тем быстрее вы уберете часть, а то и все рычаги влияния на вас. У нас есть все механизмы, чтобы облегчить борьбу с киберкатастрофами, однако мы должны собрать все эти решения воедино и организовать процесс, потому что злоумышленники хотят создать хаос и не дать вам времени на раздумья.



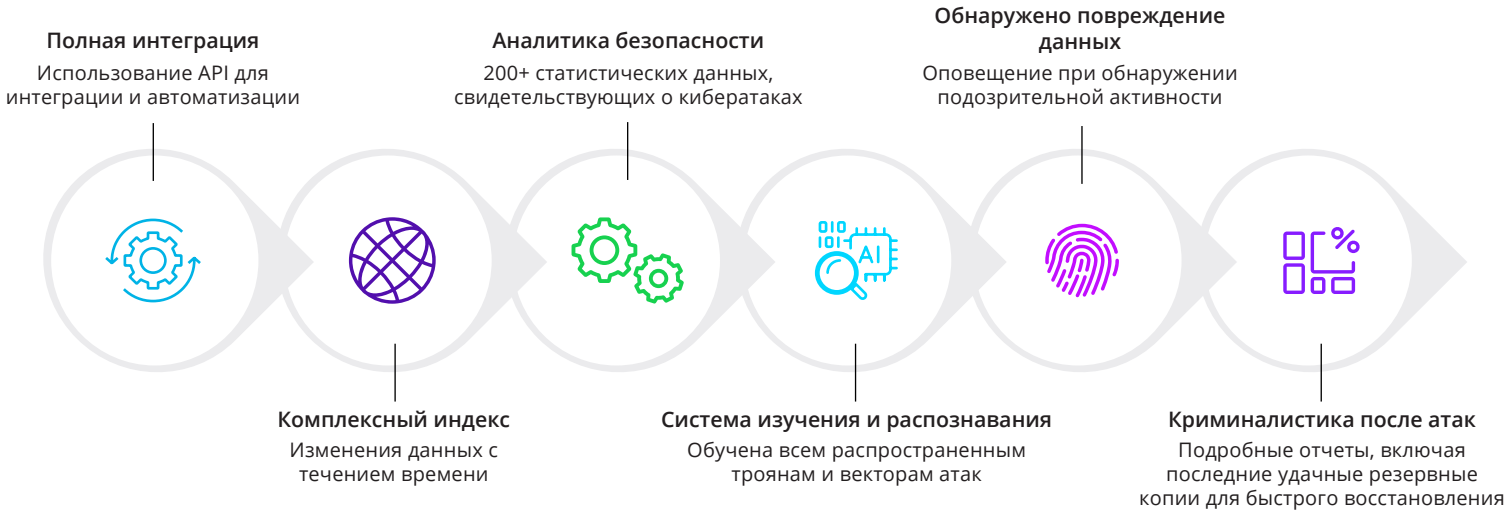
Выявляйте, управляйте и действуйте

Сегодня компании имеют сложные и многоуровневые среды, состоящие из множества инструментов, систем мониторинга и процессов. В центре многих из них находятся специальные операционные центры безопасности (Security Operations Centers, SOC). В рамках SOC существует ряд приложений, предназначенных для обеспечения безопасности инфраструктуры, в том числе множество решений, обозначенных как SIEM (Security Information and Event Management) и SOAR (Security Orchestration And Response). Среды SIEM и SOAR являются центром сбора информации обо всем, что связано с безопасностью, как только обнаруживается проблема. Следующий шаг - создание четко определенного и контролируемого процесса, который выполняется со скоростью вычислений без необходимости длительного вмешательства человека. Доли секунды имеют значение, и для того, чтобы иметь шанс ограничить уязвимость, важно выполнять процесс практически мгновенно.

Как Infinidat добивается этого? Да очень просто. Уже много лет мы используем возможности InfiniSafe в наших продуктах. У нас есть мощная эталонная архитектура InfiniSafe для семейства InfiniBox, которая легко расширяется и оркестрируется для запуска по любому событию в любой среде. В данном случае она может быть запущена средами SIEM или SOAR компании. Эти прикладные среды имеют расширяемые интерфейсы через API или CLI; их объединение с четко определенной эталонной архитектурой InfiniSafe обеспечивает полностью автоматизированный набор возможностей, которые можно организовать для проактивного и быстрого создания неизменяемых снимков для защиты наиболее важных активов компании.

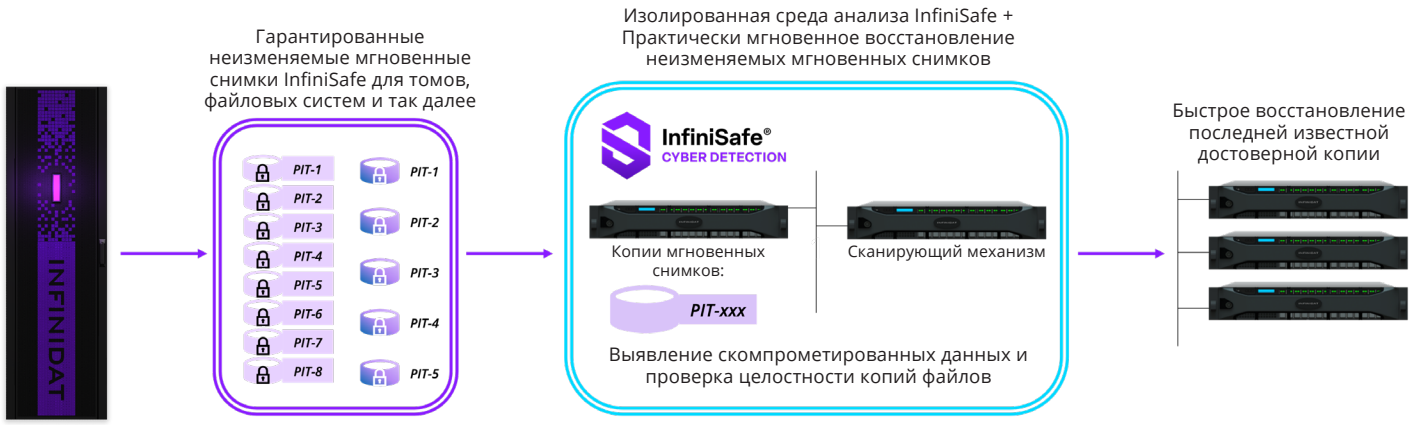
Проверьте данные и быстро их восстановите

InfiniSafe также имеет возможность организовать создание изолированной среды для анализа данных



на предмет наличия атаки – отдельного сетевого пространства, не связанного с внутренней сетью или системами пользователей, которые могли пострадать. Вы можете и должны иметь выделенный набор ресурсов вне производственной среды для тестирования и проверки данных с соответствующими инструментами и необходимым программным обеспечением. InfiniSafe может мгновенно презентовать неизменяемые снимки томов или файловых систем в изолированную среду анализа, чтобы использовать все имеющиеся в вашем распоряжении инструменты для проверки данных. Infinidat также может помочь в этом процессе проверки, используя мощные и эффективные инструменты.

InfiniSafe Cyber Detection – это дополнительное решение к бесплатным компонентам InfiniSafe. InfiniSafe Cyber Detection выполняет глубокое сканирование блочных, файловых данных и баз данных, представляя



неизменяемые снимки InfiniBox и InfiniBox™ SSA мощному механизму сканирования на основе искусственного интеллекта. В ходе сканирования проверяется целостность данных и с помощью машинного обучения на основе искусственного интеллекта выявляются любые вредоносные изменения в результате кибератаки. Более того, сканирование использует более 200 точек данных, чтобы определить, какие данные могли быть скомпрометированы, с точностью 99.99%. Такой уровень точности и детализации делает любую дополнительную проверку очень точной и удобной для принятия мер, сводя к минимуму возможные ложные срабатывания, поскольку при работе с киберинцидентами необходимо действовать быстро и точно. Для расширения этой функциональности InfiniSafe Cyber Detection необходимо приобрести лицензию на соответствующую емкость для сканирования.

Резюме

Злоумышленники создают хаос и завладевают наиболее важными активами данных, если вы не готовы к этому. Знание состояния ваших данных и их проактивная защита – это ключевой компонент, позволяющий сократить окно угроз, вернуть себе рычаги влияния и помешать тем, кто хочет получить от вас деньги, компрометируя ваши данные.