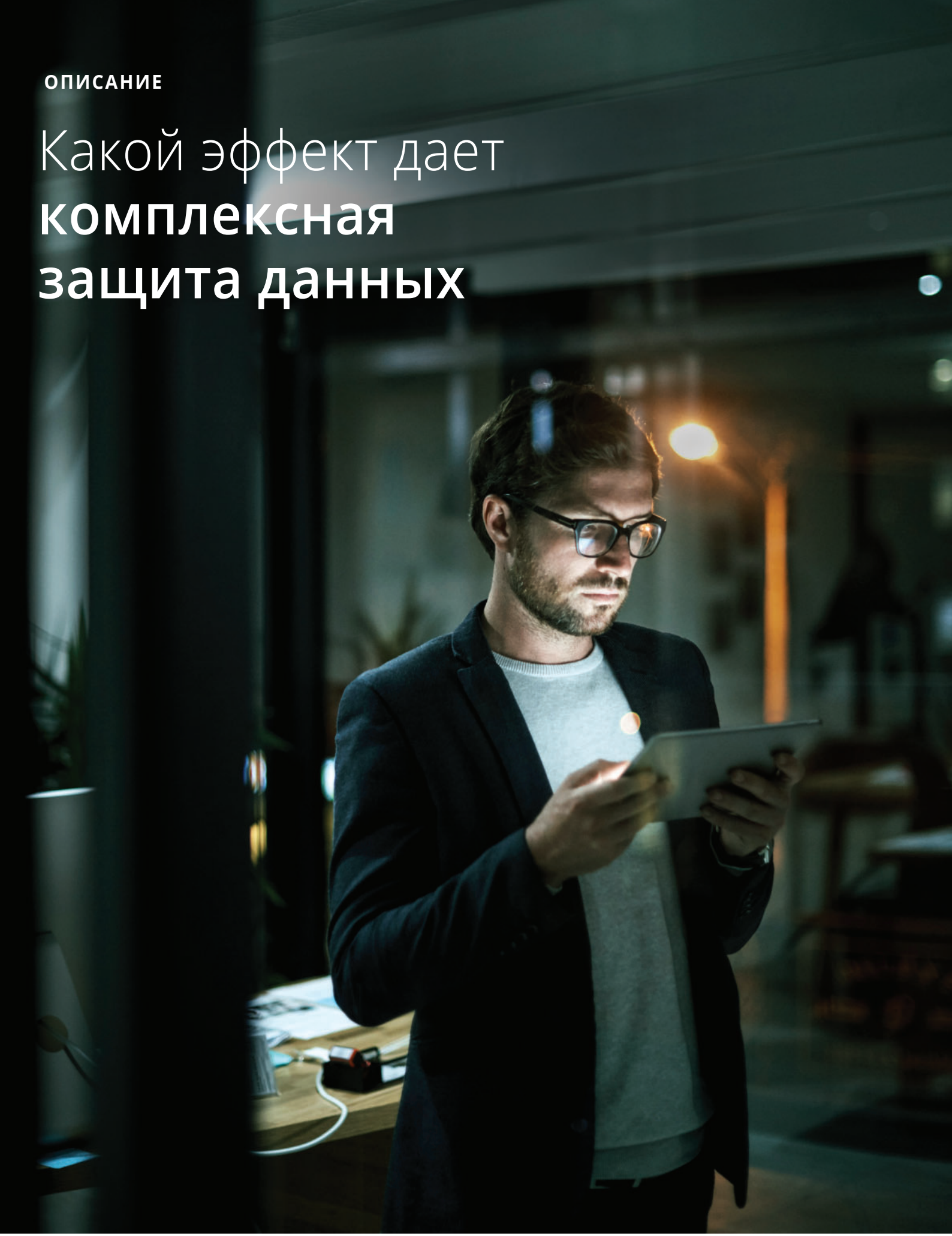
ОПИСАНИЕ

# Какой эффект дает **комплексная защита данных**



МАСШТАБ КАК КЛЮЧ К УСПЕХУ

INFINIDAT

# Предпосылки

Директорам по ИТ/ИБ пришлось нелегко в 2017-2018 гг. и вряд ли станет легче в 2019 г. В свете громких отставок из-за утечек данных в 2017 г. (Equifax, Uber, Yahoo и пр.) и ужесточения требований регуляторов по всему миру директора по ИТ/ИБ обязаны пересмотреть подход к защите данных в их компаниях. Помимо соблюдения требований регуляторов, компании отвечают перед своими заказчиками и акционерами за максимальную защиту данных как от внешних злоумышленников, так и от собственных сотрудников. Самым распространенным способом получения данных в 2017 г. была рассылка фишинговых писем сотрудникам компании (см. Отчет о расследовании утечек данных 2017 г.), в результате чего сотрудники оказываются невольно замешаны в утечках данных. Более 80% кибератак увенчались успехом из-за человеческого фактора.  Открывая внешне безобидное вложение или переходя по ссылке, сотрудник непреднамеренно ставит данные компании под угрозу. Хотя стопроцентной защиты не бывает, можно, руководствуясь здравым смыслом, уменьшить поверхность атаки в любой компании.

**Думая о защите данных от хакеров, нужно помнить о двух терминах.**

> ***«Поверхность атаки — это совокупность разных точек программной среды («векторов атаки»), в которых несанкционированный пользователь («злоумышленник») может попытаться ввести зловредные или вывести полезные данные. Сделать поверхность атаки как можно меньше – основная мера безопасности.»*** *(Википедия)*

Компания, считающая свои данные источником конкурентного преимущества и осознающая их важность для заказчиков, должна минимизировать поверхность атаки. Почему all-flash массивы этому мешают?

# Когда организационная структура определяет метод защиты

Закон Конвея гласит, что организационная структура как ничто другое прямо влияет на результат/проект. В контексте безопасности все довольно просто: если ИБ-директор и руководитель отдела систем хранения координируют свои действия, то, скорее всего, ваши данные будут шифроваться на уровне СХД и режим шифрования будет включен. СХД – это еще и «путь наименьшего сопротивления», поскольку в массивах хранения можно мгновенно шифровать данные без ущерба для производительности. Однако помогает ли шифрование на уровне СХД уменьшить поверхность атаки? Да, немного. Но при этом ВСЕ другие уровни остаются незашифрованными и данные перемещаются по сети без какой-либо защиты.

# Где же шифровать данные?

Вдумайтесь: чем выше происходит шифрование персональных/конфиденциальных данных, тем больше уровней остаются защищенными. В нижеприведенной таблице каждая строка представляет собой поверхность атаки при том или ином уровне шифрования данных.

**Заметили, как мало на самом деле шифрование на уровне СХД защищает данные? Между тем, этот способ защиты данных широко используется.**

| **Где применяется шифрование** | ✓ **Кто может видеть данные?** ⚠ **Кто может случайно спровоцировать утечку?** | | | | | | |
|---|---|---|---|---|---|---|---|
| | Администратор приложений | Администратор ОС | Администратор БД | Администратор ВМ | Администратор сети | Администратор СХД | Администратор резервного копирования |
| Приложения | ⚠ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ОС | ⚠ | ⚠ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Базы данных | ⚠ | ⚠ | ⚠ | ✓ | ✓ | ✓ | ✓ |
| Виртуальные машины | ⚠ | ⚠ | ⚠ | ⚠ | ✓ | ✓ | ✓ |
| Сеть (данные в процессе передачи) | ⚠ | ⚠ | ⚠ | ⚠ | ✓ | ⚠ | ⚠ |
| СХД | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ |
| Резервное копирование | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ | ⚠ |

# Почему all-flash массивы увеличивают поверхность атаки?

Большинство all-flash массивов (если не все) предлагают шифрование на уровне дисков и только там. Если же данные шифруются в другом месте, то all-flash массив не может уменьшить объем хранения с использованием компрессии и дедупликации, теряя всю свою экономическую привлекательность. All-flash массивы должны уменьшать объем данных в соотношении 1:3 и 1:6, чтобы заказчики могли их себе позволить.

Иными словами, развертывая инфраструктуру продуктивной среды на all-flash массивах, заказчики по сути лишают себя возможности внедрить политику сквозного шифрования, которая сейчас требуется во всех нормативных положениях по защите данных (GDPR, SB-1386, HIPAA, PCI DSS, NY-DFS и др.).

# Когда «оптимально» это еще и осуществимо

**ОПТИМАЛЬНЫЙ ПОДХОД К ЗАЩИТЕ ДАННЫХ ЧАСТО ОГРАНИЧИВАЕТСЯ РЕАЛИЯМИ ЗАКАЗЧИКА:**

- Приложение десятилетней давности, которое не обеспечивает шифрование и больше не поддерживается
- Критичное для бизнеса приложение, которое обновляется раз в год
- Владелец приложения, который не будет тратить время на внедрение шифрования

Когда доходит до дела, зачастую лишь компромисс позволяет ускорить внедрение технологий защиты данных. Для соблюдения правил компании и требований регуляторов многие заказчики предпочтут шифровать эти среды на более низких уровнях стека (БД/ВМ/ОС). Так часто приходится делать, чтобы обеспечить нормативно-правовое соответствие в срок; тем не менее стоит ограничить количество применяемых компанией подходов, чтобы избежать чрезмерных накладных расходов. Отметим еще раз, что у всех этих альтернатив эффект одинаковый – все они мешают all-flash массивам уменьшать объем хранения и тем самым увеличивают совокупную стоимость владения СХД.

# Дополнительные преимущества шифрования на верхних уровнях стека

### РАСПРЕДЕЛЕНИЕ / ПРОИЗВОДИТЕЛЬНОСТЬ

Если не брать в расчет самошифрующиеся диски (SED), то для обеспечения производительности требуются ресурсы ЦП. В ИТ-стеке часто серверов больше, чем массивов хранения. Перемещая шифрование на более высокий уровень стека, вы еще и получаете более широкое распределение рабочей нагрузки, уменьшаете нагрузку на отдельное устройство и оптимально распределяете нагрузку по вычислительным мощностям.

### ГРАНУЛЯРНОСТЬ

Чем выше происходит шифрование в стеке, тем лучше гранулярность.

Приложение может шифровать только информацию, позволяющую установить личность человека (PII), так как понимает контекст и значение данных. Это также снижает накладные расходы. Если спуститься на уровень ниже, администратор баз данных может предоставить зашифрованную и незашифрованную табличные области и поместить нужные данные в нужное место. Пусть так гранулярность ухудшается, это все равно лучше, чем шифровать ВМ или логический диск (LUN) целиком.

### ГОТОВНОСТЬ К ПЕРЕХОДУ В ОБЛАКО

Перенос шифрования на более высокий уровень в стеке — необходимое условие для любой миграции в облако, если нужно обеспечить и поддерживать тот же уровень защиты данных и в сети WAN. Данным, которые уже зашифрованы локально на стороне источника, не требуются дополнительные меры защиты при миграции в облако, что позволяет использовать как гибридное облако, так и сразу несколько разных облаков, ведь приложение не привязано к механизмам защиты конкретного поставщика облачных услуг.

### ЛЕГКАЯ ИНТЕГРАЦИЯ

Интеграция шифрования на уровнях ОС/БД/гипервизора удобна тем, что их разновидностей очень мало, в то время как самих приложений в среде много. Это может облегчить эксплуатацию.

## ЧТО ДЕЛАТЬ

- Спланируйте политику комплексной защиты данных в вашей организации
- Установите крайний срок, после которого новые приложения будут сразу разрабатываться с функционалом шифрования
- Обучите собственных разработчиков методологиям проектирования приложений со встроенной безопасностью (security-by-design)
- Изучите имеющиеся приложения, чтобы найти лучший для вашей организации способ защиты данных на лету при их передаче
- Спланируйте переходный период для шифрования давно внедренных приложений с конфиденциальными или секретными данными