Microsoft объявила о масштабной перестройке архитектуры безопасности Windows: антивирусы (AV) и системы обнаружения угроз (EDR) больше не будут работать на уровне ядра ОС.

Решение связано с инцидентом 2024 года, когда сбой обновления CrowdStrike привёл к сбоям на более чем 8,5 млн устройств.

Теперь Microsoft совместно с крупнейшими игроками отрасли — CrowdStrike, Bitdefender, ESET, Trend Micro и другими — разрабатывает новую платформу безопасности. Главная цель — исключить критические сбои и повысить стабильность Windows, избавив систему от необходимости доверять драйверам с полным доступом к памяти и оборудованию.

В ближайшее время стартует закрытое тестирование, в рамках которого вендоры смогут предложить правки API. Microsoft подчёркивает, что проект создаётся совместно с партнёрами, а не навязывается сверху.

Переход будет постепенным — сначала нововведение затронет антивирусы и EDR. В будущем изменения могут распространиться и на античит-системы в играх.

Также Microsoft готовит функцию Quick Machine Recovery для быстрого восстановления после сбоев и переработанную, теперь чёрную, версию «экрана смерти».

Все права защищены

save pdf date >>> 26.01.2026