

nexpose<sup>®</sup>  
ultimate

## Определите самые серьезные риски

Rapid7<sup>®</sup> Nexpose<sup>®</sup> Ultimate — это единственное решение для управления уязвимостями, которое приоритизирует уязвимости, средства контроля и конфигурации в современных вычислительных сетях, позволяя быстрее принимать более эффективные решения по управлению рисками.

Nexpose использует: технологии RealContext™ и RealRisk™; данные об критичных угрозах, предоставляемые платформой Metasploit; сведения об оценке безопасности, предоставляемые платформой ControlsInsight — для приоритизации и оценки рисков. Это дает возможность сконцентрироваться на устранении тех уязвимостей, которые чреваты наибольшими последствиями.

130 000

Получите решение корпоративного класса для обеспечения безопасности, которое может своевременно определить более 52 000 уязвимостей и осуществить 130 000 проверок в вашей вычислительной сети.

### Используйте комплексный подход в управлении уязвимостями

Nexpose Ultimate предоставляет самые передовые технологии для исследования систем безопасности в физических, виртуальных и облачных средах. Тесная интеграция между решениями Nexpose Enterprise, ControlsInsight и Metasploit позволяет определить наиболее значимые риски для систем безопасности вашего предприятия.

### Проводите оценку уязвимостей с помощью Metasploit<sup>®</sup> Pro

— Nexpose представляет собой единственное решение полного цикла, которое органично интегрируется с Metasploit Pro. Платформа Metasploit Pro основана на самом популярном в мире программном обеспечении для тестирования на проникновение и предназначена для оценки уязвимостей и возможностей их использования; проверки эффективности средств контроля; обеспечения эффективных мер по устранению факторов риска и их последствий.

### Приоритизируйте и выбирайте меры по восстановлению с помощью технологий RealContext™ и RealRisk™

— только Rapid7 RealContext позволит вам сконцентрироваться на самых значимых для вашей организации угрозах. Это достигается с помощью автоматизированной классификации ИТ-активов, приоритизации рисков и определения мер по восстановлению. Технология RealRisk использует подход, ориентированный на специфику угроз (threat-driven approach), и осуществляет ранжирование рисков на основе данных об известных эксплойтах и временных показателях — они повышают вероятность компрометации.

### Анализируйте эффективность ваших средств защиты и контроля

— автоматически оценивайте конечные точки и серверы, чтобы получить полное представление о развертывании защитных и контрольных механизмов и выявить их недостатки. Оцените действенность этих средств при защите от реалий современного ландшафта угроз, используя лучшие методики по снижению рисков.

201014

Rapid7 EMEA Headquarters | 1st Floor, Building 1025, Arlington House, Reading, UK

+44 (0) 1183 703500

emeasales@rapid7.com

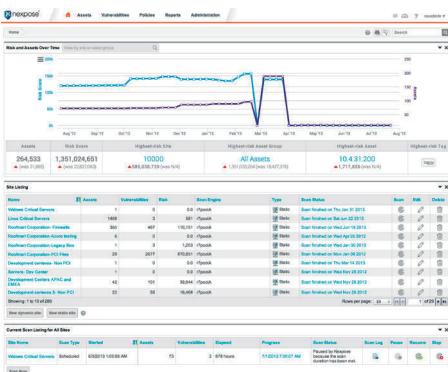
**RAPID7** | Rapid7.com

| Обзор Rapid7.com Nexpose Ultimate

# nexpose<sup>®</sup> ultimate

«Мы снизили  
риски более чем  
на 98%. Это  
очень  
впечатляющий  
показатель,  
учитывая, что мы  
открыли пять  
новых больниц в  
те же сроки».

— Скотт Эрвен  
(Scott Erven),  
руководитель отдела  
информационной безопасности,  
Essentia Health



## Определите самые серьезные риски

**Быстрые, унифицированные решения для обеспечения защиты и соблюдения нормативных требований** — сократите влияние угроз на сеть, оптимизируйте процесс оценки систем безопасности и соблюдения требований и унифицируйте отчетность с помощью единой процедуры проверки уязвимостей, средств контроля, политик и конфигураций.

**Определение уязвимостей с помощью Metasploit<sup>®</sup> Pro** — Nexpose интегрируется с Metasploit Pro, что позволяет оценивать уязвимости и возможности их использования, тестировать эффективность средств контроля и обеспечивать эффективное восстановление.

**Rapid7 RealRisk<sup>™</sup> осуществляет приоритизацию с учетом специфики угроз (threat-driven approach)** — получите точное представление о самых важных уязвимостях, используя технологию Rapid7 RealRisk. Это решение использует аналитическую информацию по различным типам угроз, включая эксплойты, систему ранжирования CVSS v2 и временные метрики факторов риска.

**Будьте на шаг впереди злоумышленников** — запатентованная аналитическая модель Rapid7 противопоставляет современным угрозам эффективные защитные механизмы и количественно оценивает успешность внедрения средств обеспечения безопасности.

**Получите всю информацию об обновлениях безопасности, приложениях, политиках конфигурирования и методах защиты.**

**Мощные возможности по анализу рисков и данных** — Nexpose предоставляет полностью настраиваемые встроенные шаблоны отчетов. Динамические группы активов

и фильтрация уязвимостей помогают специалистам по ИБ быстро оценивать риски инфраструктуры.

**Эффективное управление рисками с помощью технологии RealContext<sup>™</sup>** — только Rapid7 RealContext позволит вам сконцентрироваться на самых опасных угрозах. Это достигается с помощью автоматизированной классификации активов, приоритизации рисков и выбора мер по восстановлению.

**Удостоенные многих наград планы восстановления** — эффективно устраняйте возможные угрозы с помощью самых результативных на сегодняшний момент руководств по восстановлению. Краткие, точные и действенные инструкции помогут ИТ-специалистам быстро исправить проблемы.

**Повышение эффективности средств контроля** — получите ценную информацию о системах защиты от современных угроз и план действий с расставленными приоритетами, который позволит повысить уровень безопасности вашей инфраструктуры.

Согласуйте свою деятельность с лучшими методиками, такими как руководства Council on CyberSecurity Critical Security Controls и ASD TopMitigation Strategies, а также стандарт NIST 800-53.

**Упрощение аудита и соблюдение отчетности** — соответствуйте требованиям таких стандартов в сфере управления рисками, уязвимостями и конфигурациями, как PCI DSS, NERC CIP, FISMA, HIPAA/HITECH, Council on CyberSecurity Top 20 CSC, DISA STIGS, USGCB, и CIS.

**Детализированная фильтрация ИТ-активов** позволяет управлять различными группами активов на основе бизнес-контекста или других критериев.