NEXTLABS®

Safeguard Your Mission-Critical Data & Crown Jewels

Newsletter Q3 2022

Key Takeways

- How to Safeguard Mission-Critical Data in Today's Dynamic Digital Environment
- Intellectual Property Protection: Best Practices
- Deloitte - CMMC 2.0: Explore What it Means for You
- New Expert Q&A Series
- NextLabs Releases Global Data Access Security Suite 2022

HOW TO SAFEGUARD MISSION-CRITICAL DATA IN TODAY'S DYNAMIC DIGITAL ENVIRONMENT

Mission-critical data, intellectual property, such as development research, CAD/CAM designs, trade secrets, and strategic business plans are a company’s most important assets. Protecting these assets are essential to running your business.

Unfortunately conventional perimeter-based network security is no longer sufficient to address the increased security requirements for internal and external sharing of sensitive information. Learn how you can ensure persistent protection of mission critical data and intellectual property using EDRM technology.

In today's dynamic digital environment, businesses need a way to ensure their technical data is being persistently protected when collaborating with internal and external stakeholders. Enter EDRM, a technology that thrives in dynamic business settings that rely on collaboration of intellectual property and mission critical data with external partners and cross border business units.

Watch Now

NEXTLABS®

WHITEPAPER RESOURCE

INTELLECTUAL PROPERTY PROTECTION

In a collaborative supply chain, companies cannot simply lock their data in a safe. Instead, organizations need to take a risk management approach to IP protection: identify risks, tackle the largest ones first, design controls to address those risks, implement and audit the effectiveness of these controls, and repeat as necessary. In this white paper, you will learn about ten best practices developed by working closely with customers to protect IP.

Read More

NEXTLABS®

EXTENDING TEAMCENTER & AUTHORIZED DATA ACCESS (ADA) MODEL TO PROTECT FILES WITH DRM

Product teams seek to securely collaborate with partners and supply chains, while also delivering critical information, like trade secrets, without running the risk of compromise.

In this video, you will learn how NextLabs Teamcenter DRM helps enterprises ensure persistent protection of intellectual property, allowing products teams to securely collaborate and share sensitive designs and projects in a multi-level supply chain.

Watch Now

NEXTLABS®

SOLUTION BRIEF

PHARMACEUTICALS & LIFE SCIENCES

When it comes to data collection, monitoring, and reporting, many pharmaceutical companies have used manual controls and procedures, making it exceedingly challenging to safeguard criical data and stay in compliance with regulations. In this solution brief, you will learn how externalized authorization and digital rights management can be used to protect highly sensitive intellectual property and automate GxP compliance through the use of automated real-time policies.

Read More

NEXTLABS®

BLOG

A SENSIBLE APPROACH TO DRM AND FILE SHARING SERVICES

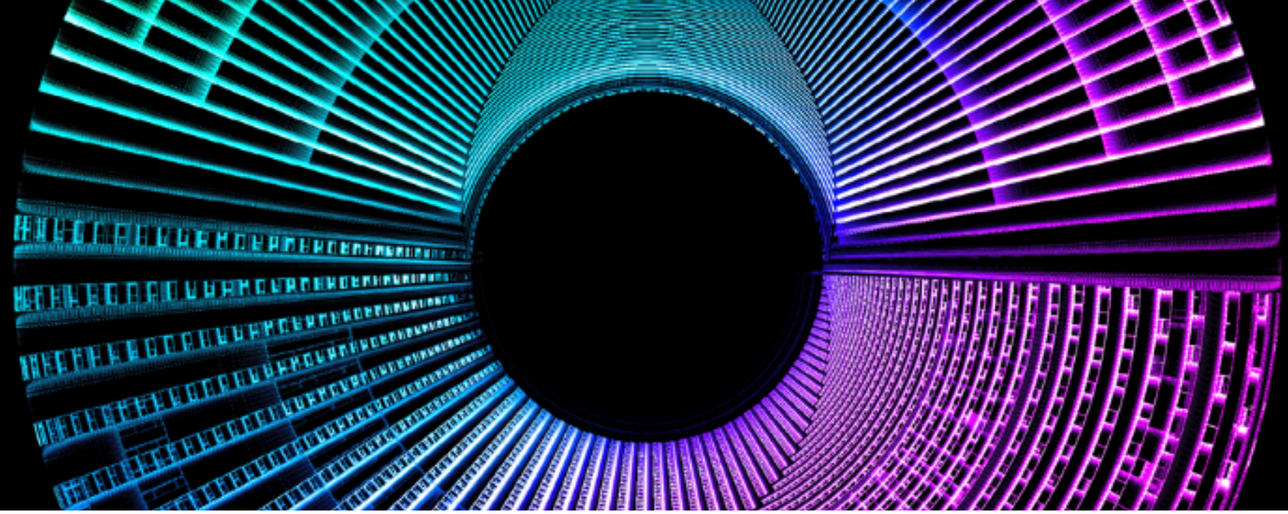
File-sharing services like Box, Dropbox, Google Drive, and OneDrive have some level of native security built into them, but it's not enough to fully protect your data once it's been shared. Stolen passwords, account takeovers, insiders with malicious intent, and just plain carelessness are part of the equation when it comes to cloud applications and security breaches.

In this blog, you will learn how digital rights management (DRM) solutions can help strike the balance between sharing and security for file sharing services.

Read More

NEXTLABS®

Deloitte.



Featured Article

CMMC 2.0: EXPLORE WHAT IT MEANS FOR YOU

The Cybersecurity Maturity Model Certification (CMMC) was designed to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). In November 2021, CMMC 2.0 was announced, with some significant changes.

In this featured article, Deloitte covers the changes between CMMC 1.0 and 2.0, the current landscape, and how enterprises can prepare for this.

Read More

NEXTLABS®

EXPERT Q&A

NextLabs is introducing a new expert Q&A series on cybersecurity to provide a platform for thought leadership via interviews with industry experts.

The Cybersecurity Expert Series explores important cybersecurity topics to provide educational and thought-provoking conversations. Through this series, industry experts will share insight, common practices, and advice on relevant topics in the industry.

Watch Now

Episode 1: part 1: NIST Mitigating Ransomware Risk Insights

In episode one of the NextLabs Cybersecurity Expert Series, NIST National Cybersecurity Center of Excellence (NCCoE) Security Engineer Bill Fisher covers data security and ransomware defense. In Part one of this episode, Bill covers what ransomware attackers are trying to accomplish, how ransomware is distinct from other types of malware, and why ransomware is still so prevalent today.

Watch Now

Episode 1: part 2: NIST Mitigating Ransomware Risk Insights

In the second part of episode one, Bill Fisher references the NIST Cybersecurity Framework as a vital component for organizations looking into mitigating cybersecurity risk. He also goes on to dive deeper into mitigating ransomware risk and what resources NIST offers to help manage these risks.

Watch Now

Episode 2: Why is Zero-Trust Architecture (ZTA) important?

In episode two, Alper Kerman details what Zero-Trust Architecture (ZTA) is, its efficacy, core components, and deployment options. Alper currently serves as the technical lead for the zero-trust demonstration project at the NCCoE and has more than 30 years of experience in IT.

PRESS RELEASE

NEXTLABS RELEASES GLOBAL DATA ACCESS SECURITY SUITE 2022

Adding major data masking and segregation enhancements, including format preserving encryption (FPE), enhanced database support, and awareness of primary and foreign key relationships.

Read More

NEXTLABS®

PROTECTING INTELLECTUAL PROPERTY AND TRADE SECRETS WITH A DATA-CENTRIC SECURITY MODEL

WEBINAR

Intellectual property and trade secrets, although intangible, can be some of the most valuable assets of an enterprise, especially as the world moves towards a more digitized knowledge-based economy. It is critical that organizations safeguard these assets to maintain their advantage in an ever more globalized competitive landscape.

Join NextLabs and IBM on **Sept. 14 at 5 PM CET (8 AM PST)**, to learn how to protect intellectual property and trade secrets with a data-centric security model. In this webinar, our experts will describe best practices for protecting intellectual property and trade secrets using a data-centric security model.

Register Here

NEXTLABS®

SKYDRM PRODUCT LINE UPDATE AUGUST 2022

NextLabs recently extended many of its SkyDRM capabilities to improve functionality and user experience for intellectual property protection, secure collaboration, and dynamic file access control. Enhancements are seen on the SkyDRM platform, along with its Teamcenter, Microsoft Office, SAP, Bentley ProjectWise, and various CAD integrations via the Rights Management Extensions (RMX).

Read More

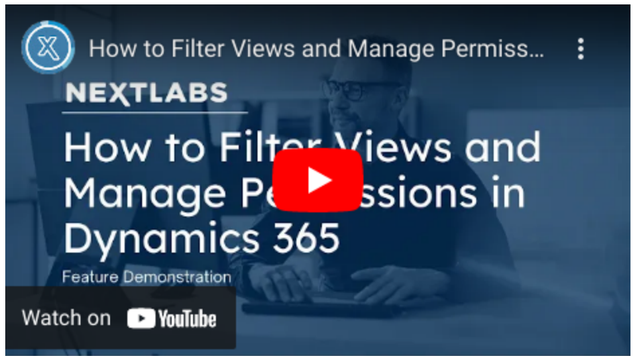
NEXTLABS®

ON-DEMAND VIDEOS

Our on-demand video catalog provides a variety of information about NextLabs' solutions and technology.

The catalog includes regularly uploaded webinars, demos, and informational introductory videos featured through the NextLabs' YouTube channel.

Explore our on-demand videos



Watch Now

Watch Now

Watch Now

Watch Now

NEXTLABS®

NEXTLABS®

POLICY DRIVEN INTELLIGENT ENTERPRISE

DATA CENTRIC SECURITY

POWERED BY DYNAMIC AUTHORIZATION