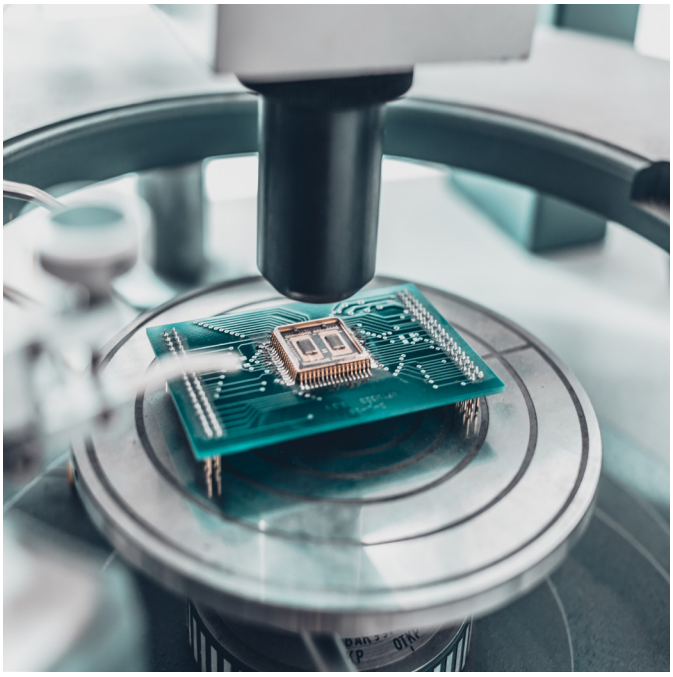
KLA-Tencor

Semiconductor Equipment



SUMMARY

KLA-Tencor is the leading supplier of process control, metrology, and yield management solutions in the semiconductor and related microelectronics industries. Central to KLA-Tencor's success is their advanced technology and their speed in servicing their system and equipment in the field. In order to help customers maximize their production yields, KLA-Tencor equips more than 2,000 field engineers with laptops containing up-to-date knowledge in system diagnostics and yield optimization analysis. However, this wide distribution of business-critical technical data also greatly heightens the risk of data leakage. Responding to this issue, KLA-Tencor chose NextLabs Data Protection software to safeguard its intellectual property (IP) in the field—across various formats and throughout its lifecycle.

ENVIRONMENT

Over 2000 field engineers using laptop computers in 18 countries across Europe, North America, and Asia/Pacific.

CHALLENGE

The need to protect valuable intellectual property (IP) for customer information and KLA-Tencor's system knowledge stored in field engineer laptops:

- How do you prevent data leakage through file sharing, e-mail, and removable USB devices?
- How do you protect data seamlessly throughout the data lifecycle without affecting a field service application or end-user workflow?

SOLUTION

NextLabs Information Risk Management Suite – NextLabs Data Protection

- Protect IP data with encryption
- Prevent data loss with renewable licensed access and usage control
- Automate data protection transparently for end users
- Monitor activities with real-time reporting and auditing

> "We looked at a number of IP protection solutions. NextLabs was the only one that was flexible and broad enough to protect the data in our field service application from the server down to the client on mobile devices."
>
> **Director of Knowledge Management**

THE CHALLENGE

KLA-Tencor's Knowledge Management team understood the challenge well: they needed to enable the business-critical sharing of system diagnostic and yield optimization data, while simultaneously protecting that data and governing its usage. While critical IP needed to be made available on field engineer laptops, these laptops were highly vulnerable to loss and theft. Analyzing this challenge, the Knowledge Management team pinpointed specific data protection requirements across the IP lifecycle, including the need to:

• Encrypt data downloaded from a server and stored on a local drive
• Update business-critical technical data that may be mishandled because it is out-of-date
• Prevent unauthorized applications from accessing critical IP• Block wrongful disclosure of IP resulting from duplication to unauthorized storage devices or file servers
• Retroactively remove IP from lost or stolen laptops

The KLA-Tencor team needed a strategy to protect IP across multiple locations, channels, and formats. They sought a balanced solution that would protect data transparently, without disrupting normal user workflow.

The team initially investigated traditional enterprise rights management (ERM) solutions, but quickly discovered they would need to invest extra time and money developing custom integrations to the field service application their engineers rely on. Plus, traditional ERM solutions simply could not address all the specific problem areas the team identified. For example, they cannot address the need to control how data is accessed and used in the field application, including the ability to terminate a running instance of that application when a computer is offline beyond a certain period of time.

THE SOLUTION

The team chose NextLabs Data Protection for its unique ability to safeguard data across its entire lifecycle. Because NextLabs' solution required no custom integration, KLATencor was able to deploy it immediately, saving the time and costs of in-house development.

KLA-Tencor now uses NextLabs Data Protection - Information Rights Management application to provide the following strategic safeguards:

• Encrypting new or updated files generated by the server application, protecting IP on the server.
• Encrypting files on the client and with local private keys, protecting IP on the laptop.
• Automatically invoking updates to the applications database and immediately deleting updated files, reducing IP exposure.
• Allowing only the fingerprinted field service applications to access the encrypted local information, including IP stored in local databases.
• Blocking the leakage of IP to unauthorized USB devices, e-mail, and file servers.
• Preventing the field service application from starting or terminating any running instances, if the laptop has been offline for a certain period of time

In addition, Data Protection monitors and logs user activity, providing real-time reports for forensic investigations and compliance audits. KLA-Tencor's Knowledge Management team deployed Data Protection successfully and rapidly to safeguard IP across the data lifecycle.

NEXTLABS® | Zero Trust Data-Centric Security

ABOUT NEXTLABS

NextLabs®, Inc. provides zero trust data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based zero trust policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, AWS, Accenture, Deloitte, Infosys, and IBM. For more information on NextLabs, please visit: **http://www.nextlabs.com**.