

A DeviceLock® Case Study: **Momenta Pharmaceuticals**

with  IRONKEY™

Abstract:

Momenta Pharmaceuticals of Cambridge, Massachusetts, a biotechnology company specializing in the characterization and engineering of complex drugs has implemented a layered data security infrastructure that encompasses encryption and control of any portable electronic devices (PEDs) allowed connection to its production network. This infrastructure includes PGP® Whole Disk Encryption for securing files on laptops, IronKey® secure USB flashdrives and DeviceLock® for endpoint port-device security. Through its robust white listing features, DeviceLock ensures that only Momenta-allocated IronKeys and other specifically approved devices are allowed per employee account. The use of any other device on a managed Windows endpoints is restricted.



“A product like DeviceLock delivers high value for its intended purpose of port and device-level security. My experience with all-in-one solutions is that they do a bit of everything, but none of them very well. With DeviceLock we got features like integration with Microsoft’s Active Directory, so that we could structure deployment around existing groups. I installed it and had it working within a day.

Tim Mugherini

Senior Manager

Network Infrastructure & Security

Momenta Pharmaceuticals

Biotech Companies

tend to amass around universities with strong biological science and engineering departments. Two of the founders of Momenta Pharmaceuticals Inc., a public company specializing in the characterization and engineering of complex drugs, met and collaborated while professors at the Massachusetts Institute of Technology (MIT). Not surprisingly, proximity to MIT still fuels Momenta's growth, with much of its scientific talent recruited into the company straight out of the university. Following this same natural, symbiotic course of events, there are several hundred other biotech companies just in the Kendall Square area of Cambridge where Momenta makes its home. Such clusters are great places for innovative science, but high-risk areas for intellectual property data leakage.

The risk is compounded by two other common traits of the biotechnology industry:

- Fierce rivalries between competing teams working in similar research areas as they race to achieve patentable breakthroughs.
- Huge winner-take-all monetary rewards for the team that is first to achieve a new patent-protected drug.

In this environment, you don't want to take the risk that one of your scientists might leave an unencrypted thumb drive loaded with their latest research at a coffee shop near work or on the podium after their last university presentation.

At least, Momenta Pharmaceuticals didn't, which is why it has a layered data security infrastructure that encompasses encryption and control of any portable electronic devices (PEDs) allowed connection to its production network. This infrastructure includes PGP Whole Disk Encryption for securing files on laptops, IronKey secure USB flash drives and DeviceLock for endpoint port-device security.

Strategic Goals

"Why encrypt a PC hard drive when you are going to allow the thumb drive lying next to it to be unencrypted?" ponders Tim Mughnerini, Senior Manager of Network Infrastructure & Security at Momenta. "To me, a strategy that accounts for the whole scenario of how employees use and move data is the only sensible approach to encryption."

"Our scientists are highly mobile workers. They need to be able to access data from our network at all times of the day and at night. They regularly collaborate with peers outside our company, particularly over at the university and with our partners. Portable storage devices are an invaluable tool for them as they travel between venues to give and attend presentations sharing findings," Mughnerini explains.

In 2008, when Mughnerini was asked to prioritize the many data security challenges he'd face on the job, he placed portable device encryption and control among the top three. By mid-2009, he had the PGP/IronKey/DeviceLock solution in place.

Massachusetts 201 CMR 17.00

Today, Momenta finds itself well ahead of the pack in its home state, where the Massachusetts Data Protection/Encryption Law, Regulation 201 CMR 17.00, is scheduled to take effect in March 2010. This legislation requires that any firm conducting business with state residents must deploy encryption and otherwise protect against data leakage. While Momenta was primarily motivated to implement its solution to protect its valuable IP data, its encryption strategy also protects the personal identity information of its employees and other Massachusetts citizens. In effect, it is an across-the-board solution that protects all data stored by the company, whatever its use.

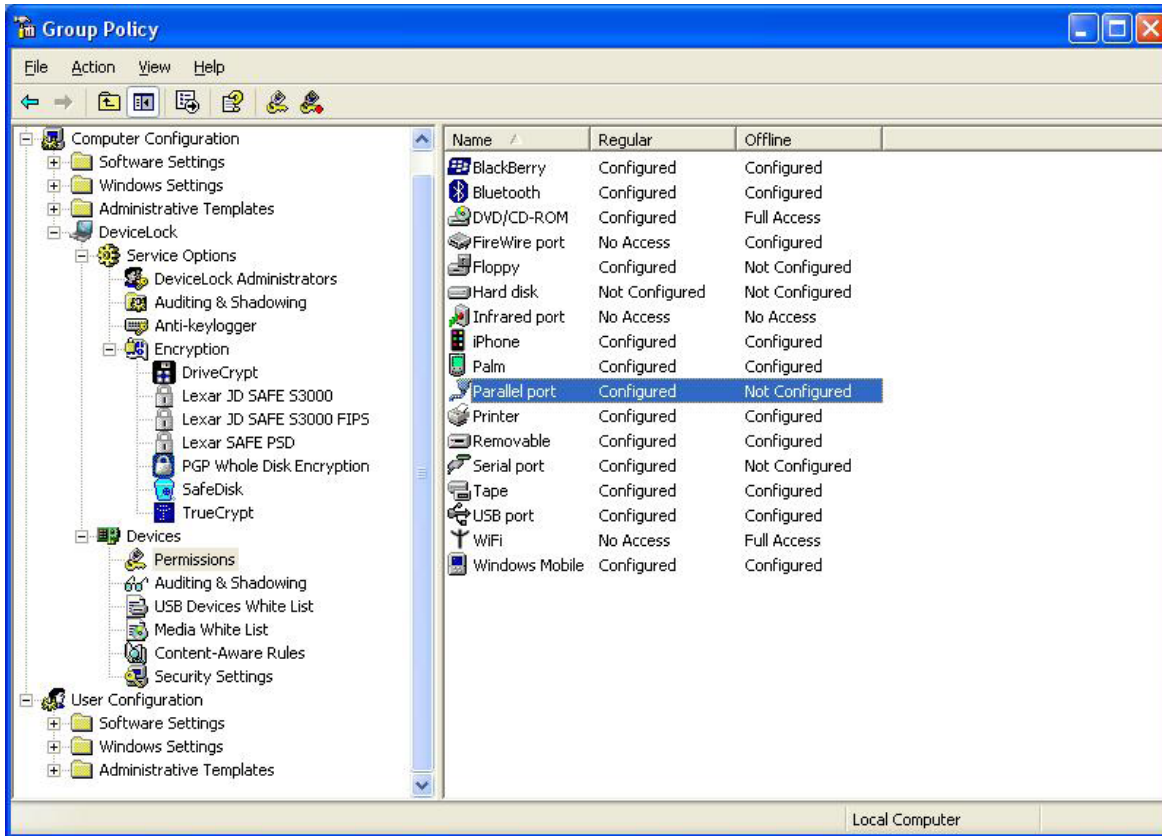
"Understanding the dynamic nature of attacks, we designed a security policy and infrastructure that applies universally to all data and all users," explains Mughnerini. "A receptionist may not be inventing new drugs, but he/she may have VPN

"I think just about everyone in IT security recognizes what needs to be done: you need to layer best-in-class security products until you've covered all the main vulnerabilities." Tim Mughnerini Senior Manager Network Infrastructure & Security Momenta Pharmaceuticals

Key Points

- ▶ **Industry:** Biotechnology
- ▶ **Security Goals:** IP Protection; Compliance with Massachusetts Regulation 201 CMR 17.00
- ▶ **DeviceLock Role:** Enforce use of only Momenta-owned IronKeys and other specifically approved USB devices.
- ▶ **DeviceLock Console:** MMC snap-in console for Group Policy
- ▶ **DeviceLock Audit:** Activated initially for threat assessment
- ▶ **Encryption Integration:** PGP® Whole Disk Encryption*
- ▶ **Approved Encrypted Devices:** IronKey® D20XXX, S-200 & D200 Series* Enterprise, Personal & Basic Models.

* Available bundled with DeviceLock from select DeviceLock channel partners.



- ▶ **DeviceLock MMC snap-in to Group Policy Management: DeviceLock administrators have full central control over access and audit rules covering potential local data leakage channels across the entire Active Directory domain forest.**

access to our production network. If he left behind a flash drive or laptop in a taxi, we would be vulnerable to an attack, just as we would be if a scientist did the same. So, our strategy is that every PC endpoint has a license for DeviceLock, all notebooks have PGP licenses, and each of our employees gets an IronKey.”

Mugherini understands why some enterprises are having greater financial and logistical difficulty deploying a grassroots strategy like Momenta’s. “Passage of the state law did help me sell management on the cost. Many companies have petitioned the state to extend compliance deadlines—now beyond a year—so they can come up with a plan and the resources to comply,” explains Mugherini. “However, I think just about everyone in IT security recognizes what needs to be done: you need to layer best-in-class security products until you’ve covered all the main vulnerabilities. I’m surprised when I talk to peers and learn that some companies have yet to do anything.”

“A product like DeviceLock delivers high value for its intended purpose of port and device-level security. My experience with all-in-one solutions is that they do a bit of everything, but none of them very well. With DeviceLock we got features like integration with Microsoft’s Active Directory, so that we could structure deployment around existing groups. I installed it and had it working within a day. We’re always leveraging this interface when we set-up new users and change

permissions. We’ve allowed certain IT Support staff the right to manage DeviceLock permission setting for various user groups; but, they cannot make global changes. DeviceLock allows us these conveniences and fine-tuning,” comments Mugherini.

Using DeviceLock Audit & White Listing

Mugherini reports that it was an eye-opening experience when Momenta first deployed DeviceLock in audit-only mode and he was able to gather data on all the devices that had been connecting to the network via end-point USB drives. “At the time, we were monitoring about 300 hosts and we found there had been 7200 devices installed at one time or another. There were legitimate reasons for about 25% of those devices. For example, many of our researchers employ scientific instruments, that connect through the USB drive. But, we also found nodes that were hosting up to eight different USB flash drives. Recognizing the security hole, we asked for the devices back. Of course, few were turned in because they’d been lost or misplaced,” laments Mugherini.

Today, Momenta’s IT department has the situation in hand. DeviceLock whitelisting is set up to allow only sanctioned IronKey flash drives to access the production network, and only by their assigned employees. “Hardware encryption is simply better. That’s the first advantage of an IronKey. Another is that you can plug it into whatever system

is available, and everything is self-contained," explains Mugherini. "If our employees were carrying PGP-encrypted files on their flash drives, for example, and they needed to use an outside guest system to unload them for a presentation, the chances that the system would have PGP installed would be slim to none." Allowed USB-connected scientific instrumentation are also whitelisted.

Building in Security Policy Flexibility

Momenta security policy prohibits the attachment of music players and other entertainment or communication devices to the production network. It has set up a guest wireless network that exists apart from the production network that offers some flexibility for those who need an Internet connection for a personal device.

In Summary

"I strive to be realistic about how much security technology solutions can deliver. The driving goal behind our deployment of DeviceLock, PGP, and IronKey was to make sure the data leaving on our devices was encrypted such that, in the event a device were lost or stolen, reasonable protections would be in place," concludes Mugherini.

About DeviceLock

For organizations of any size and industry, DeviceLock software proactively protects endpoint computers against local data leaks and malware infiltration resulting from insider negligence, accidental mistakes or malicious actions. It enables IT security personnel to precisely control, log, shadow-copy and audit end-user access to all types of local ports and peripheral devices, including personal mobile devices, as well as local and network printers. Complementing its

port, device, and data channel-based controls with data type-level security, DeviceLock supports true file type detection and filtering. In addition, DeviceLock blocks operations of USB and PS/2 hardware keyloggers.

About IronKey

IronKey is the global leader in providing secure and managed portable storage, authentication, and trusted virtual computing solutions for mobile workers. IronKey multifunction portable security devices, management software and associated services are designed to meet the security, performance, and privacy standards of the most demanding enterprise and government customers. IronKey solutions range from IronKey Basic, the world's most secure USB flash drive, to the IronKey Enterprise Virtual Desktop solution for carrying a secure operating system and virtual desktop environment on a pocket-sized device. IronKey products are FIPS 140-2, Level 3 validated. Thousands of customers use IronKey, including Fortune 500 companies, enterprise organizations in financial services, healthcare and legal markets, as well as government agencies, including FEMA, NATO and DHS. For more information, please visit www.ironkey.com.

About Momenta

Momenta Pharmaceuticals is a biotechnology company specializing in the detailed structural analysis of complex mixture drugs. Founded in 2001 based on technology initially developed at the Massachusetts Institute of Technology, Momenta is applying its technology to the development of generic versions of complex drug products, as well as to the discovery and development of novel drugs. To receive additional information about Momenta, please visit www.momentapharma.com.

"Hardware

encryption is

simply better.

That's the first

advantage of an

IronKey."

Tim Mugherini
Momenta
Pharmaceuticals

DeviceLock
Proactive Endpoint Security

2440 Camino Ramon, Ste. 130

San Ramon, CA 94583, USA

email: us.sales@devicelock.com

Toll Free: +1 866 668 5625

Phone: +1 925 231 4400

Fax: +1 925 886 2629

The 401 Centre, 302 Regent Street

London, W1B 3HH, UK

Toll Free: +44 (0) 800 047 0969

Fax: +44 (0) 207 691 7978

Via Falcone 7

20123 Milan, Italy

Phone: +39 02 86391432

Fax: +39 02 86391407

Halskestr. 21

40880 Ratingen, Germany

Phone: +49 2102 89211-0

Fax: +49 2102 89211-29

[www.devicelock.com]