



The discovery and development of stem cell therapeutics

Biotechnology Firm Implements Cost Effective Solution to Meet LAN Security Challenges

As an innovator in biotechnology, StemCells, Inc. understands the need for investing in state-of-the-art infrastructure – from their clinical lab equipment to their networking solutions. That's why they chose the Nevis LANenforcer solution for deploying access control within their enterprise to protect data integrity and confidentiality as a solution for intellectual property protection and improved auditability.

StemCells, Inc. needed a way to implement a compliant LAN security strategy and at the same time, contain costs and improve productivity. Nevis' LANenforcer was chosen as the foundation for StemCell's LAN security strategy.

About StemCells, Inc.

StemCells, Inc. is a clinical-stage biotechnology company focused on the discovery, development and commercialization of cell-based therapeutics to treat diseases of the nervous system, liver and pancreas. The Company's programs seek to repair or repopulate neural, liver or other tissue that has been damaged or lost as a result of disease or injury. StemCells is the first company to directly identify and isolate human neural stem cells from normal brain tissue. These cells are expandable into cell banks for therapeutic use, which offers the potential of using normal, non-genetically modified cells as cell-based therapies. StemCells has approximately 40 U.S. and 100 non-U.S. patents.

Key Challenges

StemCells, Inc. was faced with a number of business and technical challenges with respect to protecting sensitive data, particularly with respect to ensuring appropriate access control, traffic analysis, and securing against malware outbreaks.

Security Policy Requirements

- Provide increased access control and security for the executive staff, administrators, and third parties;
- Enhance existing centralized security controls at the server datacenter and R&D Labs;
- Provide an audit trail that reliably ties user identity to access control violations for meeting regulatory compliance and auditing purposes;
- Protect common access areas from unauthorized access.

Operational Requirements:

- Initiate agile migration from legacy LAN switches with next generation technology;
- Decrease IT operational expenses due to virus outbreaks and exploits;
- Limit access to specific StemCells network resources to only specific users and user groups based on organizational role and responsibility profiles;
- Secure conference rooms and public access areas by forcing guest users to authenticate and provide granular access control policies for LAN resources;
- Detect and prevent malicious code - including zero day exploits - from propagating to other users and servers on the networks;

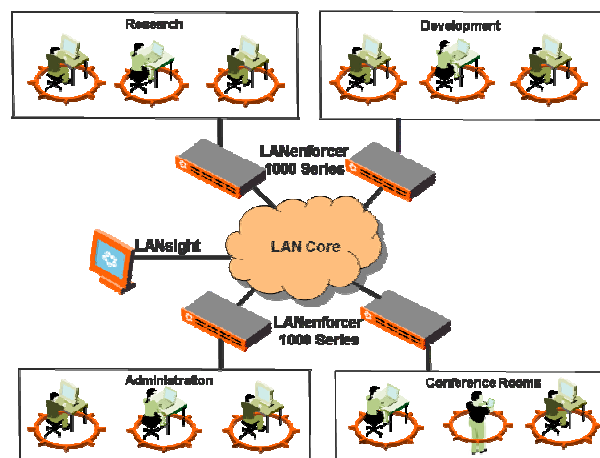
Nevis' Solution for StemCells

By implementing the Nevis LANenforcer solution, StemCells has addressed all of the technical requirements of their corporate security policy. Specifically, Nevis LANenforcer Switch technology provides StemCells with consistent, repeatable, auditable and verifiable practices needed to access and track vital compliance-relevant data access and activity. From a security perspective, StemCells enjoys the following benefits from the Nevis solution:

- ✓ Policy-based access control to corporate resources;
- ✓ Correlation of security violations to specific user identities, providing a reliable audit trail to demonstrate due diligence and conduct in-depth investigations;
- ✓ Immediate and proactive protection against malware outbreaks;
- ✓ Blocking and quarantine of zero day worm outbreaks within microseconds through per port/per user anomaly detection features;
- ✓ Ability to secure data transmission via wire speed encryption over the LAN.

Access Control Achieved via Security Zone Architecture

As seen in the diagram on the right, StemCells is in the process of deploying the LANenforcer 1048 switches. The 1048's will be used to segment their LAN into specific security zones. Granular security policies are enforced on a per port / per user basis to ensure the principle of least privilege, and maintain data integrity and confidentiality.



Nevis Delivers Rapid ROI to StemCells

Overall, the Nevis solution represented a 20% savings compared to competing independent intrusion prevention solutions in a combined switch technology platform. Additionally, the IT team has significantly reduced the time spent investigating the root causes behind security incidents. Through leveraging the LANsight manager, StemCells can immediately associate potential suspicious activity to a specific user. By reducing costly disruptions associated with malware outbreaks, StemCells has enjoyed increased productivity through its Nevis implementation. Patching servers and applications no longer requires escalated procedures based on increased threat activity, saving critical IT administrative resources for other IT projects. Finally, Nevis facilitates StemCells' audit process by demonstrating granular access controls specifically tied to user profiles and mission-critical resources.

"Nevis' LAN security solution provides a scalable strategy for increasing the security surrounding our own Intellectual Property. Nevis' LANenforcer lets us define per port / per user access control policies for highly granular control and threat mitigation. We now maintain a highly secure LAN at a fraction of the cost."

--Director of IT, StemCells, Inc.