



Random Password Manager Provides Privileged Identity Management for Micronas

Securing a multinational enterprise with more than 20 offices, 330 servers, 2,000 workstations, and 1,800 employees is a challenging job. But Micronas, a semiconductor manufacturer for major automotive electronics companies, maintains the security of its IT infrastructure through an efficient, well-trained staff and the use of carefully-selected security solutions.

The Situation

Paul Blenderman, Manager of Windows Systems and Infrastructure at Micronas, needed a way to easily manage the local administrator password for every server in his enterprise. To be prepared for emergencies, Blenderman's team needed fast, reliable access to the local admin accounts on each system but did not want any of the credentials to be identical or to be stored in an insecure manner.

"Of course the most basic solution is to set each server with a random password and then leave it," Blenderman said. "But we wanted secure and immediate access to all our passwords to address problems we experienced in the past, like restoring computers with older versions of Windows. We were sometimes unable to log in with our domain accounts."

"And if you don't know the password for the local account, you have a serious problem," he emphasized.

In addition to lost productivity, a concern with inconsistent and ineffective password management – and especially unnecessary password reuse – is that if a single privileged account password is compromised, an unauthorized user can gain peer-level access throughout the enterprise.

The Solution

Blenderman briefly considered writing a script to perform password changes, but abandoned the idea after considering all of the difficulties. While scripts can handle basic password change tasks, they are time-intensive to create and maintain; they lack documentation, troubleshooting, and reporting features; and they pose the risk of one failure affecting multiple systems and users.

"A script or other manual alternatives would have been too much work on 330 servers," Blenderman said. "And you also need a

Profile: Micronas

Micronas is a semiconductor designer and manufacturer that operates throughout the world. The company is a leading supplier of cutting-edge IC and sensor system solutions for automotive electronics. www.micronas.com

The Situation

Micronas required a privileged account management solution to provide unique, automatically updated passwords for each system.

The Solution

Deployed Random Password Manager to automate all privileged account password management operations in the enterprise.

The Result

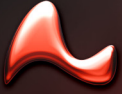
Micronas now has secure control over the privileged accounts in its network with convenient, audited access to the passwords.

way to store the passwords in a secure and encrypted manner. So a one-time solution would not have been a real solution. It becomes too much trouble to do things internally. We prefer to purchase products that can do everything you need and more."

With these considerations in mind, Blenderman began investigating privileged account password management solutions. To maximize his productivity he searched for a product that can regularly update every privileged account in the network, store the account credentials in an encrypted database, and allow delegated users to access the passwords on demand.

Lieberman Software's Random Password Manager met all of these criteria. This privileged identity management solution continuously randomizes local administrator and root account passwords on all systems in the enterprise, and enables temporary recovery of current passwords through an audited web interface. It ensures that each system maintains unique account credentials, preventing one compromised password from granting unrestricted access to other systems in the network and helping organizations meet the access control and auditing requirements of today's regulatory compliance mandates.

Random Password Manager secures passwords using AES-256 encryption in a SQL Server database with optional hardware-based encryption validated to FIPS 140-2 levels 2 and 3. Ran-



“We’re now happy with the security of our servers. We know that we can still access them if the domain trust ever fails, and Random Password Manager runs smoothly without manual intervention...”

Paul Blenderman | Manager of Windows Systems and Infrastructure, Micronas

dom Password Manager supports Windows NT/2000/XP/Server 2003/Vista/Server 2008, Linux and UNIX servers and workstations; SQL Server, MySQL, and Oracle databases; and Cisco and Juniper hardware devices.

Random Password Manager logs all password changes, verifications, and recoveries in a secure, relational database and can warn supervisory personnel of unusual activity through emails or an alerting system that’s integrated with Microsoft System Center Operations Manager, SNMP managers and other frameworks.

The Result

Blenderman now runs password randomization operations according to a schedule that he controls. The password change jobs for all of his servers complete rapidly, and are set up to run at off-peak hours.

“I scheduled the password updates as a monthly batch job,” he said. “The program sends an activity report by email.”

Blenderman also reports that Random Password Manager was simple to deploy and implement, and that he’s rarely required product support.

Blenderman said, “We’re now happy with the security of our servers. We know that we can still access them if the domain trust ever fails, and Random Password Manager runs smoothly without manual intervention. This product eliminates some of the worries of maintaining a secure and efficient infrastructure.”

About Lieberman Software Corporation

Lieberman Software provides privileged identity management and security management solutions to secure the cross-platform enterprise. By automating time-intensive administration tasks, Lieberman Software increases control over the IT infrastructure, reduces security vulnerabilities, improves productivity, minimizes business disruption, and ensures regulatory compliance.

Lieberman Software pioneered the privileged account security market, having developed its first product to address this need in 1999. The company is a managed Microsoft Gold Certified Partner headquartered in Los Angeles, CA with a support office in Austin, TX. For more information, see www.liebssoft.com.

