

**InfoExpress CyberGatekeeper:
Red Bull Customer Case Study**

Red Bull

High-Flying Beverage Company Soars With Secure Mobile Computing

From motocross freestylers in Madrid to paragliders leaping off cliffs in the Austrian Alps to high flying air races in Ireland, the name Red Bull has become synonymous with extreme sports enthusiasts across the globe. Since its initial distribution in Austria in 1987, the popularity of the Red Bull Energy Drink has surged to over \$1.2B in sales in 130 countries. One reason the business has soared is due to a solid IT infrastructure, and the move to secure mobile computing.

Challenge: Supporting a Large Mobile Computing Workforce

Red Bull North America maintains a large distributed and mobile sales and marketing workforce that requires corporate network access from just about everywhere imaginable. Being able to supply high-quality connectivity from home offices, hotels, customer sites, sporting events, and other locations, has been a top IT priority. It has also been one of the IT department's biggest challenges.

With so many mobile computing employees requiring remote access to the corporate network, the Red Bull IT team realized it was making itself more vulnerable to viruses and worms. The team took an aggressive, non-compromising approach to its network access control and security in order to minimize any interruptions to the network and the business due to a malicious code attack.

The IT staff realized that the remote access user laptops required more than just anti-virus. After researching endpoint security options, it was decided that the combination of VPNs, personal firewalls, and an endpoint enforcement capability would give the type of strong protection that they required.

But, unless the solutions were easy to deploy and manage and virtually transparent to the users, any productivity gains from the faster remote connections could be negated by a complicated security process that users would eventually reject.

Solution: InfoExpress Endpoint Security Suite

In 2002, Red Bull found the one vendor that could meet their stringent security and usability requirements - InfoExpress. After a short evaluation, Red Bull purchased the complete Endpoint Security Suite which CyberGatekeeper policy enforcement, CyberArmor endpoint personal firewall, and VTCP, a remote VPN.

Today, CyberGatekeeper complements existing endpoint security by inspecting all remote access devices and making sure each is compliant with Red Bull security policies. As part of an automated inspection process, CyberGatekeeper ensures that the personal firewall and anti-virus are installed, running, and patched with the latest policy and signature update files. Endpoints that fail to pass the policy compliance requirements are quarantined and remediated before they are allowed access to the network.

The IT staff has deemed CyberGatekeeper enforcement a real workhorse operating quietly and vigilantly in the background, while making sure every remote access to the network is free from infections and mis-configurations per the security policies set by Red Bull.

Red Bull is confident that they made the right investment with InfoExpress and the entire InfoExpress Endpoint Security Suite. It has been a win-win for everyone involved - the users, IT, and the business.

Customer Requirements

- 1) Boost remote and roaming employee productivity
- 2) Endpoint security transparent to mobile and distributed employees
- 3) Enforce the use of anti-virus and InfoExpress' CyberArmor endpoint firewall

Main Security Issues

- 1) Keep endpoints secure when connected over wired and wireless broadband services
- 2) Continuously monitor, detect, and remove non-compliant endpoint systems connected to the network
- 3) Block admission of potentially harmful devices from network access

Customer Benefits

- 1) Being able to take full advantage of the productivity gains from remote access and mobile computing
- 2) Improved network and endpoint up time with a minimum amount of administration
- 3) Reduces overall help desk costs by customizing the end user experience and enforcing application updates