SOLUTION BRIEF

BIOS-SHIELD™

JANUS TECHNOLOGIES

Elevate endpoint security and manageability with BIOS-based protection

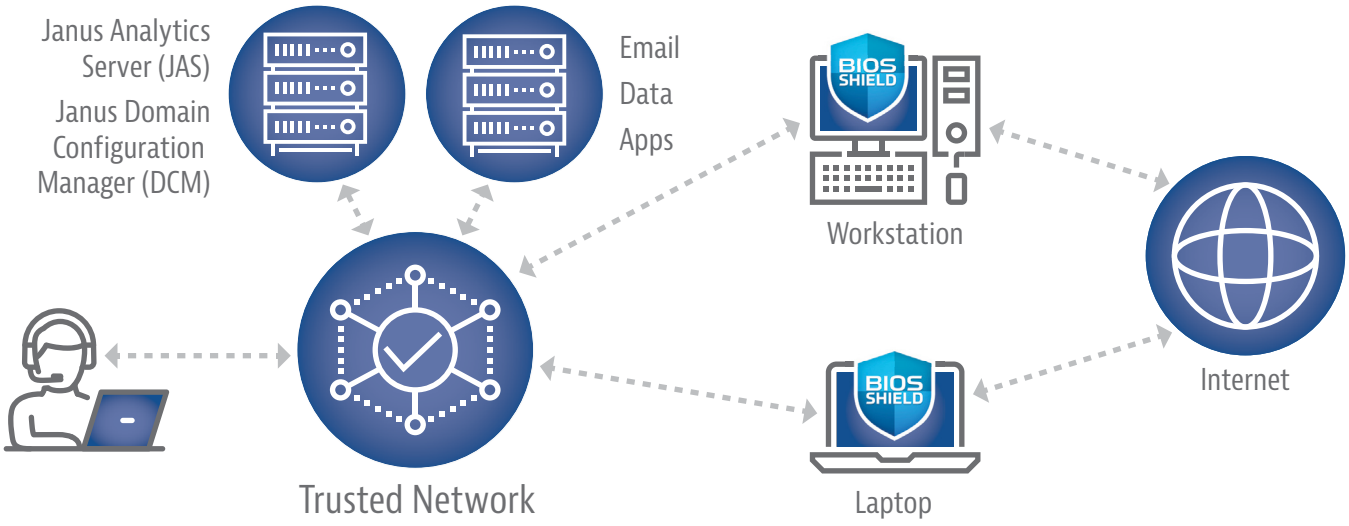
Add a new level of protection against today's threats

How secure is your organization's data? As thousands of recent cybersecurity attacks have proven, today's data is way too valuable—and too sensitive—to risk its security on a software-only solution. That's why we've taken an entirely different approach to helping organizations like yours protect themselves against ever-evolving threats.

While most of today's endpoint security solutions rely on operating system resources or add-on security apps designed to detect and block intrusions, **BIOS-SHIELD™ for Enterprise offers a tamper-proof solution** that locks down your endpoints and permits centralized management that increases administrative efficiency and helps reduce downtime.

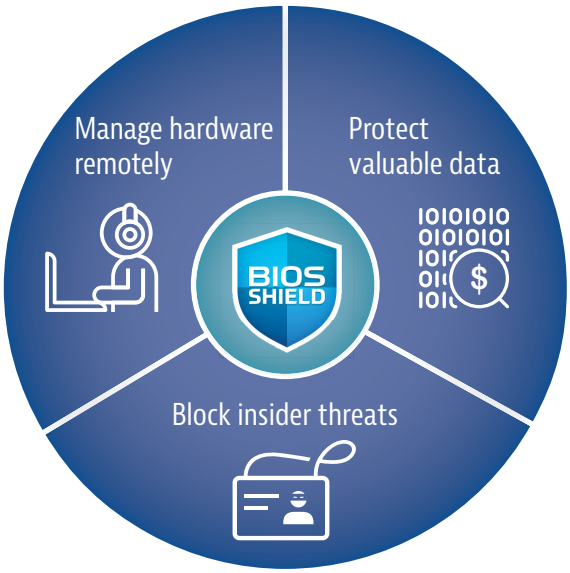
BIOS-SHIELD delivers BIOS-based technology to work along with your existing security measures. So it can deliver greater protection, providing additional security for workstations, PCs and laptops—along with real-time monitoring and analytics. It revolutionizes endpoint security by **handling security tasks in BIOS, instead of software.**

How BIOS-SHIELD for Enterprise works



Until now, endpoint security depended on operating system (OS) resources or third-party solutions—including firewalls, anti-virus, anti-malware or VPN protection. BIOS-SHIELD technology provides an additional layer of protection that sits between the PC's hardware and its operating system, where it can't be detected by hackers. This innovative technology works with existing security measures by handling added tasks in the BIOS, instead of software.

One solution addresses three critical challenges



BIOS-SHIELD is specially designed to help your organization defend against the dangers posed by insider threats, protect data from malware and manage hardware remotely.

Block insider threats

It's often assumed that most cyberattacks are launched by outside groups or individuals. But the truth is, **55 percent of cyberattacks are carried out by insiders**—either in an effort to malign the company or as the result of carelessness.[1] BIOS-SHIELD for Enterprise helps block insider threats to sensitive data by establishing peripheral security for USB-compatible devices and monitoring user activity. You can **set policies to define and control USB access rights**, preventing unauthorized USB access. What's more, you can defend against insider threats by **recording a user's display, mouse movements and keystrokes**—and then use that information as input for forensic analysis.

Protect valuable data

The threat of malware continues to grow—in terms of both frequency and sophistications. In fact, more than **4,000 ransomware attacks alone occur every day.**[2] BIOS-SHIELD can help protect against malware that's often "imported" when users inadvertently click on potentially harmful links or counterfeit URLs. Because we know that malware is most likely to find its way to your systems from a variety of well-known regions, BIOS-based **geofencing allows administrators to prevent internet access** to specific geographic areas. Should malware infect a BIOS-SHIELD-protected endpoint, administrators can easily—and reliably—**restore the device to its previous state.**

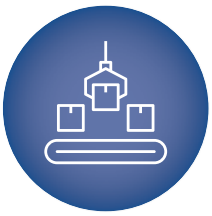
Manage hardware remotely

BIOS-SHIELD can **improve productivity and reduce downtime** by empowering administrators to remotely configure, manage, monitor, and control their organization's BIOS-SHIELD-protected endpoints. And BIOS-SHIELD will **automatically push out new BIOS-SHIELD profiles and updates.** What's more, administrators can schedule operations such as backups and activity monitoring to meet their organizations' specific needs. But should a problem arise, BIOS-SHIELD can help ensure that it doesn't become a catastrophe—by enabling administrators to **recover quickly if files are found to be compromised** or were accidentally deleted.

See how BIOS-SHIELD can help resolve multiple security issues

These three use cases illustrate the ways in which BIOS-SHIELD can help businesses in different industries by delivering greater protection against both malicious and unintended security incidents.

Making it easier for a manufacturer to block insider threats



Manufacturers have become prime targets for cyber criminals, who focus on stealing trade secrets and causing a physical disruption to operations. In fact, a manufacturer's most valuable asset is typically its intellectual property (IP), leaving the company vulnerable to insider threats—both unintentional and malicious—that could result in the loss or theft of this critical data.

BIOS-SHIELD allows manufacturers to **monitor and analyze user activity** and catch potential issues in real time, enabling quick restoration of production lines to help meet output schedules. So manufacturers can avoid the serious risks of intellectual property theft and malicious tampering by recording screen images, keystrokes and mouse movements to track user activity and support critical forensic discovery. And with USB peripheral security, administrators can set policies to **block unauthorized access** by defining and controlling USB access rights—to prevent an insider from downloading files to a USB drive.

Helping a video gaming company enhance security and protect their data from malware

In the action-packed world of online gaming, staying ahead of the game is a top concern for the companies that produce digital entertainment. That means giving designers and engineers the flexibility they need to freely access the internet and gain a creative advantage over the competition, at the risk of exposing their workstations and the network to malware.

With BIOS-SHIELD virtualization technology, a video gaming company can deploy workstations that have dual operating systems with dual, isolated network connectivity. One OS is configured to access the internet, and the other to access the company's internal network. With the "air gap" between the two network access points, any malware encountered on the internet has no way to invade the internal network—**enhancing the network's security** and **protecting company data from malware**—while giving developers the freedom they need to explore the internet. That air gap between corporate data and the public-facing internet also keeps corporate data from becoming publicly accessible. And geographic selection options let IT administrators prevent internet access to known high-risk regions. Once set, only administrators can disable those safeguards.

SOLUTION BRIEF

BIOS-SHIELD™

JANUS TECHNOLOGIES

Empowering a law firm to remotely manage hardware

These days it's not unusual for even a small law firm—or any other type of small business—to have at least a few remote employees. It's a good way to grow and develop new specialties. And while it can also be a highly effective and efficient way to get work done, it can pose problems for the IT administrator who needs to ensure that every employee is using a PC that's configured correctly.

BIOS-SHIELD makes it easy to **centralize endpoint management** by enabling its IT administrator to quickly configure, manage, monitor, and control PCs and laptops remotely. By automating the configuration of BIOS-SHIELD features and scheduling back-ups, an admin can save time and protect resources. At the same time, BIOS-SHIELD lets businesses **recover data quickly** to protect against either accidental or malicious data corruption. An admin that needs to reboot and restore a PC, whatever the reason, can do so remotely in minutes—not hours—taking the PC back to the state of its last backup.

See for yourself how BIOS-SHIELD for Enterprise can take your security to the next level

Learn more about how BIOS-SHIELD can help protect your data in a borderless world. Visit us online at www.janustech.com. We'll be happy to answer your questions or arrange for a demo.

Kifer Commerce Park
Sunnyvale, CA 94086

[1] IBM X-Force Threat Intelligence Index 2017.
[2] https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view