Protect your IT systems with next generation security

How trusted computing from IBM PureFlex System secures your systems against emerging threat profiles

IBM

Contents

No organization is immune

A multinational electronics manufacturer and supplier to some of the world's largest technology firms is hacked by a self-proclaimed group of Greyhats. Apparently related to a protest over working conditions, the hack results in the release of a massive amount of data including email logins, server logins and bank account credentials of large technology companies.

A global telecommunications company notices increased probing of their IT systems. Further investigation reveals that a foreign government is conducting daily probes of their IT infrastructure platform looking for a way to control their systems. As you read this, they are actively fighting to secure their systems against these foreign government attacks.

A data breach occurs at a large payment processing company but was limited to only a "handful of servers." Even with such a seemingly small breach, the company releases a statement saying around 1.5 million credit and debit card numbers from all the major credit card companies were compromised.

What these three real-life examples have in common is that the perpetrators attacked these companies through their IT systems. That is because these systems now house your most critical information. Your IT systems

represent your organization's communication backbone and are the conduit through which your staff shares ideas with each other, communicates with your customers and accesses your strategic organizational knowledge.

If successful, such attacks on your systems can expose your organizational, employee and customer financial and personal data. Or they can detrimentally impact your company's competitive advantage or even jeopardize national security. While the financial impact of these attacks is nearly impossible to measure accurately, we do know that over 400 million new variants of malware were created in 2011.[1]

Therefore, it is essential that you actively secure your IT infrastructure from increasingly bolder, more invasive and less detectable threats that are immune to traditional antivirus and antimalware solutions. This requires a more comprehensive approach to IT security.

Your systems are targeted

Long before the Internet was developed, individuals were trying to gain unapproved access to IT systems and the critical data they contain. While technology has changed and advanced over the decades, human nature has not. The difference is today's systems contain substantially more—and more valuable—information than they did in years past. For example, today's corporate IT infrastructure houses:

a) Corporate financial details and projections.
b) Executive and legal communications including email and voicemail.
c) Employee records including tax ID numbers and bank account data.
d) Customer financial and personal details including credit card information.
e) Business trade secrets and strategic plans.
f) Money in the form of digitized account balances.

Even more, your IT infrastructure may contain geopolitically useful information without you even knowing it. That's because you may not know what kind of data a particular political or military organization finds valuable. And this puts you at the worst kind of risk—an unknown risk.

Attacking for financial gain

To prove how regularly hackers target businesses, you need look no further than today's headlines. Recently, a major credit card transaction processor reported a breach where hackers were able to obtain personal and financial information about customer accounts. One bank executive estimated between 1,000,000 and 3,000,000 accounts were affected. And this was the second breach this company had experienced in the previous 12 months.

Not only did this impact the individual customer accounts, but it damaged the reputation of the company where the breach occurred. And according to the New York Times, "Security consultants say the sophistication of these attacks is increasing." So whether your systems house the financial and personal details of customers, or confidential corporate financial information, hackers have either already targeted your systems or likely will. In fact, the Computer Security Institute's 2010/2011 Computer Crime and Security Survey found that nearly 50 percent of respondents had experienced at least one IT security incident during the survey year.[2]

Attacking for nonfinancial gain

While financial gain can be an obvious reason for hacker attacks, it is by far not the only incentive. Since the last century, denial-of-service (DoS) attacks that are intended to cripple systems and take them offline have devastated organizations around the globe, no matter how secure their systems might

have appeared. The National Security Administration (NSA) has identified that cyber attacks on a nation's economy can be just as devastating as attacks on military or security assets. Therefore, large online companies, major telecommunication providers, global news organizations and even highly secure government agencies have all been targeted. And the hackers behind these DoS attacks are motivated almost exclusively by nonmonetary gains. Unfortunately, when your organization depends on an information network, a DoS attack can quickly cripple your ability to function at even a rudimentary level.

Beyond the disruption or revenge justifications typically behind DoS attacks, there is another nonfinancial reason hackers can seek to penetrate your system—espionage. This would seem obvious to a company involved in military or security-based activities. However, just because your business does not serve the military or security markets does not mean that you are not vulnerable. Your business may be targeted by corporate spies looking for competitive advantage data on servers, such as designs for next generation products, research results that form the foundation for patents, or even strategic planning data such as acquisition or new target markets.

Or your company may supply component pieces installed in larger systems, and corporate spies could target your system seeking vulnerabilities that would allow them to attack those larger systems. For example, Symantec reported on the Nitro attacks in summer 2011 where 48 companies spread over eight countries, including multiple Fortune 100 companies, were targeted.[3] These companies were involved in the development of materials for military vehicles or the ancillary efforts of developing the manufacturing infrastructure for the chemical and advanced materials industry.

Where your systems are vulnerable

Obviously there are a wide variety of reasons why hackers would target your IT infrastructure. Once you realize your business is a legitimate target for somebody or some organization, the next step is to identify—and then block—the access points those hackers would use to compromise your system. Modern system security architecture relies on a "defense in depth" approach but hackers are now much more skilled at discovering unsecured access points and exploiting them wherever they may exist. To secure your IT infrastructure from would-be attackers, you have to protect all of these potential access points—access points that continue to grow in number.

Traditional attack profiles

Hackers have always exploited a system's biggest shortcoming, one that is virtually impossible to secure—the human user. The use of a single password and user ID across all of a computer user's system interactions, or the use of trivial user IDs and passwords, are well-known exploits that can provide weakly defended backdoors into higher security components. But structured security profiles along with physical site and machine policies can generally mitigate much of this risk.

So hackers became smarter and soon the computer user was simply the entry point to controlling programs running on the computer. Often referred to as the application level, these attack profiles include techniques such as phishing, Trojan horses and backdoors. Although software version upgrades often patch known application-level vulnerabilities, weaknesses in existing software are continually being discovered and new applications are constantly being introduced. Fortunately, the application-level attack profile is so well known that system exposure risk is generally sufficiently managed through appropriate user security policies combined with modern antivirus and antimalware software that are then coupled with hardware and software firewalls.

As security software and user security policies began plugging the application-level vulnerabilities, hackers set their sights on the next deeper level—the operating system (OS) and hypervisor layers. If a hacker can compromise the OS or the hypervisor layers, they can avoid detection by most security software running at the application layer, they will have greater access to the system and they will be able to remotely control the system. These attack profiles include techniques such as spyware, malware and rootkits where the hackers cloak their software to prevent it from being discovered, then use their cloaked software to intercept calls to the OS. While more sophisticated than application level attacks, most robust system security plans address OS or hypervisor level exposure and reduce system risks.

Emerging attack profiles

As IT security professionals developed software and security policies that protected high value IT infrastructure, the traditional attack profiles were no longer as effective as they once were. So attacks evolved to a new level, going even deeper than the OS and hypervisor layers—to system levels that have traditionally been assumed to be secure. That means application, OS and hypervisor breaches are no longer the biggest threats to your system. Rather, attacks on the firmware and platform-infrastructure levels such as bootkits, as well as attacks by system management controllers, are the most dangerous threats facing you in the future.

This is possible because subcomponents are now manufactured worldwide making it difficult to monitor for security. So system management and boot firmware Core Root of Trust for Measurement (CRTM) code elements are established to serve that security-monitoring function. But if a CRTM can be corrupted, then an attacker can insert any desired code deep in the system. This allows a vendor, disgruntled employee or even a foreign entity to implant malware, viruses or the like into system subcomponents, making detection difficult to impossible without specialized methods.

There is a simple reason this type of supply chain attack is appealing—if hackers can infiltrate the system at these levels, they will have full control over the system and the system owner likely will not even know the system has been compromised. That is because often these attacks cannot be detected by current antivirus and antimalware solutions.

Because of these emerging attack profiles, governments are responding with increased security requirements for their systems, their service providers and their vendors. And many of those service providers and vendors are in turn passing those security requirements through to their partners, vendors and contractors. As these new standards cascade through the IT industry, IT professionals must recognize and react to the impacts those standards will make on their organizations.

The overall view of system security

Clearly, those who seek unauthorized access to your system have grown more advanced in recent years. As more and more mission-critical information resides on your IT systems, the stakes in this cat and mouse game continue to rise. And as your key business data begins migrating to the cloud, remember the available-anywhere benefits of cloud computing also provide an additional access point through which your system security could be compromised. This is particularly important since cloud computing requires that you trust datacenters and administrators you typically have little knowledge of. So it is important to know that the systems your cloud computing are built on have superior hardware, firmware and software security as well as strong security policy enforcement. That security is even more vital to your business if other businesses rely on your private cloud—and depend on its security.

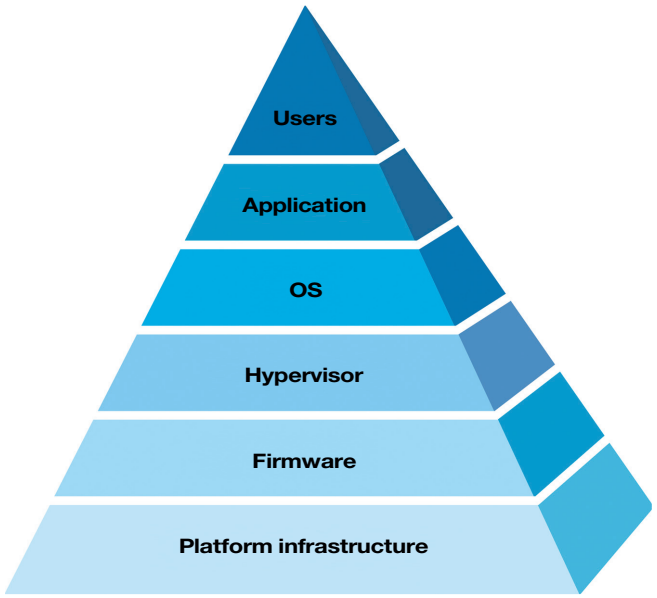

Figure 1: A compromised layer provides access to every layer above the compromised layer

As the graphic shows, the platform infrastructure and firmware levels are the foundation upon which your system security rests. The hypervisor, OS, application and user levels depend on the security of the platform infrastructure and firmware—the system boot hardware and Basic Input/Output System (BIOS) firmware as well as the system management boot hardware and firmware such as baseboard management controllers (BMC). So without securing the complex and sophisticated base of this system pyramid, a hacker can use the platform infrastructure and firmware as access points to your system. And once they control the base of the system pyramid, they control your entire system—usually without you even knowing they have that control.

The solution is to increase platform infrastructure and firmware-level security by creating a Trusted Computing Base (TCB). That is because when your system's platform infrastructure and firmware is secure, the rest of the system security structure can be more easily supported on that solid foundation.

How IBM can secure your system's foundation

Using a TCB secures your system's hardware, and thus the foundation of your entire IT infrastructure. The IBM TCB implementation is evolutionary and addresses system hardware vulnerabilities that fall into two broad classifications: Systems Management and Boot Firmware. Since both feed into the Systems Security layer which houses the hypervisor and OS, the IBM TCB can prevent attacks at the system hardware and firmware level.

As the following diagram shows, there are two major attack surface categories that must be protected: Systems Management and Boot Firmware. Within each category, there are multiple attack surfaces that can be exploited.

1.Systems Management
- a) Intra chassis communication links
- b) Extra chassis communication links
- c) Scripting and command line interface (CLI) application interfaces
- d) Initial/default setup environment
- e) Security object provisioning
- f) System management—user ID and password control
- g) System management—controller integrity

2. Boot Firmware
- a)Unified extensible firmware interface (UEFI) code updates
- b)UEFI attack by BMC
- c)Intel Trusted Execution Technology (TXT) support

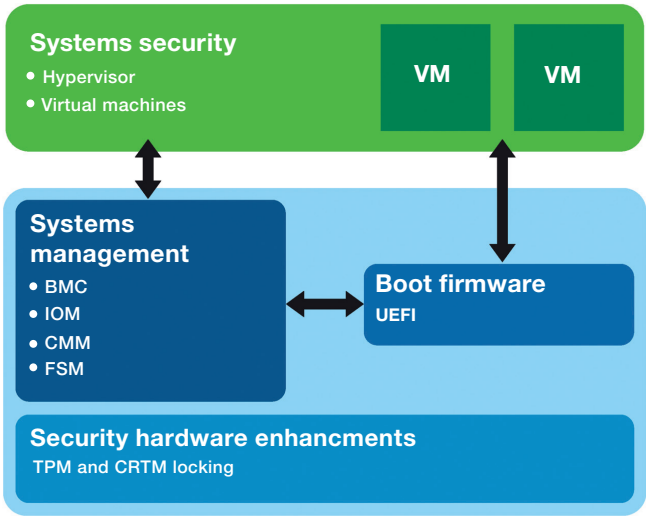

Figure 2: Broad classifications of infrastructure and firmware attack surfaces

Each of these 10 attack surfaces represents an entry point through which a hacker can compromise your platform infrastructure and controller, and ultimately your system. That's why the IBM® PureFlex™ System was designed and built to systematically address each of these attack surfaces.

1.a. Intrachassis communication links

These are the communication links between the different chassis systems management components used to provision, configure and control the system. Very privileged operations are performed over these links and keys and other sensitive data are shared over these links.

The threat. An attacker can monitor these links and collect protected credential information such as user IDs, passwords and keys from the data stream. Using this information, the attacker can then pose as a legitimate user, login and attack the storage, computational and networking nodes and inter-object messages (IOM) in the system.

The legacy solution. These links were not traditionally encrypted. Security depended on the physical security of the chassis such as a physical lock on the system or securing the system within a locked room.

The PureFlex System solution and innovation. Security critical intrachassis communication links are now encrypted. This is entirely new functionality.

1.b. Extrachassis communication links

These are the communication links from the chassis systems management components to administrators allowing them to directly connect to systems management microcontrollers.

The threat. These links allow customers direct access to computational, storage and networking nodes. If these links are not secure, attackers can monitor the traffic on these insecure links and extract legitimate credential information. Just as with the intrachassis communication links, the attacker can then pose as a legitimate user and login to, penetrate and corrupt the system.

The legacy solution. Previously, customers could not directly connect to—nor communicate with to secure—system management microcontrollers on chassis IT elements.

The PureFlex System solution and innovation. Customers can now directly connect to systems management controllers on nodes. Further, security policy and provisioning in the chassis allow these links to be centrally set up so they can be safely managed with minimal administrator intervention required.

1.c. Scripting and CLI application interfaces

These are unsecure interfaces such as telnet where a CLI can be accessed on systems management components. This provides an attacker an open interface to run scripts, search for and open password files, escalate privileges and more.

The threat. Very powerful operations can be performed at the CLI which can expose an entire system. For example, an attacker could execute programs from the command line to edit the system's firewall settings or open a known weakness. That would in effect leave a backdoor open through which the attacker could later re-enter the system and then corrupt the system or extract sensitive data.

The legacy solution. There were no systemic measures available that could prevent these types of operations from being performed.

The PureFlex System solution and innovation. With high security mode set in the chassis management module (CMM), CLIs can only be executed over secure links and the logins used are centrally controlled by lightweight directory access protocol (LDAP). This is entirely new functionality.

1.d. Initial and default setup environment

During out of the box setup, your security policy is not yet in place and manufacturing default user IDs and passwords are well known. Further, this same situation occurs should the component need to be reset to manufacturing defaults to recover from a failure after deployment.

The threat. Because manufacturing default user IDs and passwords are well known, the system is vulnerable until setup or reset is complete. In addition, components within and beyond the information technology element chassis are not known to each other—in other words, they are not cross-certified.

The legacy solution. Manufacturing default user IDs and passwords were allowed to exist after initial setup or reset was complete. Components within the chassis were not allowed to communicate outside of the chassis so cross-certification was not an issue.

The PureFlex System solution and innovation. Manufacturing default user IDs and passwords must be changed on the first login to a chassis component and direct administrator communications with chassis components are now allowed over secure communication links. In high-security mode, this protects the chassis from exposure once setup or reset is complete and eliminates well-known system backdoors.

1.e. Security object provisioning

Security object provisioning includes those security functions necessary to define and start a system or component, or update the system or component due to changing system status. This includes the base user IDs and passwords to start core system functions, keys and their associated certificates to establish secure links as well as security policies required by nodes to establish connections.

The threat. Keys, certificates and other credentialing that are essential to security have previously been provided in an ad hoc fashion. Unless these objects are provisioned by the system or configured by people with an in-depth system understanding, it can be difficult to know if this has been done correctly and enormous security holes may exist.

The legacy solution. There was no chassis security policy or security provisioning of IT elements and switches. All security objects needed by the IT elements and switches had to be handled through scripts or through manual intervention by administrators.

The PureFlex System solution and innovation. The customer sets the security policy, and then certificates and keys are automatically provisioned to the nodes and IOMs. This means rather than using highly-skilled personnel to manually provision the system security functions and provide ongoing security management monitoring, the PureFlex System does this automatically thereby dramatically reducing system administration.

1.f. System management—user ID and password control

User IDs and passwords across the entire systems management level are like the key system at a large hotel. That means there are a few master keys which will access any component and numerous local user IDs and passwords that allow access only to specific system management components.

The threat. The local user IDs and passwords are often managed in an ad hoc fashion and not centrally controlled. This creates the opportunity for an attacker to introduce a rogue user ID, penetrating the system by cracking well-know local user IDs and passwords, weak passwords and the like.

The legacy solution. Since these controllers only run Linux, these systems have historically possessed only standard Linux security—no trusted computing and no trusted secure system management controller boot.

The PureFlex System solution and innovation. Much as a large hotel has a centralized system to manage keys and ensure security for each room, LDAP can now be used for centralized user ID and password control. Therefore, no local IDs can be used that may jeopardize the system security (for example read-only simple network management protocol is allowed). Because password strength is now controlled by the new chassis security policy, executing this level of security is no longer a serious administrative burden.

1.g. System management—controller integrity

To remain free of threatening software, the systems management controllers must be able to boot to a secure state with a hardened attack surface.

The threat. Viruses, malware and rootkits can enter the computational, storage, and network nodes through the systems management controllers. Because these controllers form the foundation for the entire system, that provides an unsecured path to attacking the system (OS) itself.

The legacy solution. Since these controllers only run Linux, these systems have historically possessed only standard Linux security—no trusted computing and no trusted secure system management controller boot.

The PureFlex System solution and innovation. The PureFlex System uses a Trusted Platform Module (TPM) based computing model with embedded Linux that allows for future recurring security checks. It provides for the trusted launch of a signed Linux OS image to ensure code is correct and provides security policy enforcement to ensure that threats cannot enter the system. This lays the foundation to actively check the runtime security state of system management controllers.

2.a. UEFI code updates

The UEFI code updates are the ongoing software updates to the currently installed UEFI that fix known code problems or provide additional functionality. Because it contains the entire UEFI BIOS image for the system, a compromised UEFI code update can introduce a large security breach into the system.

The threat. Rootkits and other malware that can be inserted into "impostor" code updates can take control of the system at a very deep level and be extraordinarily difficult to detect. Therefore, the CRTM code element runs in the UEFI BIOS before anything else, scanning subsequent code for security breaches. Because the CRTM and the UEFI have different update requirements, for maximum security they should be separately protected and the UEFI should self-load.

The legacy solution. Historically, the only security that existed for UEFI code updates was UEFI CRTM code signing, meaning the UEFI CRTM was the only element that included a digital signature to prove authenticity and verify tampering has not occurred.

The PureFlex solution and innovation. Code signing is now implemented separately for the entire UEFI code update as well as the embedded CRTM. In addition, the code update packages for the BMC and CMM are also signed. This has expanded UEFI code signing from just the CRTM to the CRTM plus the entire separate UEFI code update—a key component in creating the system TCB.

2.b. UEFI attack by BMC

BMCs such as the IBM integrated management controller (IMMv2) have enormous control over the system and the UEFI. Because of this control, they are part of the TCB and must be hardened.

The threat. A BMC can update UEFI code, update hardware firmware such as field programmable gate arrays (FPGA) and interrogate processors and memory among other actions. Therefore, a BMC has the ability to implant threats in the UEFI, implant threats in the systems software stack and impose other security risks.

The legacy solution. Since these controllers only run Linux, historically, the only security available to this attack surface was the generic Linux security features for BMCs.

The PureFlex System solution and innovation. The PureFlex System provides separate IMMv2 TPM and CRTM which first establishes a static root of trust measurement (SRTM) for the BMC as well as signed Uboot and Linux kernel images. This ensures IMMv2 boots to a correct and trusted state.

In addition, there are now signed code updates for systems management (IMMv2, CMM, and so on) and the hardened IMMv2 attack surface greatly enhances the ability of these systems management components to stop new threats from entering. Together, this provides three key security improvements for these system management components: 1) trusted secure boot, 2) trusted CRTM and TPMs, and 3) signed code updates.

2.c. Intel TXT support

Intel TXT is a hardware security solution that protects IT infrastructures against software-based attacks by validating the behavior of key components within a server or PC at startup. Because Intel TXT is rooted in the processor itself, system support for this function can improve security.

The threat. Large UEFI code images with a great deal of third party code are difficult to verify, which exposes the entire system. Keeping the TCB of the UEFI as small as possible so its security properties can be verified, as well as dynamically launching a systems root of trust such as Intel TXT, greatly reduces UEFI threats.

The legacy solution. Until now, there have been no dynamic launch capabilities.

The PureFlex solution and innovation. Intel TXT support is now included, which allows software that supports it to implement Intel TXT. This enables current Intel TXT functionality to dynamically validate platform components in the boot and launch environment. It also allows future enhancements of the dynamically launched root of trust as well as reduced TCB size and enhanced UEFI security during the boot process.

Increased security without increased administration

The PureFlex System provides a giant leap forward for system security. But as any business knows, your IT systems are only as secure as the weakest link. That means if the increased security capabilities force an escalation of system administration requirements, but the organizational constraints dictate static staffing levels, many of those security gains will not be realized.

Fortunately, the PureFlex System not only automates the new security enhancements, but also much of the previous security administration—functionalities that if not automated would require ongoing intervention by highly-skilled, dedicated staff to manually establish, monitor and manage. What this means is that with a PureFlex System you get increased security of your systems while maintaining—or even reducing—system administration requirements. So you can pursue a more hardened system without worrying about adverse impacts to current staff loads or staffing requirements and their associated costs. Or even the business costs of isolating a potentially infected system from the remainder of your information network.

The IBM PureFlex System advantage

The IT environment is an increasingly dangerous place. Hackers have uncovered an entirely new way to circumvent the security of current systems. They are now attacking system layers that were previously assumed secure. And their attempts to break into systems through these attack surfaces continue to grow.

The value of a PureFlex System is crystal clear. Secure your system now before these emerging threats become even more common. Establish hardware and firmware level security for you organization as well as your customers. And maintain or even reduce the staff time required to administer your systems in the process when compared to manually implementing these TCB level security features.

The following table shows key security features of the PureFlex System and why you should demand those capabilities from your computing solution. As you can see, the PureFlex System has been designed to prevent you from becoming the next hacker headline.

IBM PureFlex System Feature	Protection/Benefit Delivered
Verified boot of IMMv2 and CMM	Ensures systems management microcontrollers boot to a correct and trusted state
Trusted computing features for IMMv2 and CMM (requires TPM modules dedicated to CMM and IMMv2)	Enhances the ability of these systems management components to detect new threats, store/protect key hierarchies and demonstrate their security properties to other components
Centralized enforced platform management user ID control	Ensures consistent, cross-system ID and password strength, reducing threat of easy or well known userid/password security backdoors
Trusted Platform Module (TPM) for System Management Controllers	Provides a cryptographically measured launch of the signed Linux OS image and delivers ability to verify the OS code after install
Secure intra-chassis communication links	Encrypts links within the chassis to prevent unauthorized collection of protected credential information such as user IDs, passwords and keys from the data stream
Security object provisioning	Reduces the time, effort and skillset required to set certificates and keys which are automatically provisioned, to the nodes and IOMs
Security established out of the box and security holes eliminated from remaining past the out of the box setup process	Protects the chassis from exposure once setup or reset is complete and eliminates well-known system backdoors
Signed BIOS updates, signed update of key systems management components	Prohibits impostor update code from gaining access to the BIOS and key systems management components

Why IBM?

The platform infrastructure and firmware levels of your IT systems are an extraordinarily interconnected environment. That complexity alone makes it difficult to secure one potential access point without inadvertently creating new system weaknesses. Because this is a never-ending battle, you need a company capable of applying significant staff and financial resources to securing this complex environment over the entire life cycle of your IT systems.

For over 60 years, IBM has been applying global staff and financial resources to successfully solve business computing challenges. IBM continues to invest heavily in research and customer deployments with the goal of pushing the technological edge even further. The result is industry leadership in Smarter Computing technologies and expert integrated systems including the PureFlex System.

IBM is committed to continuing to make those investments in technology and securing that technology because our customers and internal teams depend on safe, secure technology. So the IBM research teams identify not just today's security threats, but also the security threats of tomorrow. With that knowledge, these talented technical experts fortify IBM hardware, software and cloud platforms against those threats. That's why IBM can provide the TCB that protects your systems against current and emerging threats. All backed by the experience required to tailor a solution for your unique needs.

For more information

To learn more about the IBM PureFlex System, please contact your IBM marketing representative or IBM Business Partner, or visit the following website: **ibm.com**/pureflex

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: **ibm.com**/financing

IBM Corporation
Systems and Technology Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2012

[1] Paul Wood, editor, Internet Security Threat Report, 2011 Trends, Volume 12 (Symantec, April 2012), 45.

[2] Robert Richardson, 2010/2011 *Computer Crime and Security Survey* (Computer Security Institute), 2.

[3] Eric Chien and Gavin O'Gorman, *The Nitro Attacks: Stealing Secrets from the Chemical Industry*. Symantec Security Response, 2011.

Please Recycle

WAW12355-USEN-00