IDC TECHNOLOGY SPOTLIGHT

Datacenter Security: Ensuring Protection at the Server Level

September 2014

Adapted from *Worldwide Security 2013 Top 10 Predictions, by Christian A. Christiansen*, John Grady, et. al., IDC #239424

Sponsored by IBM

IDC believes that security should be baked into datacenter servers from the start, not smeared on later as an afterthought. This means that security is embedded in the core hardware and firmware below the operating system and applications. These baked-in features enhance security utilities embedded into operating systems, browsers, applications, networking, and management products. All these embedded security capabilities should integrate with security products and services for holistic protection. These connected security layers can substantially improve server security in datacenters by improving threat prevention, detection and remediation.

This Technology Spotlight explores the trends affecting datacenter server security, including trends influenced by what IDC calls the 3rd Platform of compute, and discusses the role that System x plays in the growing market for datacenter security with its new System x M5 servers — the x3650 M5, x3550 M5, NeXtScale nx360 M5, NeXtScale System with Water Cool Technology, and Flex System x240 M5 Compute Node, which all contain the latest Intel Xeon E5-2600 v3 series processors (with up to 18 cores per processor).

Introduction

IDC predicts that security hardware and software spending in the datacenter will grow faster than the overall security market. Security will grow at 7.6% from just over $28 billion in 2011 to nearly $41 billion in 2016. In the datacenter, security will grow from nearly $11 billion to more than $16.5 billion over the same period, a rate of 9.3%.

Datacenter security requirements focus on protection (data and applications access), reliability, availability, and scalability. As datacenter architectures have changed with the growth of public and private clouds, security requirements for new deployment models have evolved as well. Security solutions must easily scale alongside the platforms they are protecting so that organizations benefit from virtualization and consolidation in a secure fashion. While virtualization has increased dramatically, most environments are still a blend of physical and virtual. Consequently, consistent policy management across both types of environments is a key requirement for security solutions in the datacenter.

Embedded security as a mechanism for "secure by default" becomes even more important in these dynamic and elastic environments. When new resources come online, embedded security functions ensure immediate protection.

Targeted malware and attacks are increasing at an incredible rate, and more advanced technologies that tie into advanced intelligence feeds, behavioral analysis, contextual awareness, and other components are necessary. If new datacenter objects are not immediately protected, a window of vulnerability is opened for automated attacks. Moreover, manual processes bog down the entire security process because the volume of alerts sometimes causes IT to miss anomalous behaviur that

has not been seen before. This can create ongoing vulnerability issues. Embedded security functions automate protection so datacenters can focus on preventing advanced targeted attacks by reducing gaps in defenses. Improving protection reduces threats, which increases datacenter reliability and availability.

Benefits of Platform and Firmware Security

Security issues often negatively impact efficiency and reliability. Many organizations mention that attacks and breaches can disrupt datacenter operations for hours, days, or even weeks. Embedding security at the hardware and firmware levels improves attack protections and detection. This generates the following business benefits:

- Improves code testing, ensures continuous validation, and confirms updates — all of which establish and maintain chain of trust for upper layer software and applications
- Prevents unauthorized changes that interrupt operations by signing code, controlling administrative changes, verifying all changes and updates
- Reduces audit and compliance problems with trusted administrative privileges, full disk encryption, key management, secure firmware, and rigorous security testing
- Prevents difficult to detect boot level (rootkit) attacks with trusted platform management (TPM) and prevention of unauthorized firmware updates
- Facilitates secure firmware rollback which prevents unauthorized firmware updates to previous authentic versions unless they are performed by a secure mechanism or by an authorized user so as to avoid opening previously closed vulnerabilities. Enables security by default, which provides additional protection, closes "vulnerability windows" opened by manual security processes, and improves datacenter reliability.

Market Trends

As the threat ecosystem is now populated by highly sophisticated criminals and professional espionage agencies (both private and public), attacks are focused on server data because such data is the new currency.

Attackers now use a process that comprises many of the following tasks:

- Detailed research on targets
- Careful development of reconnaissance strategies
- Thorough mapping of all technical and organizational vulnerabilities
- Testing exploits on other companies that are not targets
- Stealthy attacks using coordinated tactics designed to confuse and mislead defenders
- Concealment of all signs of compromise so attackers can remain resident for months or years without detection
- Compromise of associated systems (customers, partners, suppliers, contractors, consultants, etc.)

Another technique is "exfiltration." Like "infiltration," when attackers gain entrance, exfiltration is the concealed exit that includes the transfer of targeted data without leaving evidence of which systems, applications, and data were/are compromised. This process, often referred to as a "kill chain," may or

may not rely on custom malware or "zero-day" attacks. (These attacks use unknown vulnerabilities that have not been publicly reported, and patches have not been developed.) In fact, IDC believes that zero-day malware is used in less than 10% of all attacks. Most attacks exploit known vulnerabilities.

Attackers' successes are all too common. In the past year, hundreds of millions of accounts have been breached. Victims include prominent retailers, restaurant chains, online auctions and social networks. These attacks are board-level priorities because they expose senior management to customer distrust, widespread public damnation, class action suits, congressional hearings and regulatory costs. In the last two years, these breaches have gone from a nuisance to a severe business disruption. Moreover, IDC believes that attackers' skills are growing far more sophisticated than IT's ability to defend.

Considering System x Servers

System x platforms are designed with security built-in on three levels. At the hardware and processor level, all the latest x86 industry security standards have been incorporated, including Intel security processor features for protection against malware and faster encryption. At this level System x also incorporates the latest technology from the Trusted Computing Group. On top of these industry standards exists a set of System x platform-specific innovations — together called System x Trusted Platform Assurance. These are features and practices that include development, build, test, and field deployment processes. Now, with the new System x M5, a third layer of security enhancements has been introduced that includes optional self-encrypting drives with IBM Security Key Lifecycle Management for simplified protection and management of enterprise data-at-rest, support for TPM 2.0, and a secure firmware rollback feature.

The current System x platform includes such models as the x3500 M4 (tower, 5u rack mountable), the x3550 M4 (rack, 1u), the x3650 M4 (rack, 2u), the NeXtScale nx360 (rack, 1/2u) — all of which will now see an M5 generation with this recent launch.

It is worth noting some of the latest x86 security standards that System x — as well as competing x86-based servers — supports. The industry has come a long way in providing a solid first line of defense for end customers with these standards. They help protect compute nodes and system management infrastructure, provide faster encryption, and protect against malware and privilege escalation attacks.

System x incorporates these standards and in some cases extends them. For example, a TPM (Trusted Platform Module) for secure storage of server credentials in a dedicated microprocessor is a standard x86 security feature. System x, however, has gone a step further and incorporates two dedicated TPMs — one for the management and one for the system — unlike competing servers. Other standards that System x supports include encryption support at the CPU level and UEFI/BIOS (Unified Extensible Firmware Interface /Basic Input-Output System) protections to prevent unauthorized code from being loaded when the server boots and before the operating system is loaded. System x servers also check the digital signature of all firmware every time before firmware executes in order to protect against rogue malware attacks.

While the industry standard security features have improved x86 security greatly, they have not prevented all security breaches, and System x therefore has a second layer of protection consisting of features and practices, as previously noted. System x Trusted Platform Assurance ensures that all firmware is securely built, digitally signed, and verified prior to installation and execution at a customer site. All System x servers undergo a secure development process and are subject to a stringent and ongoing validation process with controlled updates. This cycle of secure processes establishes a “chain of trust” that higher layers in the system such as the applications can take advantage of. To convey this concept in laymen’s terms, consider that just as a chain is only as

strong as a weakest link, a system is only as secure as its most vulnerable layer. In order for a layer to be reliable and secure, it must trust the layers beneath it. So by delivering secure hardware and firmware, System x servers establish a secure platform for upper layer software and workloads.

It is easy to underestimate what is required to develop such a chain of trust through firmware and hardware integrity. It is therefore useful to dive a bit deeper into these practices and features. System x firmware development starts with architects defining and approving all designs. A review board then determines whether the designs comply with System x requirements and industry standards. Code development is subject to inspections, and all code is kept in code retention servers; any changes to the code are tracked and audited. To convert the source code into object code, the source code is sent to protected build servers. The object code is then sent to secure signing servers used exclusively for providing digital signature in a highly protected physical environment.

Challenges

IDC defines the 3rd Platform as the confluence of a dramatic growth in cloud computing, mobility (and BYOD), Internet of Things, social networking and Big Data. These major trends are changing how organizations leverage and benefit from data but they have also opened up new fronts in terms of security attacks and predictive, proactive, and reactive responses required. However, cloud, mobile, social, and Big Data security measures can only be as strong as the hardware and firmware on top of which they are built.

The 3rd Platform offers huge opportunities, but at the same time causes increased security threats, and therefore drives greater security needs. Security discussions almost always focus on hackers, crackers, criminals, spies, and other negative elements. However, senior management, business unit leaders and IT are more interested in solutions that will provide positive benefits (increase customer satisfaction, hasten time to revenue for new products and services, streamline supply chains, and improve corporate margins).

The challenge is to translate server security capabilities into business benefits by reducing the attack surface, building a chain of trust that has demonstrable customer and operational benefits, and using security best practices to prevent server misconfiguration.

Conclusion

The need for information technology to address IDC's four pillars of the 3rd Platform (mobility, cloud, social business, and analytics) offers opportunities for security product growth. Attackers, who are organized, continue to target enterprises, government entities, and individuals. These attackers are targeting the $12 trillion ecommerce business. In addition to direct transactions, businesses use the Web and messaging systems for marketing, customer service, and information sharing. IT is an indispensable component of the business process, and IT security also remains at the top of the spending list.

Many factors contribute to the continued growth in IT security. These factors include the difficult threat environment. The volume of threats targeting enterprises continues to grow. The speed with which threats are increasing (millions of malware variations) is making it increasingly difficult for security solutions to keep up. Malware that targets mobile devices is growing considerably, too. To defeat advanced malware, hardware must include embedded security at the platform layer. With hardware and firmware security, organizations can prevent malware and denial of service attacks at these layers — a critical capability given that attacks at these layers are increasing. Also critical is security that is both automated and scalable. If IBM can address the challenges in this paper, IDC believes that its System x servers — which deliver embedded, built-in security at the hardware and firmware layers that establish a secure foundation for upper layer applications and workloads — have a significant opportunity for success.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com