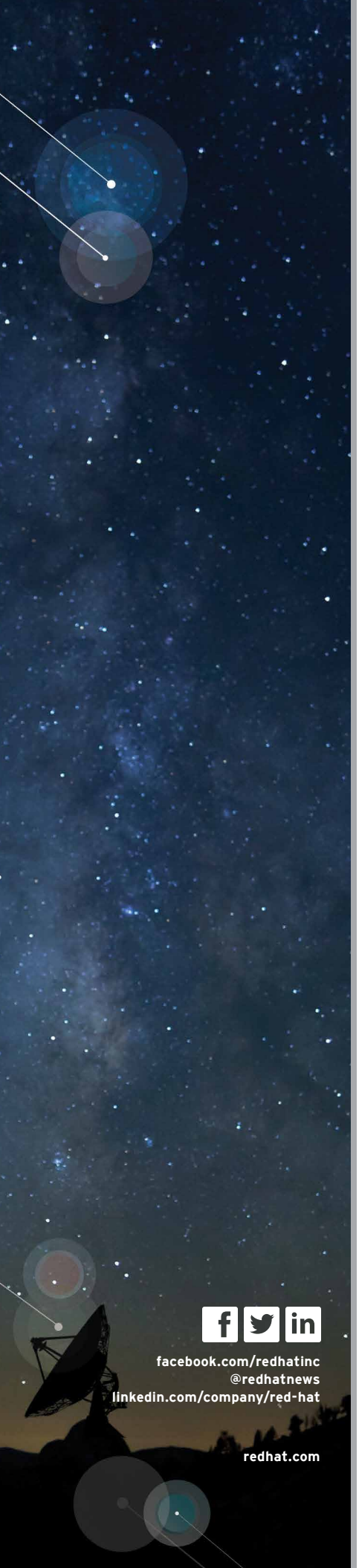

RED HAT® ENTERPRISE LINUX®

redhat.

WHITEPAPER

HOW RED HAT DELIVERS A SECURE ENTERPRISE PLATFORM FOR NEXT-GENERATION DATACENTERS

EXECUTIVE SUMMARY

Security has always been an important consideration when selecting a server operating system for enabling business-critical applications and other essential workloads. This is true now more than ever, especially for enterprises looking to build next-generation datacenters.

Red Hat's recognition of this situation is demonstrated by the extensive set of processes and practices we employ to deliver an exceptionally secure, open source server platform. Key differentiators that set Red Hat® Enterprise Linux® apart include a history of security innovation, the coverage Red Hat provides for the thousands of software packages that comprise a complete solution, the quality of service with which Red Hat executes related security responses and software update processes.

SERVER OPERATING SYSTEMS AND THE NEED FOR SECURITY

Unfortunately, there are many forces conspiring to diminish the effectiveness of traditional network-based countermeasures such as network firewalls and intrusion prevention systems. A few notable examples include the following:

- A threat landscape characterized by increasingly sophisticated malware and other attacks designed to evade network defenses by targeting vulnerabilities at higher layers of the computing stack
- The so-called dissolving perimeter – a condition brought on by user mobility and other trends that enable communication traffic to bypass designed chokepoints, or eliminate such locations in the network all together
- The evolution to next-generation, dynamic datacenters featuring extensive use of server (and other) virtualization technologies, cloud computing practices, and flatter network designs — all of which contribute to the dissolving perimeter phenomenon

A significant outcome is the emphasis this situation places on the need for robust security at an organization's endpoints — especially the server platforms used to enable key business applications and workloads.

To be clear, the need for security in a server operating system is nothing new; it's only the magnitude of this need that has been increasing, particularly in recent years. Accordingly, neither are Red Hat's efforts in this area new. For Red Hat, delivering an exceptionally secure open source server platform has always been a top priority. The remainder of this paper demonstrates this point by explaining the key practices, processes, and overall strategy Red Hat uses to achieve this all-important objective for Red Hat Enterprise Linux. The focus in this case is on

the security of the platform itself. This is in contrast to the many security features and services the solution makes available to the applications it serves, such as cryptographic libraries and routines. Details on these additional capabilities can be found at www.redhat.com/solutions/it/security/

"Vulnerabilities affecting this portfolio [end-point PCs] have increased in three years, or by 71% in the last 12 months alone. This trend is primarily the result of vulnerabilities in third-party programs, which in turn are also much harder to patch as a result of a lack of a unifying patch mechanism. By neglecting the risk of ubiquitous third-party programs, users risk being compromised by cybercriminals every day, despite the deployment of other security measures.

2010 SECUNIA HALF YEAR SECURITY REPORT, HTTP://SECUNIA.COM/GFX/PDF/SECUNIA_HALF_YEAR_REPORT_2010.PDF

DELIVERING A SECURE PLATFORM

For Red Hat, delivering a secure platform in the first place breaks down into two high-level areas: incorporating and applying innovative security mechanisms at the core of the solution and extending coverage to account for the security of all the open source packages that comprise Red Hat Enterprise Linux.

INNOVATING AND INFUSING

Red Hat has an extensive history of innovation and related efforts focused on enhancing the security of the base Red Hat Enterprise Linux operating system. Early initiatives dating back to the beginning of the previous decade include the formation of a dedicated security response team, the implementation of a single, secure mechanism for distributing all software updates, and the decision to have the product's firewall on by default (approximately 3 years in advance of a similar decision by Microsoft when it released Windows 7 in 2009). Another major initiative that is representative of Red Hat's efforts in this area are its commitment to having SELinux integrated into the operating system and enabled by default (2005).

Originally developed by the NSA, Security-Enhanced Linux is a powerful feature set that provides a mechanism for enforcing granular, system-level access control policies through the use of Linux Security Modules in the Linux kernel. Without getting into all of the underlying details, what this enables – by leveraging a combination of the default "targeted policy" used by Red Hat Enterprise Linux and administrator-defined custom policies – is a configuration where network-exposed system services are confined to the minimum privileges required to do their jobs. The net result is considerably less risk of these programs causing harm if they become compromised, for example due to a buffer overflow, application-level misconfiguration, or any other type of exploitable vulnerability.

EXTENDING COVERAGE

The second strategy Red Hat uses to deliver a secure platform in the first place is that of extending our coverage to account for the security of the more than 3,000 packages that comprise a Red Hat Enterprise Linux distribution. Red Hat takes this approach in part to compensate for fact that, with an open source solution, it's very difficult to count on secure coding practices having been followed for other than our own contributions to the code base.

The issue is the risk posed by third party software – or, for open source projects, upstream packages that others are responsible for developing. Think of it this way. If you're a major hardware vendor, is all the code running in your device yours? Did you develop it all in house? More than likely it's a combination of material that was internally written, obtained via acquisition, leveraged from an open source project, or licensed from other parties. And that's okay. It's just that when something goes wrong, like a major vulnerability is discovered, it doesn't matter who or where the problem was introduced. From the customer's perspective, the issue is all yours, even if the affected piece of code isn't.

The same situation applies for major operating systems. Perhaps to an even greater extent if you consider the myriad applications and utilities typically used to "build a system" and ultimately make it useful. Granted, with other operating systems some of these third party resources include their own update mechanisms. But many others do not. And when something goes wrong with one of these other components, like it or not, the impact to the customer experience reflects on the entire solution.

Specific steps Red Hat takes to avoid this situation with Red Hat Enterprise Linux include the following:

Knowing exactly what's being shipped. Red Hat has identified that knowing what is included in the product is essential, and takes the time and effort to build the binaries for Red Hat Enterprise Linux from the associated source code. Security-related advantages of this approach compared to simply obtaining builds from upstream projects include:

- enablement of a secure and reproducible build environment that (a) eliminates malware from infected machines, (b) ensures that a build can be accurately re-created at any point in the future, and (c) allows consistent delivery of highly quality security fixes in a timely manner
- elimination of unnecessary features and redundant embedded libraries, thereby reducing the potential attack surface and the effort required to fix any related issues that arise
- validation that the appropriate compiler flags were used to engage applicable security features, such as stack protector, FORTIFY_SOURCE and position independent executable features
- targeted insertion of additional security protections and bug fixes

Careful selection and configuration of packages. Red Hat tracks the security performance of software packages over time. Any software packages with repeated occurrences of egregious flaws receive extra attention, ranging from selection of or modification to the packages themselves, to not including them in our product. In addition, Red Hat identifies those software packages likely to have the highest degree of exposure and works to optimize their default settings for a strong security profile. A good example is Mail Transfer Agents such as sendmail which we configure by default to not monitor the network. This way customers who don't need an externally facing mail service don't get one and, reducing the out-of-the-box risk profile.

Providing third party packages we know customers will use. Red Hat Enterprise Linux isn't just a bare operating system but a feature-rich environment with many tools and applications that customers want to use. For example, to view PDF files on a desktop, installations of Red Hat Enterprise Linux includes several open-source PDF viewers. Red Hat Enterprise Linux also includes an optional packaged version of Adobe Reader, but note that Red Hat cannot provide the same level of security service that it can for open-source alternatives.

VALIDATION

The effectiveness of Red Hat's approach to delivering and maintaining an exceptionally secure server platform is demonstrated by one simple fact: of the five worms affecting customers of all Red Hat products — not just Red Hat Enterprise Linux — over the past 10+ years, none have been zero-days. The associated vulnerabilities were all fixed in advance of the worms being released (by as much as 18 months). Moreover, the one worm that could have affected Red Hat Enterprise Linux was automatically blocked from the outset by SELinux.

Automated analysis and enforcement of security practices. Red Hat uses a suite of quality assurance tools to prevent an extensive array of potential security issues. Numerous protections added to the compiler (gcc) and run-time library (glibc) focus on detecting common programming mistakes and attempts to exploit them. Other tools perform standard functions, such as virus detection and proper patch integration. Changes to FORTIFY_SOURCE flags, setuid executables, and exported API functions are just a handful of the types of deviations that might be cause for concern, and that require sign off from Red Hat's security engineering team.

Upstream relationships and community involvement. Red Hat engineers are an integral part of many upstream projects (e.g.Apache , Mozilla,and OpenSSL) and contribute to many others as a means to influence the security of resulting packages. We also participate on industry panels, stay involved with the development of relevant security standards, and work with peers and competitors to further improve the security of open source projects in general. By helping upstream open source projects handle security issues effectively and efficiently we reduce the risk not only to Red Hat's users, but to all users.

MAINTAINING A SECURE PLATFORM

Complementing Red Hat's efforts to deliver a secure platform in the first place are the steps it takes to maintain a high degree of security from after that initial delivery, that is, into the maintenance phase. Key elements of the Red Hat strategy in this area include having a dedicated security response team, a highly detailed process for managing vulnerabilities, intelligent patching practices, and secure mechanisms for distributing updates. Also central to Red Hat's approach is the conviction that, by itself, having the right response processes in place is not enough. Equally important is the quality of service with which these response processes are executed.

DEDICATED SECURITY RESPONSE TEAM

The Red Hat Security Response Team (SRT) is the force that strives to provide high quality fixes in a timely manner for vulnerabilities in all Red Hat products. As the overall owner of the response process, the SRT establishes governing policies and procedures and, with knowledge, collaboration and determination, shepherd each issue along in a manner consistent with its designated severity level. Beyond overseeing the process, the team also performs many of the individual steps itself, including alert tracking, initial triage, and development of the resulting security advisories. Furthermore, the team serves as the primary interface on security issues for Red Hat customers. In this capacity, it is responsible for responding to security related inquiries, investigating customer-submitted issues, providing periodic progress reports for any prolonged investigations, and, in general, helping customers to keep their systems updated and secure.

It's also important to recognize that the Red Hat SRT is a dedicated team. This is in contrast to other organizations where security response is just one of the functions assigned to developers and engineers also responsible for getting products out the door on time. This distinction is critical and is what ultimately enables Red Hat not just to respond to security issues, but to do so with a premium quality of service.

RED HAT VULNERABILITY MANAGEMENT PROCESS:

- identify security issues
- assess severity
- create fixes
- package fixes
- disclose fixes
- distribute updates

THOROUGH VULNERABILITY MANAGEMENT PROCESS

Although dedicated ownership of the security response function is critically important, so too are the processes that define and provide consistent performance of the required tasks. Accordingly, what lies at the heart of Red Hat's efforts is a very thorough process for managing vulnerabilities. Details of the sub-components for this process and how Red Hat goes about executing them are as follows:

Identifying security issues. Red Hat actively scours numerous outlets to supplement its own internal findings of security flaws in Red Hat Enterprise Linux. Typical sources include public mailing lists and sites for specific technologies and projects, vulnerability clearing centers such as the CERT Coordination Center, the Mitre CVE project, well-known bug hunters, and even other Linux vendors. An added challenge, however, stems from the fact that Red Hat doesn't write all the code for Red Hat Enterprise Linux. What this means is that when someone finds a flaw in the Apache web server, for example, they'll most likely report it to the Apache Software Foundation – and not necessarily to Red Hat. This is another reason why involvement in upstream projects and the open source community is so critical to Red Hat; these relationships serve as another significant source of vulnerability discovery.

Assessing severity. Also known as triage, this step in the process is all about determining the actual severity of the vulnerability — as opposed to the severity assigned by the person who reports it. In addition to the nature of the vulnerability and the types of exploits likely to operate against it, other assessment considerations include which specific pieces of code are impacted, the sensitivity of the applications they support, and their potential degree of exposure. In other words, this step involves not only a heavy dose of technical judgment skills, but also an understanding of the bigger picture, the overall landscape within which any given flaw exists. This further demonstrates the need for and value of a skilled and dedicated response team.

Creating fixes. The designated severity level determines the overall fix strategy and the intensity with which the SRT "project manages" the process going forward. For example, critical vulnerabilities are responded to on an emergency basis. Key resources are marshaled and coordinated to develop and distribute a fix as rapidly as possible — often within a day.

This part of the process also includes the usual checks and controls for product integrity, such as regression and compatibility testing, approval chains, and automated enforcement of who is authorized to do what and when (e.g., in terms of testing, approving, and committing changes). One significant difference, however, is Red Hat's commitment to back-porting fixes — an approach that significantly reduces the potential for compatibility issues and the introduction of additional vulnerabilities.

Packaging fixes. In general, Red Hat does not batch security fixes; it notifies customers immediately once an update/patch becomes available. Rather than provide monthly updates, Red Hat releases patches as soon as they are available. To some extent a natural byproduct of using open source software, this approach has the benefit of minimizing the embargo period, or amount of time that Red Hat knows about an issue in advance of the public. By deliberately keeping embargoes short in this manner – on average approximately three weeks for Red Hat Enterprise Linux – customers are protected from the risk of exploits that are unknown to Red Hat. In comparison, alternate approaches that keep vulnerabilities private for much longer periods of time risk exposing customers to exploits that could otherwise be easily thwarted.

Disclosing fixes. Red Hat's general philosophy when issuing Red Hat Security Advisories (RHSAs) is that these communications are to be exceedingly open and detailed about what is being fixed, how it's being fixed, and what the potential impact is for both the original issue and the fix. This is in stark contrast to the practice of fixing multiple undisclosed issues under cover of a broader, publicly disclosed deficiency – an approach that may work up to the point that the unknown "fixes" actually break something else. Or not including enough information so that customers are able to make a truly informed decision.

Distributing updates. Consistent with an "extend and embrace" strategy of extending coverage, Red Hat provides customers with secure mechanisms for notification and delivery of updates. Providing coverage for all Red Hat Enterprise Linux packages minimizes the risk of customers not updating their software by making the process of doing so considerably easier. There's no need for organizations to wrangle with multiple update tools, or, worse, to manually "hunt and peck" to obtain information about security issues and their fixes for each and every piece of software they elect to deploy. Red Hat also ensures the integrity of all product updates by taking appropriate and proven measures, such as generating and storing all signing keys in hardware and keeping them separate from keys used for other purposes – a best practice that other vendors have failed to maintain in the past.

QUALITY OF SERVICE

There's no doubt that having thorough vulnerability management and responses processes is essential to keeping a server platform secure over time. Equally important, however, are the finer points of not "what" but "how" everything is being done. This "quality of service" factor is particularly critical for facilitating the customer end of the process when it comes to maintaining system security. The bottom line is that if customers are unable to quickly obtain and easily consume the security fixes they need, then nothing else we've done actually matters. Their systems will remain insecure despite our efforts to ensure otherwise.

For Red Hat, the focus on quality of security service is reflected not only by the decision to have a dedicated security response team, but also in many other aspects of its approach to delivering and maintaining a secure server platform. Specific examples include the emphasis Red Hat places on:

For information on Red Hat Enteprise Linux government standards and certifications, see **www.redhat.com/solutions/industry/government/certifications.html.**

- Responding to all security issues. In contrast to many of our competitors, our security processes are not limited to the software that we create ourselves, but extend to cover all third party software that is ultimately available as part of a complete solution. The net result of this considerable investment on our part is a smoother, lower risk and less costly ownership experience for Red Hat customers.
- Responding to important issues quickly. For Red Hat Enterprise Linux, there is no bundling of fixes to wait for a monthly release. The goal, simply put, is to fix security issues that arise in a manner commensurate with their level of severity. For critical vulnerabilities, that means having an update available to fix them the same or next calendar day after public disclosure responding in less than one day.
- Facilitating customers' responses. Red Hat recognizes that if the solution is not easy to consume – if it isn't easy for customers to execute their response processes quickly and efficiently — then it's not much of a solution. This is why, for example, Red Hat:
    - Provides customers with direct access to the Red Hat SRT and commits to responding to all email communications within three working days. According to internal data collected by Red Hat, 99.4% of communications in 2012 received a human response within one business day, even during holidays..
    - Provides customers with secure mechanisms for obtaining security notifications and fixes.
    - Provides customers with extensive metadata about each flaw, including when and how it was discovered, when it became public, and what full disclosure of precisely what is being fixed, how, and why.

The net result is a high quality of security service for customers of Red Hat Enterprise Linux customers, and, overall, an exceptionally secure platform for enterprise workloads.

CONCLUSION

A big part of what makes Red Hat Enterprise Linux the premier Linux platform for enterprise workloads is the fact that it is exceptionally secure, as evidenced by its Common Criteria certification at EAL4+. This is the result of an extensive set of policies and processes Red Hat has put in place to both deliver a secure platform in the first place and over time. Key aspects of our approach that help set Red Hat Enterprise Linux apart from the competition in this regard include:

- An extensive history of innovating and incorporating at the core of the platform new security mechanisms intended to thwart entire classes of vulnerabilities
- The coverage provided in terms of both initial hardening and ongoing security response for all of the more than 3000 packages that comprise a complete distribution — as opposed to doing so only for the software Red Hat creates
- An investment in having a dedicated security response team and its commitment to ensure that Red Hat Enterprise Linux customers not only have a secure platform, but also receive a superior "quality of security service."

ABOUT RED HAT

Red Hat is the world's leading provider of open source solutions, using a community-powered approach to provide reliable and high-performing cloud, virtualization, storage, Linux, and middleware technologies. Red Hat also offers award-winning support, training, and consulting services. Red Hat is an S&P company with more than 70 offices spanning the globe, empowering its customers' businesses.

NORTH AMERICA
1-888-REDHAT1

EUROPE, MIDDLE EAST AND AFRICA
00800 7334 2835
europe@redhat.com

ASIA PACIFIC
+65 6490 4200
apac@redhat.com

LATIN AMERICA
+54 11 4329 7300
latammktg@redhat.com

facebook.com/redhatinc
@redhatnews
linkedin.com/company/red-hat

redhat.com
#10900617_V5_0413