Securing OpenStack Clouds

> "The OpenStack community is taking security seriously..."[1]
>
> **Daniel Chow, a Q&A with security expert Corey Nachreiner**

Anyone who reads the news knows that IT security breaches are a constant issue, and they've caused major problems for healthcare providers, governments, and enterprises. Most incidents have been attacks on traditional infrastructures. Today, however, clouds are becoming ubiquitous. Organizations around the world are choosing cloud technologies for an optimal mix of reliability, flexibility, and value. A key question for modern IT is "how are security, compliance and privacy affected by cloud?"

According to the 2016 State of the Cloud Survey[2], ongoing security risks are a major concern for organizations evaluating cloud computing and are seen as the primary barrier for cloud migration.

Of course, security isn't a new concern. Many of the highest paying positions in IT today are security related[3]. Seasoned administrators know that complete security is hard to achieve in the world of general-use computing. We've become comfortable with proprietary ecosystems issuing patches and updates, but there's a perception that open source technologies aren't as secure,

don't do a good job addressing vulnerabilities, and can expose enterprises to increased risk.

In this paper, we'll address some of the questions about security, compliance and privacy we've received from users and technologists. We'll demonstrate OpenStack readiness for your workloads, and facilitate trust and relationships between your team and the OpenStack community.

1 How safe and secure is open-source OpenStack?, ComputerWorld, September 2015, http://www.computerworld.com/article/2984352/enterprise-applications/how-safe-and-secure-is-open-source-openstack.html

2 http://www.hytrust.com/cloud-sddc-study/

3 http://www.cio.com/article/2933173/salary/10-highest-paying-it-security-jobs.html

The OpenStack community values cloud security.

With OpenStack software, security is a multi-stakeholder effort with broad participation from some of the biggest users and IT vendors in the world, and those stakeholders take security seriously. OpenStack has reached a significant level of maturity, with 65% of actual users in a recent survey[4] in production or full operational use. "Notable Fortune 100 enterprises BMW, Disney and Walmart have irrefutably proven that OpenStack is viable for production environments [5]." These users and others, including Best Buy, eBay, Comcast and Bloomberg, have chosen OpenStack for their enterprise production environments.

Overall Security

Aren't open source projects like OpenStack easy to attack?

Many IT infrastructures rely on open source software, including Linux and Apache. The Open Source Hardening Project was established by the US Department of Homeland Security in 2006 to check the security of open source software, and found that in 250 open source projects, there is one software flaw for every thousand lines of code[6], comparable to proprietary software. In addition, an independent report[7] by Coverity demonstrated that open source software has significantly fewer code defects than commercial software.

Like in Linux and Apache, security starts with clean code, and our view is that OpenStack is more secure, not less, because it's open source. We find no evidence that open source software is more flawed or more risky than proprietary software. In fact, public access to source code, keeping it open and available for review, means that bugs can be found and fixed more quickly.

> Many companies in the OpenStack Marketplace[8] help organizations like yours architect and deploy secure OpenStack clouds, by extending OpenStack enterprise security capabilities and solving unique requirements.

Can OpenStack be secure?

Securing an OpenStack cloud is not unlike securing any other IT infrastructure—requiring a similar set of tools and skills and a similar understanding of security. Securing OpenStack is an extension of a well-understood problem—securing normal IT infrastructure, such as keeping the infrastructure patched, reducing attack surfaces, and managing logging and auditing.

Hundreds of the largest organizations in the world, including financial services firms such as PayPal[9] and TD Bank[10], and government organizations such as the National Security Agency[11] and the Argonne National Laboratory[12], rely on OpenStack. These industries can be especially security-conscious.

Securing the Code Base

How does OpenStack ensure that the stack is secure?

Security is a critical concern for OpenStack, and it is constantly being evaluated and addressed at all layers—the base operating system and third-party tools through applications and everything

4 http://www.openstack.org/assets/survey/April-2016-User-Survey-Report.pdf
5 http://www.openstack.org/enterprise/forrester-report/
6 http://www.computerweekly.com/news/2240076780/Lamp-software-found-to-have-fewest-bugs
7 http://go.coverity.com/rs/157-LQW-289/images/2014-Coverity-Scan-Report.pdf
8 http://www.openstack.org/marketplace/
9 http://www.informationweek.com/strategic-cio/paypal-declares-its-100--openstack-cloud/d/d-id/1319694
10 https://www.youtube.com/watch?v=b4Gt4oNZVIQ
11 https://www.youtube.com/watch?v=NgahKksMZis
12 https://www.openstack.org/user-stories/argonne-national-laboratory-us-department-of-energy/

in between. Unlike many commercial cloud platforms, OpenStack security is a collaborative effort across thousands of developers who work together to ensure that OpenStack provides a robust, reliable, and secure cloud for public, private, and hybrid deployments. But expecting thousands of distributed developers to write a secure cloud platform without support, guidance or direction isn't realistic.

Support, guidance and direction is provided to the thousands of developers by four highly skilled security groups. These people work collaboratively to keep insecure code out of production, vigilantly pursue security fixes, and eliminate exposures across all OpenStack projects. These groups are:

1. The OpenStack Security Project
2. Project-specific security experts
3. Commercial OpenStack vendors
4. OpenStack project developers

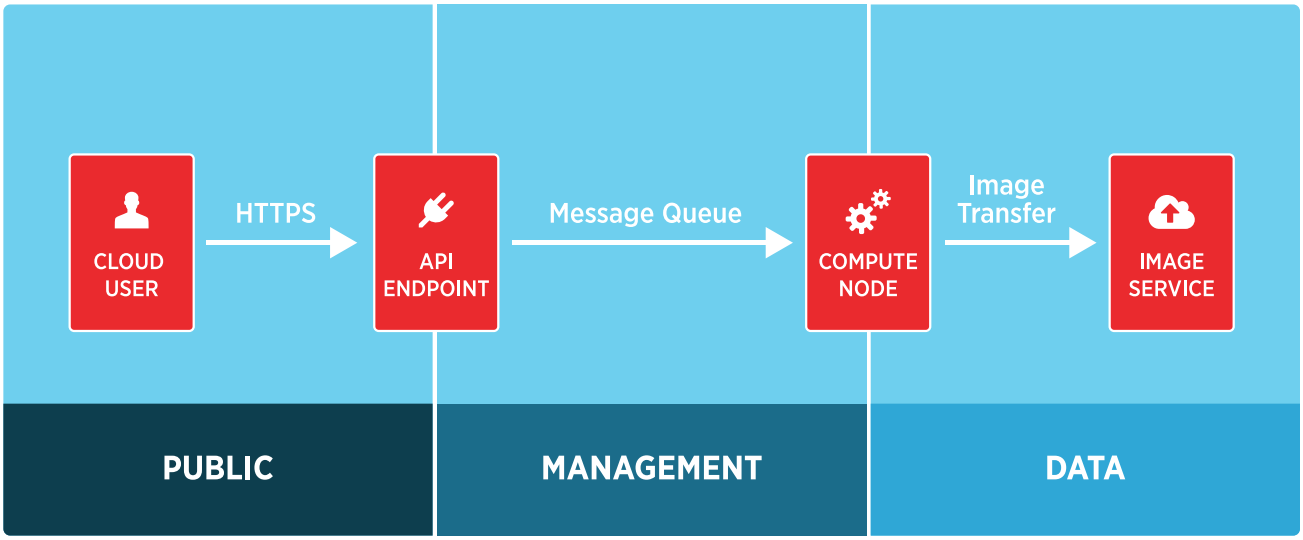
What does the OpenStack Security Project do?

The OpenStack Security Project[13], and the Vulnerability Management Team (VMT)[14] within it, coordinates the work needed to identify, limit, and resolve security issues and vulnerabilities across the OpenStack projects.

Comprised of approximately 250 members, the Security Project consists of several active efforts at any time, as well as ad-hoc patch-and-fix development to help resolve problems that crop up in the field. Through improvements to code, architecture, and various documentation efforts including vulnerability management, the Project helps secure the OpenStack code base, as well as provides deployers with the documentation needed to make sound security choices.

The Security Project communicates across the OpenStack community and serves as a central point of contact for any security issues. It also publishes the OpenStack Security Guide, Advisories and Notes.

OpenStack Security Guide. The OpenStack Security Guide provides best practices learned by cloud operators while hardening their OpenStack deployments. This book was written by a close community of security experts from the OpenStack Security Project for organizations implementing OpenStack. The guide includes 17 chapters on specific OpenStack security considerations including, for example, the three security domains (public, management and data) and bridging between them. It is regularly updated. Read the guide[15] online.



OpenStack bridges between three security domains

13 https://wiki.openstack.org/wiki/Security
14 https://security.openstack.org/vmt-process.html
15 http://docs.openstack.org/sec/

Advisory Activities. The Security Project issues Security Advisories (OSSA)[16] and Security Notes (OSSN)[17], both of which are aimed at OpenStack users and vendors who either run OpenStack or distribute OpenStack for commercial use.

- Security Advisories address vulnerabilities and are a function of the VMT. Once the VMT has identified a fix for a vulnerability, the VMT releases a Security Advisory for the community. An advisory details the nature of the vulnerability and any workarounds or patches needed to mitigate it.
- Security Notes complement Security Advisories, are owned by the Security Project, and can be issued for almost anything affecting the security of OpenStack deployments. Security Notes address vulnerabilities in third-party tools typically used within OpenStack deployments and provide guidance on common configuration mistakes that can result in an insecure operating environment.

Are there also project-specific security experts?

Since security is so important to OpenStack, most of the critical OpenStack projects have their own security liaisons. Those liaisons are core reviewers for each project (Nova, Neutron, etc.) and are responsible for ensuring only secure code is incorporated in the general releases. Liaisons work closely with the Vulnerability Management[18] Team to help assess the impact of reported issues, coordinate the development of patches, review proposed patches and propose backports. A full list of liaisons can be found here[19].

How do commercial vendors help with OpenStack security?

There are many OpenStack ecosystem companies[20] that rely on OpenStack in their commercial products and their own internal cloud implementations. They have a vested interest in making sure that OpenStack is fully secure, and to do so, they have dedicated security teams working on OpenStack, building out tooling, finding issues, and making OpenStack stronger.

As they uncover security issues, they engage with the Security Project and/or the VMT to collaboratively develop fixes, which are then made available to the broader OpenStack community through advisories, notes, or new releases.

How does the OpenStack Security Project team help developers write secure code?

In a sense, the Security Project team, project liaisons, and commercial security experts all support the OpenStack project developers. However, there are a few special ways that project developers get support and assistance to write secure code. Outside of all their other functions and publications, the OpenStack Security Project developed a set of guidelines and best practices[21] to help project developers avoid common mistakes that lead to security vulnerabilities within the OpenStack platform. These guidelines and best practices have been widely adopted across the OpenStack community.

In addition to the guidelines, the Security Project introduced tooling and automation to improve the overall security of OpenStack projects. The OpenStack Security Project currently manages three tools to help address security issues:

1. Bandit[22] —Bandit is a security linter[23] for Python source code. It's a stand-alone tool which can be downloaded and run against source code. Any application developer writing in Python can also use Bandit to verify the security of their code.

16 https://security.openstack.org/ossalist.html
17 https://wiki.openstack.org/wiki/Security_Notes
18 https://security.openstack.org/vmt-process.html
19 https://wiki.openstack.org/wiki/CrossProjectLiaisons#Vulnerability_management
20 https://www.openstack.org/foundation/companies/
21 https://security.openstack.org/#secure-development-guidelines
22 https://wiki.openstack.org/wiki/Security#Bandit_-_Python_Security_Linter
23 A small program that checks code for errors. See http://www.sublimelinter.com/en/latest/about.html

2. Syntribos[24] —This is a tool in development that finds security issues in OpenStack RESTful APIs and services, detecting problems automatically.
3. Anchor[25] —Anchor is an ephemeral PKI certification authority built to address the requirement for a simple, easily deployable PKI service for OpenStack infrastructures. It uses automated issuing rules and short life certificates to mitigate many of the common certificate security issues that exist today[26].

Finally, if an issue crops up, OpenStack project developers are also able to request design guidance via the OpenStack Security IRC channel or the openstack-dev mailing list.

Is there a clear-cut process to report security issues?

There's an established process for reporting issues that's described in detail on the OpenStack Security Overview page[27]. To report a bug, OpenStack developers use Launchpad.net[28]. Once the bug is received it will be reviewed by the VMT in private. They will involve the smallest number of developers possible to triage the vulnerability before publicly releasing the fix following a standard responsible disclosure process.

Assisting Deployers

Where should deployers begin?

Most organizations choose the assistance of an OpenStack distribution or other commercial provider when deploying OpenStack. Many of these distributions are listed in the OpenStack Marketplace, where you can find a detailed view of these providers' offerings. All OpenStack deployers, in-house or commercial, should follow the OpenStack Operations Guide[29] for step-by-step guidance. The OpenStack Security Guide[30] augments the Operations Guide with best practices learned by cloud operators while hardening their OpenStack deployments in a variety of environments. The Security Guide also can assist with hardening existing OpenStack deployments or evaluating the security controls of OpenStack cloud providers.

The Security Guide has several fundamental objectives, including:

- Identifying the security domains in OpenStack
- Providing guidance to secure your OpenStack deployment
- Highlighting security concerns and potential mitigations in present day OpenStack
- Discussing upcoming security features
- Providing a community-driven facility for knowledge capture and dissemination

This book was written by a close community of security experts from the OpenStack Security Group and is regularly updated. Read the guide[31] online today.

What are the critical elements of a secure OpenStack cloud?

Some of the most important considerations addressed by the OpenStack community include:

- Management
- Secure communications
- API endpoints
- Identity
- Dashboard
- Compute
- Block and object storage
- Shared file systems
- Networking
- Message queuing
- Data processing

24 https://pypi.python.org/pypi/syntribos
25 https://wiki.openstack.org/wiki/Security#Anchor_-_Ephemeral_PKI
26 Ibid., p. 5
27 https://security.openstack.org/#how-to-report-security-issues-to-openstack
28 https://launchpad.net/openstack
29 http://docs.openstack.org/ops/
30 Op. cit., p. 3
31 Op. cit., p. 3

- Databases
- Tenant data privacy
- Instance security management
- Monitoring and logging
- Compliance

The guide provides insights and guidance for all of these areas.

Does OpenStack support multi-factor authentication?

At its most basic, authentication is the process of confirming identity, and a familiar example is providing a username and password when logging in to a system. However, the risks of username/password logins are well known and many organizations seek alternatives.

Multi-factor authentication is used for network access to privileged user accounts. The OpenStack Identity service (Keystone) supports multiple methods of authentication, including username and password, LDAP, and external authentication methods. Keystone supports, and many users implement, federated identity to establish trusts between Identity Providers (IdP) and the services provided by an OpenStack cloud[32]. Servers may also enforce client-side authentication using certificates. Using multi-factor authentication helps to reduce the risks of brute force attacks, social engineering, and spear and mass phishing attacks.

For more details, visit the Security Guide Authentication page[33].

Does OpenStack encrypt data?

OpenStack supports volume encryption, ephemeral disk encryption, and disk-level encryption for object storage. Encrypted data sent over the network remains encrypted. Various back-end infrastructure components (such as storage) can also be used to augment data encryption by, for example, leveraging the authentication and encryption capabilities of the iSCSI protocol, if supported. Other third-party tools can be used within OpenStack to enhance general encryption capabilities.

Refer to the Data Encryption chapter of the guide[34] for more detail.

Can OpenStack support commercial and government compliance standards and certifications?

Compliance means adhering to regulations, specifications, standards and laws. It is also used when describing an organization's status regarding assessments, audits, and certifications. Many organizations using OpenStack must comply with regulations such as HIPAA or PCI DSS. OpenStack can be used to support third-party certifications and regulatory requirements with security hardening, using the same governance and operational controls as you would for any enterprise-level infrastructure. For more information, review the OpenStack certifications and compliance page[35].

How can OpenStack support an organization's privacy policy?

Privacy is an increasingly important element of a compliance program. Businesses are being held to a higher standard by their customers, who have increased interest in understanding how their personal information is treated. An OpenStack deployment will likely need to demonstrate compliance with an organization's privacy policy. As with any other IT infrastructure, this area requires comprehensive planning, thought and investment. By using established best practices, including those published by governments, a holistic privacy management policy may be created and practiced for OpenStack deployments.

How do I get updates and patches?

OpenStack has major releases twice a year, all of which are available to the OpenStack community and the public. Organizations can download immediate fixes from the appropriate project's repository. For most users, patches will be

32 http://docs.openstack.org/security-guide/identity/federated-keystone.html

33 http://docs.openstack.org/security-guide/identity/authentication.html

34 http://docs.openstack.org/security-guide/tenant-data/data-encryption.html

35 http://docs.openstack.org/security-guide/compliance.html

tested and distributed by their distributor, which typically have accelerated release processes for security fixes in-between major releases, ensuring urgent security fixes are tested and released in appropriately urgent timeframes.

Is there a clear-cut process for users to report security issues?

OpenStack users report issues on Launchpad[36] for the particular OpenStack project identified or suspected, using the private security bug option. See the "How to Report Security Issues to OpenStack" section of the OpenStack Security page"[37] for more information.

Wrapping it up

Do enterprises have secure OpenStack clouds in production?

Many organizations[38] use OpenStack in production, including those with high security requirements for payment handling (e.g. Walmart.com, PayPal), and financial services (TD Bank, Bloomberg, Wells Fargo). Public and hosted private cloud providers have similar requirements to protect their hosted clients' applications and data, and in addition, must secure each tenant from the others. IBM Blue Box, for example, offers Private Cloud as a Service (PCaaS) using OpenStack, hosting thousands of customers across 17 datacenters covering North America, South America, Europe, the Middle East, and Asia.

Blue Box's chief product officer, Hernan Alvarez, said:

"The threat surface in cloud changes constantly. That's why working with open source cloud software like OpenStack makes so much sense. The network effect of thousands of developers publicly sharing newly discovered vulnerabilities and patches, as well as improvements in areas like identity management and bare metal support, improves security and quality for everyone. Meanwhile, we focus on automation and tooling to ensure we can push updates to all of our customers as soon as those updates are made. It's a great solution for managing threats at the infrastructure layer."

How do I learn more?

Most organizations considering OpenStack will choose an OpenStack public[39] or hosted private[40] cloud provider, or a distribution[41] for deployments. These typically have security expertise to help enterprises like yours implement a secure OpenStack cloud.

However, for organizations that aren't using a distributor, the resources throughout this paper will help. The most critical are the Security Guide[42], Security Notes[43], and the Operations Guide[44].

For specific OpenStack security issues, you can engage with the OpenStack Security Project Team[45], the OpenStack Security IRC Channel[46], and the Developers Mailing List[47].

In conclusion, security is a priority for the OpenStack community and we're engaged in making it better. We're here to help organizations like yours succeed. For more general information about OpenStack, including our new book, *OpenStack: The Path to Cloud,* visit the OpenStack in the Enterprise page[48].

36 Op. cit., p. 5.
37 https://security.openstack.org/
38 http://superuser.openstack.org/articles/section/user-stories
39 http://www.openstack.org/marketplace/public-clouds/
40 http://www.openstack.org/marketplace/hosted-private-clouds/
41 http://www.openstack.org/marketplace/distros/
42 Op. Cit., p. 3
43 Op. Cit., p. 4
44 Op. Cit., p. 5
45 Op. Cit., p. 3
46 https://wiki.openstack.org/wiki/IRC
47 http://lists.openstack.org/cgi-bin/mailman/listinfo/openstack-dev
48 http://www.openstack.org/enterprise

CONTRIBUTORS

Kathy Cacciatore, *Consulting Marketing Manager,* **OpenStack Foundation**

Jamie Clark, *Vice President, Architecture,* **Solinea**

Rob Clark, *Distinguished Engineer, Cloud Security and OpenStack Security Project Technical Lead (PTL),* **IBM Corporation**

Travis McPeak, *Senior Security Architect,* **IBM Corporation**

Brian Whitaker, *President / Founder,* **Zettabyte Content, LLC**

OpenStack is a registered trademark in the Unites States and in other countries. All other company and product names may be trademarks of their respective owners.

This work is licensed under a Creative Commons Attribution-NoDerivatives 4.0 International License. For more information on use, please visit http://creativecommons.org/licenses/by-nd/4.0/. To view a copy of this license, visit https://creativecommons.org/licenses/by-nd/4.0/legalcode.

Front page image by Mark Fischer, available at https://www.flickr.com/photos/fischerfotos/7454996046/. It is licensed under a Creative Commons Attribution–ShareAlike 2.0 Generic License. For more information on use, please visit https://creativecommons.org/licenses/by-sa/2.0/. To view a copy of this license, visit https://creativecommons.org/licenses/by-sa/2.0/legalcode.