

MUST READ [HOW TO UPGRADE FROM WINDOWS 10 HOME TO PRO WITHOUT HASSLES](#)

## Juniper firewall fiasco is a major blow-up for government's backdoor rhetoric

Opinion: If ever there's been a shining example of why government backdoors are a bad idea, the motherlode just got served up hot on a platter.



By [Zack Whittaker](#) for [Zero Day](#) | December 23, 2015 -- 16:07 GMT (00:07 GMT+08:00) | Topic: [Security](#)



*(Image: file photo via CBSNews.com)*

Aaron Sorkin may not be a household name, but you've probably heard of his work. From "The West Wing" to "The Social Network," and "Studio 60 on the Sunset Strip," and "The Newsroom," Sorkin has dedicated the name of one episode in each of his productions to [asking the same question](http://www.vulture.com/2014/12/newsroom-aaron-sorkin-what-kind-of-day-has-it-been-west-wing-sports-night-studio-60.html) (<http://www.vulture.com/2014/12/newsroom-aaron-sorkin-what-kind-of-day-has-it-been-west-wing-sports-night-studio-60.html>):

"What kind of day has it been?"

Let me tell you that almost every day of the year, it's been a complete and unmitigated disaster for security. Encryption is used by banks to keep your money safe, it's used by government to keep its secrets safe, and it's used by companies to protect your data. But despite being the very fabric of keeping society and the internet safe and secure, encryption has been threatened by far too many narrow-minded bureaucrats with little knowledge or foresight to the consequences of its unraveling, who are paid by businesses to act as proxy spokespeople on their behalf for the trade-off of staying in power.

Encryption. It's become the hot topic of the year, with sides both for and against fighting for their heartfelt belief. The security community has consistently had to fight to be heard, knowing their views will be unlikely to influence policy, because they are -- sadly -- people without a badge or an embossed business card, or an office on the Washington DC political mile.

FBI director James Comey has called on companies to [use encryption backdoors](#)

(<http://www.zdnet.com/article/because-there-is-no-such-thing-as-a-secure-backdoor-gosh-darn-it/>), so much so he's promised he's not a "maniac" about it. Senate intelligence committee chair Richard Burr [called encryption](#)

(<http://thehill.com/policy/cybersecurity/262879-lawmakers-no-evidence-encryption-used-in-san-bernardino>) a "big problem out there that we are going to have to deal with," despite also saying that it likely wasn't used in the Paris terrorist attacks, or more recently, the shooting in San Bernardino. And Britain, on the other side of the pond, is pushing for counter-encryption legislation, which may force companies to weaken or ditch encryption at the behest of the government.

---

**READ THIS NEXT**

---



(<http://www.zdnet.com/article/apple-in-refusing-backdoor-access-to-data-faces-huge-fines/>)

**Apple, in refusing backdoor access to data, may face fines**  
(<http://www.zdnet.com/article/apple-in-refusing-backdoor-access-to-data-faces-huge-fines/>)

Analysis: Yahoo faced growing fines in 2007 when it refused to participate in the PRISM program, which sets a precedent for non-compliance with government demands.

**Read More**

(<http://www.zdnet.com/article/apple-in-refusing-backdoor-access-to-data-faces-huge-fines/>)

All too often, the encryption debate has been driven by the ill-informed media [citing unnamed and anonymous US intelligence officials](#)

(<https://twitter.com/zackwhittaker/status/677189883425898496>), who by virtue of their jobs have a biased stances. And yet some of those media outlets also [called the Juniper firewall backdoor code discovery](#) (<http://www.cnn.com/2015/12/18/politics/juniper-networks-us-government-security-hack/>) akin to "stealing a master key to get into any government building."

In the case of Juniper, it really is that bad. The networking equipment maker, with thousands of enterprise customers, said last week it had [found "unauthorized" code](#) (<http://www.zdnet.com/article/juniper-screens-devices-had-default-backdoor-password-rapid7/>) that effectively allowed two backdoors to exist for as long as three years. Nobody disputes that this was a backdoor. Juniper said it had no evidence to suggest the backdoor had been used, but also warned [there was "no way to detect" if](#) (<http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713>) it had been.

The NSA was blamed for creating weakened cryptography that Juniper went on to modify -- and badly. Exactly how the other backdoor got there remains a big question. In any case, companies who were running affected versions of Juniper's firewalls were likely also targets of the suspected nation state attacker.

Juniper's clients also include the US government, including the Defense Dept., Justice Dept. and the FBI, and the Treasury Dept., [reports The Guardian](#) (<http://www.theguardian.com/technology/2015/dec/22/juniper-networks-flaw-vpn-government-data>), which may put federal government data at risk.

If ever there's been a shining example of why government backdoors are a bad idea, the



Juniper's products, services, or technology is a bad thing. Once the backdoors were found, it took just three days for the master password used in the backdoor to be posted online, sparking open season for any hacker to target a Juniper firewall.


If whoever planted the backdoor was non-American, it highlights the point the security community has been making for months: these backdoors can and will be used and abused by the enemy.

Why  
(http://www.zdnet.com/article/why-juniper-flaw-is-a-major-backfire-for-governments-backdoor-plans/#ftag=RSSbaffb68)

Apple  
refusing to face fines (http://www.zdnet.com/article/apple-in-refusing-to-face-fines/)

NSA  
(http://www.zdnet.com/article/nsa-whelmed-with-data-ineffective/)

As the  
(http://www.zdnet.com/article/panic-in-congress/)



AdCh **READ MORE**

replay

a failure of leadership, not intelligence  
(http://www.zdnet.com/article/juniper-flaw-is-a-failure-of-leadership-not-intelligence/)

Apple  
face fines (http://www.zdnet.com/article/apple-in-refusing-to-face-fines/)

NSA  
effective, says whistleblower  
(http://www.zdnet.com/article/nsa-whelmed-with-data-ineffective/)

As the  
panic" in Congress  
(http://www.zdnet.com/article/panic-in-congress/)

**How Microsoft's data case could unravel the US tech industry** (<http://www.zdnet.com/article/why-microsoft-data-case-could-unravel-the-us-tech-industry/>)

**If you have 'nothing to hide', here's where to send your passwords**  
(<http://www.zdnet.com/article/if-you-have-nothing-to-hide-heres-where-to-send-your-passwords/>)

**Meet the shadowy tech brokers that deliver your data to the NSA**  
(<http://www.zdnet.com/article/meet-the-shadowy-tech-brokers-that-deliver-your-data-to-the-nsa/>)

## RECOMMENDED FOR YOU



**A real-life lightsaber?**  
Military device cuts through metal | ZDNet



**Get Windows 10:**  
Microsoft's biggest software upgrade in history begins today | ZDNet



**How-to: Burn your Windows 7 .ISO to DVD disc** | ZDNet



**Does "Delete forever" in Gmail really mean it?** | ZDNet

[Learn more](#)

Powered by **YAHOO!** for you

**JOIN DISCUSSION**

**SHOW COMMENTS**

## SPONSORED

- 1 Email Encryption
- 2 Cloud Storage
- 3 Free Microsoft Office
- 4 Free Spyware Removal
- 5 Data Encryption
- 6 Disable The Firewall
- 7 CRM Solutions
- 8 Quality Hearing Aids

AdChoices

## AWS Cloud

Bring your app to the  
**AWS Cloud**



Launch new apps & test existing apps.

**Try free for one year**

 **amazon**  
web services



## AWS Cloud

Bring your app to the **AWS Cloud**



AdChoices

Launch new apps &  
test existing apps.

**Try free for one year**



# Salesforce acquiring quote-to-cash app startup SteelBrick

The CRM giant's venture capital arm started backing SteelBrick earlier this year.



By [Rachel King](#) for [Between the Lines](#) | December 23, 2015 -- 23:05 GMT (07:05 GMT+08:00) | Topic: [Cloud](#)

Following speculation [earlier this week about a merger](#) (<https://www.theinformation.com/salesforce-com-in-talks-to-buy-steelbrick-for-600m?shared=712815>), **Salesforce** is buying one of the startups already backed by its venture capital arm.

The target of the deal is **SteelBrick**, a startup making quote-to-cash software.

SteelBrick CEO Godard Abel [confirmed the deal in a statement](#) (<http://blog.steelbrick.com/blog/salesforce-signs-definitive-agreement-to-acquire-steelbrick?>



(<http://www.zdnet.com/article/salesforce-as-takeover-target-heres-a-look-at-the-potential-buyers/>)

**Salesforce as takeover target: Here's a look at the potential buyers**

(<http://www.zdnet.com/article/salesforce-as-takeover-target-heres-a-look-at-the-potential-buyers/>)

Salesforce has a gawdy market cap so the field of potential acquirers is limited. Nevertheless, a handful of tech giants led by Oracle could pull off a deal.

## Read More

(<http://www.zdnet.com/article/salesforce-as-takeover-target-heres-a-look-at-the-potential-buyers/>)

\_\_hssc=&\_\_hstc=127800018.d4225990e1b02a4b8b489e5df5deb5ae.1450332865621.1450332865621.1450332865621.

[1dfb-4353-afaf-892b25cf866d%7C37e3075c-f9e7-4d66-86e1-3798d7b266f6](#)) on Wednesday.

"We have witnessed how Salesforce has pioneered the shift to enterprise cloud computing and set the standard for customer success in the industry," Abel wrote about the agreement. "Many of our team members have already enjoyed growing their careers in the vibrant Salesforce ecosystem as customers and partners for many years, and we're excited to join Salesforce."

Salesforce is paying approximately \$360 million for SteelBrick, [according to an 8-K filing with the U.S. Securities and Exchange Commission](#)

(<https://www.sec.gov/Archives/edgar/data/1108524/000110852415000041/steelbrick8-k.htm>). The deal is expected to be complete by the end of Salesforce's first fiscal quarter on April 30, 2016.

In February, Salesforce Ventures took part in an \$18 million Series B round led by Shasta Ventures with participation from previous investor Emergence Capital. That brought SteelBrick's fundraising pool to a grand total of \$29.5 million raised over the previous year at the time.

With cloud and mobile-based programs for producing sales quotes and orders, SteelBrick serves approximately 200 companies, including Cloudera, Nimble Storage, Nutanix, and HootSuite.

The SteelBrick CPQ was also built and delivered natively via the Salesforce1 Platform, the foundation for the San Francisco corporation's Internet of Things strategy first unveiled at Dreamforce 2013.

Abel also wrote SteelBrick's quote-to-cash apps will be integrated within Salesforce products.

---

**JOIN DISCUSSION**

---