
# WHITE PAPER
# Development of Server Breach Defenses - Fortress™

## EXECUTIVE SUMMARY

Fortress™ protects Ubuntu(R) and Debian(R) Linux servers. It will protect the entire LAMP stack or portions thereof along with FTP and SSH. It has done so for 3 years outside any firewall. For the last 300+ days it has withstood attacks (over 3.5 million without counting pings) in a global challenge from 184 countries without breach. It was also the only product to withstand a $10K hacking challenge at Defcon(R) in their 17 year history. With Fortress™ you get the equivalent of these products all in one:

- DDos Protection
- WAF (Webserver Application Firewall)
- HIDS (Intrusion Detection)
- Ransomware & Malware Protection
- End Point Security
- Social Engineering (Phishing) Protection
- Server Breach Security / Firewall
- **AND** Autonomous Operation

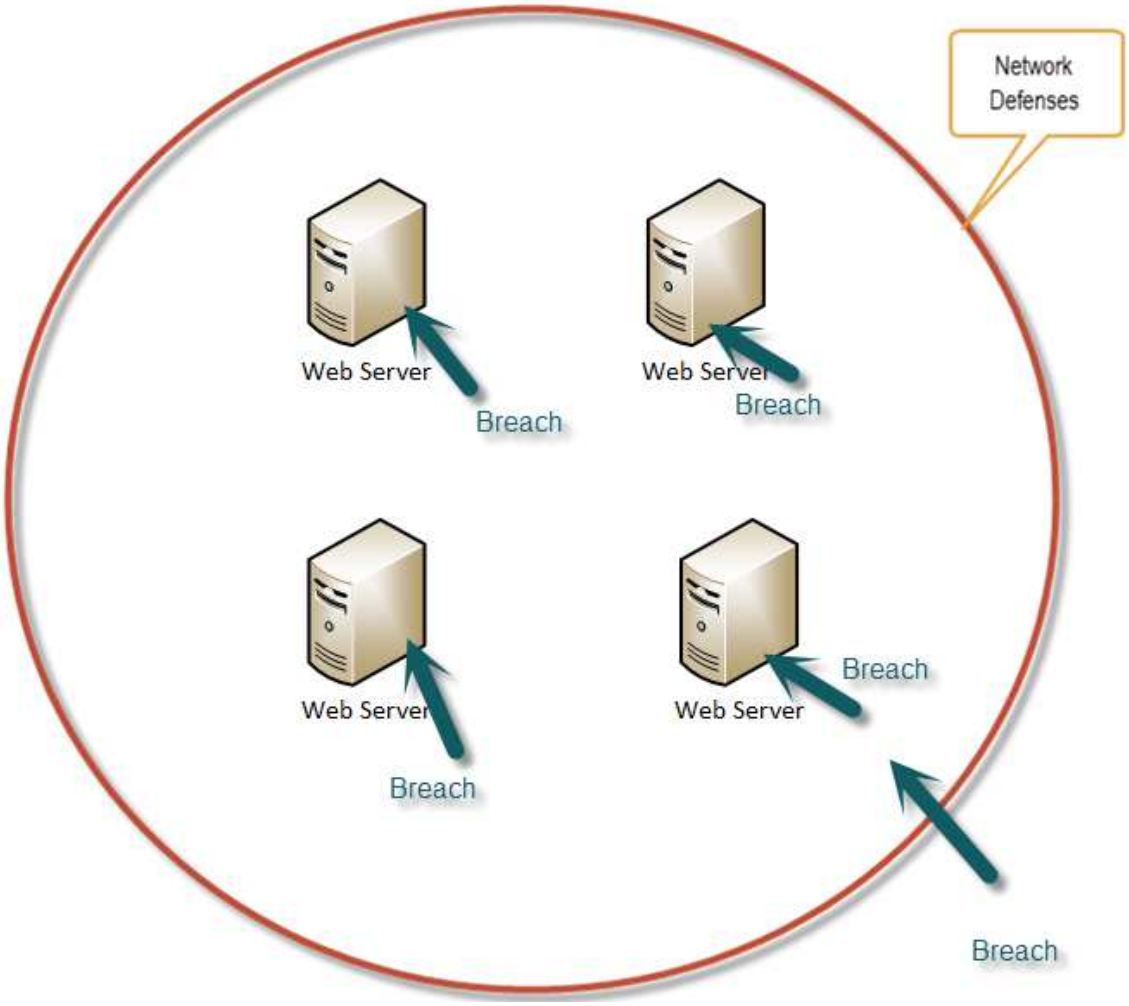
These are all integrated into a single product from one vendor for a fraction of the cost of separate purchases. You also save on people because Fortress™ only calls for help from humans if enough of its defensive layers are breached. We have never gotten the call, except for testing. Fortress™ installs in 15 to 45 minutes (depending on server speed) from a file small enough to send through email.

WHITE PAPER

# Development of Server Breach Defenses - Fortress™

Currently, if malware is successful in breaching the network it can then move horizontally from server to server, infecting them all. There has to be a better way, we thought at Secure Web Apps.

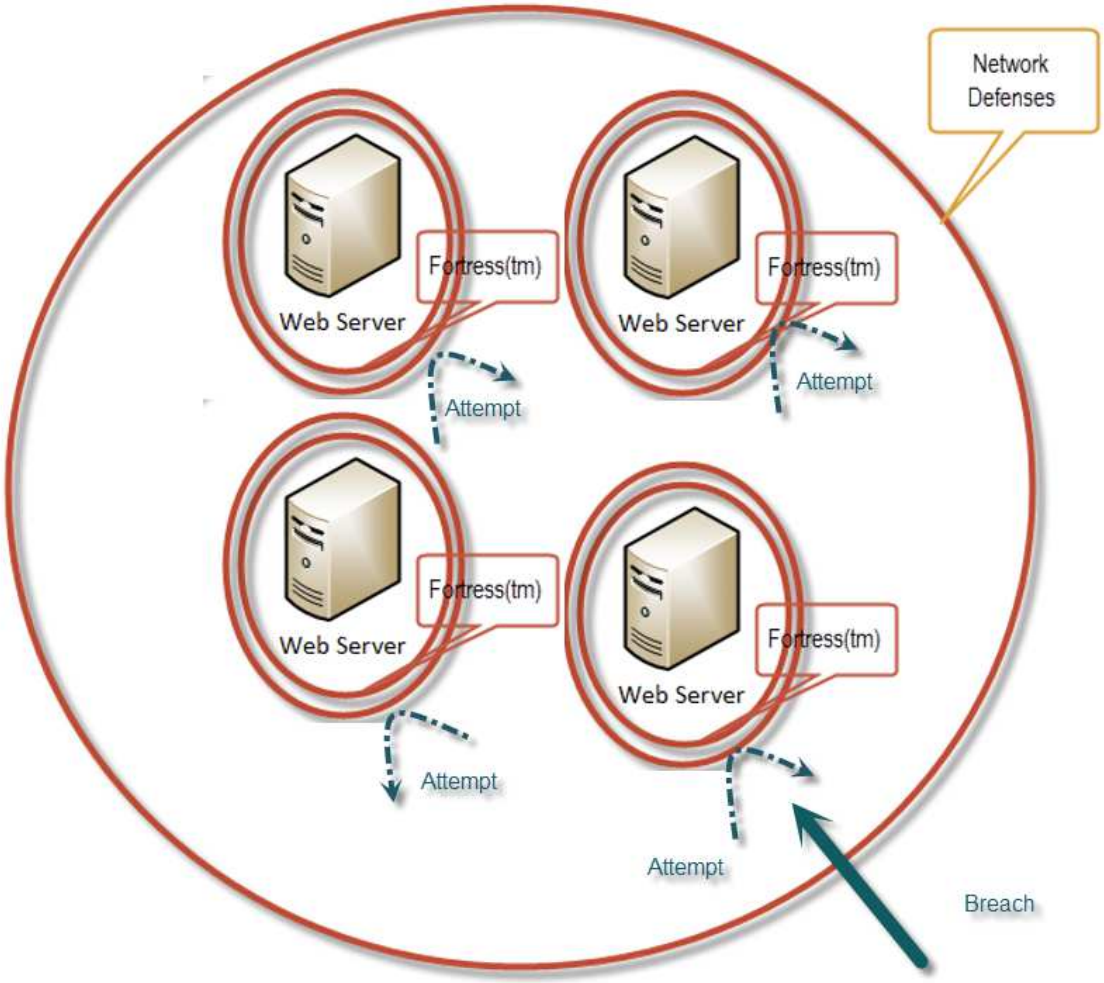
WITHOUT FORTRESS




What if each web-server was a mini-fortress, protected in its own right and secure from the rest of the network in the case of compromise of either the network or other devices upon the network? We picked the LAMP stack servers of Ubuntu and Debian. Our design goal was to continue functioning within a totally compromised network:

WHITE PAPER
Development of Server Breach Defenses - Fortress™

WITH FORTRESS




We began work fortifying our servers using multi-layered defenses. The idea behind this being that if a bad-actor was successful in breaching a layer of the defenses, that they would only find another layer awaiting them. Something like this:

WHITE PAPER
Development of Server Breach Defenses - Fortress™

Example of Defense in Depth

If a bad-actor starts defeating the outer layers, a human is alerted to help. Otherwise defenses are automated. Except for testing, we have NEVER received an alert. This means that with Fortress™ you don't need as many security staff to monitor servers it is on. And good staff are in short supply.

We began our work on servers that were outside the network firewall. When a server firewall was first brought up, we measured hacking attempts at the 10K / day level *on a brand new server*! As we added more security, we went to the web and began trying various hacker tools against our defenses to no avail. We also started researching all the reported attacks around the world that disclosed attacker TTP (tactics, techniques and procedures). We began playing those against our defenses and, if they would work, tightening our defenses. Soon we found that none of them were working against the defenses.

Disbelieving our own results, we looked for a hacker of military or military-grade systems. We found one who was once observed hacking a tank from his cell phone. The military hacker had 15+ years of experience hacking. He has worked for various government contracts and agencies involving network engineering, forensics, network defense, offensive security, and pen testing. He currently holds various industry certifications (CISSP, CASP, OSCP, OSWP, RHCE, Cloud+, Security+, Mobility+…) He also creates and teaches Network Defense, and Offensive Security classes for a fortune 500 company between pen testing engagements and network security engineering work.

We asked him to "beat the door in" of our server. The result: "This particular host is a hard target and so long as software remains updated and user web applications are reviewed and controlled, it will likely remain a hard target". In English, he couldn't get in.

Security threats are constantly evolving so we still weren't satisfied. We began looking at our product (by now we had named it Fortress™) and thought about security over time. Everyone knows that security degrades overtime due to new threats and due to human fallibility. So we began working on a new feature to ensure that Fortress remained secure. So one part of Fortress™ to secure the server and another to keep the server secure. Fortress™ also alerts the administrator and management when anomalies are detected.

So now we have Fortress™ guarding our servers. Remember that environment of 10,000 hacking attempts/day. We continued to see over 24 million attempts over a 2 and 1/2 year period! So just in case, we were viewing an anomaly we went to another server in a completely different network. To help the hacker's find the server, as this one sat behind a firewall, we put up a rather interesting website or honeypot as it were:

And if a link was clicked upon, one got an apparently encrypted page:


We left the server with these web pages for two weeks and measured over 34,000 hacking attempts, most from China, Ukraine and Bosnia.

Then we added Fortress™ to the server containing the above website and we measured ZERO successful hacking attempts during the next two week period.

Still don't believe us? We put together a target server containing Fortress™ without anything of value on it. It contains a target website. As of this writing, the target server has been attacked as part of a global challenge over 3.5 million times from over 184 countries out of 196 total and over 305 days WITHOUT SUCCESS! How many other vendors challenge the whole world to hack their product? You will find up-to-date details of our challenge on our website at: SecureWebApps.com . You may wish to take the challenge yourself!

After awhile of watching the challenge, we decided to test Fortress™ further. We took it to DefCon(R) and offered $10,000 for anyone to hack it. No one could. In fact it is the first product in the history of DefCon(R) that wasn't hacked when a challenge was issued. Next we took it to several military red teams and have heard unofficially that they couldn't get in. While this was going on, several red teams from Fortune 100 firms had a go at Fortress™ as well and failed to breach its defenses. It has also been through another challenge at another security conference and another military red team has been invited to try Fortress™.

Meanwhile we continue to advance the defenses. While the military red team attacks were occurring, we rebuilt our servers and upgraded Fortress™ to version 2.0 which uses knowledge from the millions of attacks against it to strengthen its defenses. Once you license Fortress™ you will continue to get

updates to defend against new threats and even better against old threats. We provide support as well as tiered pricing. We have also extended this technology to the Linux desktop in our DrawBridge™ product. We are also hard at work on our Moat™ product to protect Windows workstations from Ransomware and Phishing attacks.

If you aren't using Fortress™, why not try it today? We are happy to arrange a no-cost trial in your environment. Want Fortress™ in a cloud environment? Try our Managed Secure Web Services.

Oh, did we mention that Fortress™ deploys in 15-45 minutes (depending on your server speed) from a program contained in an email?