

EQUIFAX PAIN



Equifax suffered from one of the most damaging cybersecurity breaches ever: 143 Million Americans' personal information compromised.

Get the facts and learn how to protect your company.

PROBLEM OVERVIEW

- » Equifax suffered from one of the most damaging cybersecurity breaches ever: compromising 143 Million Americans' personal information.
- » Equifax CIO and CISO "retired" from the company on 15 September 2017.
- » The Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB) are both investigating the incident.
- » At least two Congressional hearings are scheduled.
- » Insider trading investigation occurring now on three top Equifax executives.
- » Dozens of class action lawsuit has already been filed.
- » Cybercriminals exploited a US website vulnerability - Apache Struts CVE-2017-563, used by most F500s, a patch was available a few days after discovery but not applied.

THE SOLUTION: UNIKERNEL SECURITY

✓ Single Process

Linux and Windows are both multiple process systems that were designed decades ago and could not envision the cloud environment we live and work in today. Unikernels are single process systems. By design they can **not** run code that was not intended to run. Shell code exploits, also known as remote code execution exploits by definition do not work on unikernels.

No Users

When your website boots up you not only have remote code execution in place but you have tens of potential users that can login to execute said code (and they are always "bad users"). Unikernels have **no** users and **no** remote code execution - it's designed that way. No more Equifax incidents - not on your watch.

No Shell


The shell is a 40 year old construct designed in a different time period. Today in Silicon Valley engineers are used to working with tens, hundreds, thousands or even more systems at a time. The shell is an antiquated concept that only lends it's hands towards those who want to do your company harm. There are no shells on unikernel systems - they simply don't exist. They can not exist. This is by design.

Reduced Attack Surface

Compared to a bloated Linux system that has hundreds of millions of lines of code with drivers for everything from USB drives to audio drivers to libraries such as libxslt that have FTP servers embedded in them unikernels are refreshingly small. Sometimes as small as 10Mb or maybe even kilobytes. Sometimes smaller then this document.

Less code equals Less exploits. Protect yourself and hop on the future cloud.

CONTACT US

 (888) 726-4283

 sales@deferpanic.com

 www.deferpanic.net

THE ENTERPRISE SERVICES UNIKERNEL COMPANY

DeferPanic is the only production ready, fully managed unikernel platform in the industry today.

We save companies money on infrastructure and ops cost while at the same time taking real proactive security measures to limit attacks.