**MinSec Cookbook - Linux Servers hosting Medium or High Risk Data**

**Before you begin:**

* Complete a Risk Assessment
* Retire any unneeded servers

1. **Install** [**BigFix**](https://uit.stanford.edu/service/bigfixforservers) 
   1. Subscribe to the service as a ‘BigFix for Servers Administrator’ by submitting a [Help ticket](https://stanford.service-now.com/services?id=get_help&cmdb_ci=84d7c11a1374e20063eadf82e144b05b).
   2. Install [BigFix for Linux Servers](https://uit.stanford.edu/service/bigfixforservers/linuxservers).
2. **Install the** [**Splunk Universal Forwarder**](https://uit.stanford.edu/service/splunk) 
   1. Request a Splunk account by opening a [Help ticket](https://stanford.service-now.com/services?id=get_help&cmdb_ci=c9c7811a1374e20063eadf82e144b0f4).
   2. Install [Splunk Universal Forwarder for Linux Servers](https://uit.stanford.edu/service/splunk/linux-server).
3. **Request a** [**Privileged Access Workstation (PAW)**](https://uit.stanford.edu/service/paw)
   1. PAWs are only required for administering High Risk servers and applications, and for administering Carbon Black Protection.
   2. Request a PAW by opening a [Help ticket](https://stanford.service-now.com/it_services?id=sc_cat_item&sys_id=0c6cccd613bce2008a9175c36144b026).
4. **Install** [**DUO for Linux servers**](https://uit.stanford.edu/service/webauth/twostep/duo_ssl)**.**
   1. Request your API keys and Duo API hostname by opening a [Help request](https://helpsu.stanford.edu/helpsu/3.0/auth/helpsu-form?pcat=twostep).
   2. Deploy Duo to your systems.
5. **Install** [**File Integrity Monitoring (OSSEC)**](https://uit.stanford.edu/service/ossec)
   1. [Deploy OSSEC using BigFix](https://uit.stanford.edu/service/ossec/install-bigfix).
6. **Configure your host-based firewall**
   1. Configure your firewall in default-deny mode, and permit only the minimum necessary services.
7. **Regularly scan for vulnerabilities with** [**Qualys**](https://uit.stanford.edu/service/qualys)**.**
   1. Request a Qualys account by opening a [Help ticket](https://stanford.service-now.com/it_services?id=sc_cat_item&sys_id=c0ec401a13bce2008a9175c36144b04b).
   2. Sign in to the [Qualys console](http://qualysguard.stanford.edu/) to manage custom scans and reports.
8. **Review your compliance with the other** [**MinSec standards**](https://uit.stanford.edu/guide/securitystandards)**.**
   1. Apply high severity security patches within seven days of publish, and all other security patches within 90 days.
   2. Review and update your system inventory records in [NetDB](https://uit.stanford.edu/service/netdb) and SUSI.
   3. Enforce [password complexity requirements](https://uit.stanford.edu/service/accounts/passwords/quickguide), and review your existing admin accounts and their privileges.
   4. [Physically protect](https://uit.stanford.edu/guide/securitystandards/faq#physical_protection) your server
   5. Implement [PCI DSS](https://www.pcisecuritystandards.org/security_standards/), [HIPAA](http://hipaa.stanford.edu/), [FISMA](http://csrc.nist.gov/groups/SMA/fisma/controls.html), or [export](https://acp.stanford.edu/compliance/export-controls) controls, as applicable.