CFEngine

CFEngine is an enterprise software solution that ensures your endpoint software and firmware is securely configured, patched and updated - dramatically reducing the attack surface from data breaches. CFEngine already ensures the security of systems and devices for organizations such as Samsung, Deutsche Telekom, DirecTV, Comcast, Intel, JPMorgan Chase and the US Navy.

Endpoint device security configuration management

Extending the perimeter

With the increasing connectedness of devices extending beyond the corporate firewall, the need to protect assets outside the network has reached new heights. The unique challenge lies in that these assets are not only outside the supposed "protected perimeter," but they can be very heterogeneous in form. They are not simply server systems. These devices span across the imagination, from industrial control systems to medical devices -- and beyond. The heterogeneity coinciding with the increase of interconnectedness greatly expands the attack surface.

The endpoint devices are naturally the most vulnerable in the technology stack from the data center to the networks that connect them, and malicious attackers are well aware of this. And the more critical the device is, the more centrally important it is to have each endpoint adopt security self-governance within the device itself to protect it from the many attack vectors that exist.

The most common attack vectors that have driven many of the recent well-publicized data breaches include:

- Insecure encryption protocols (SSL, TLS, keys)
- Open network ports of unnecessary or unused services
- Default user accounts/ passwords
- Insecure user privileges and file permissions
- File changes without detection fails to provide proper response to potential low-level hacks and exploits

Base-level security hardening and compliance

Due to its lean agent footprint, CFEngine can provide base-level security hardening from within your devices rather than relying

Our customers

Chevron SAMSUNG comcast. intel JPMorganChase DIRECTV

CFEngine

Endpoint device security configuration management

on either a corporate network or Cloud-based security proxying. Agent-based endpoint security provides a much more robust approach in protecting your devices from security breaches. With CFEngine, an enterprise security agent will continually ensure device integrity from within and its autonomous nature means it will continually execute whether or not there is network access.

While CFEngine can provide automated software/firmware updates and patching (please see datasheet), it can also provide your organization with security configuration management within the device itself:

- Harden and secure encryption protocols
- Remove unnecessary services to secure network ports
- Detect and correct any default user accounts/passwords
- Properly configure and manage user privileges and file permissions
- Detect, audit, and remediate any file changes -- providing a proper response to a potential exploit

According to the Center of Internet Security, **80%-95% of known vulnerabilities can be eliminated** by implementing a solution adhering to such compliance standards such as CIS Benchmarks. Other legal and regulatory requirements include HIPAA for healthcare, NERC for energy, SOX for accounting, and PCI for payments processing.

The Internet of Things have yet to standardize on a set of regulatory requirements. While these are in the process of being defined, according to SANS Institute, "new frameworks, legislation or regulations will increase reporting burdens on security managers."

CFEngine provides security managers with a comprehensive and flexible reports dashboard, policy compliance, and inventory management reports to provide rapid intelligence on your fleet of devices and enable regulatory and compliance reporting.

Device requirements

- Linux and UNIX-like systems. Please contact us for additional platform support
- 25 MB RAM Available
- 50 MB free disk space
- 400 Mhz CPU

CFEngine, Inc
contact@cfengine.com
470 Ramona Street
Palo Alto, CA 94301
(650) 257-0233