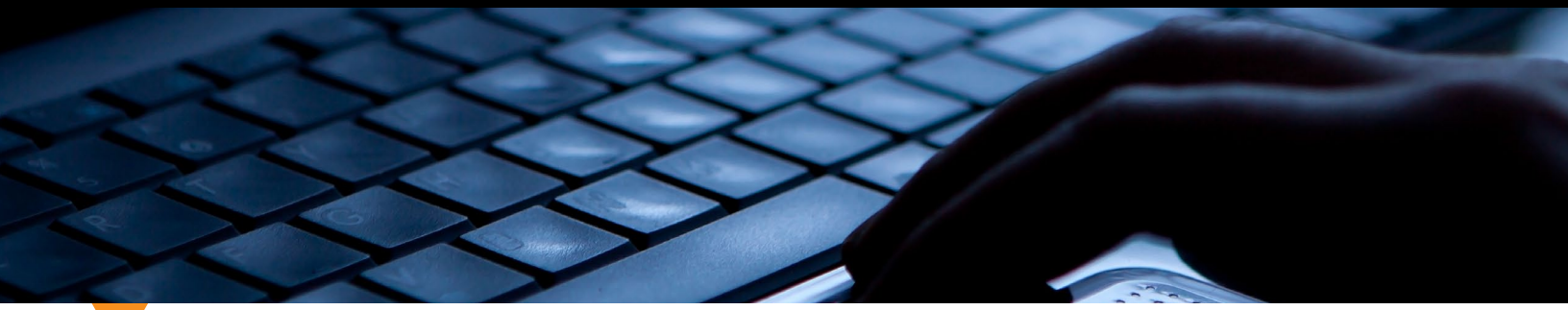
Using a Layered Approach to Secure Against Insider Threats

Combining Security Best Practices with Common Sense



IT security spending is projected to reach $86 billion in 2016. But what percentage of that will be spent on protecting organizations from themselves?

An organization's relative success in securing against the external threat does not necessarily mean it is equipped to protect against weak points inside the organization. Insiders have better knowledge of the security practices the organization has implemented – and their potential weaknesses. They are granted access where outsiders aren't, putting them closer to sensitive resources. In 2013, Forrester Research estimated that insider threats accounted for as many as 61% of total attacks on worldwide organizations. Whether stemming from a malicious, carefully planned insider attack or a careless employee in a hurry, the insider threat is one that needs to be approached in the same way as any information security problem – with a layered approach and awareness of that organization's individual risk profile and needs. What sets the insider threat apart from the external attacker, however, is that the people putting the organization at risk aren't necessarily recognizable as enemies – they are employees, and they are not all malicious, which means data needs to be protected without impeding day-to-day productivity. Successfully protecting against insider threats is a matter of policy and employee awareness as much as sophisticated technology.

Organizations Know Their People. Wave Knows How Their People Use Their Data.

An individual organization's culture and risk profile will provide the context to know what physical security policies to implement, and how to build awareness of basic security best practices that address the human, low-tech element of insider threats.

This is a critical part of protecting against insider threats, but it is insufficient as a stand-alone solution – without the technology to enforce these policies, there is nothing to stop users from causing a data breach, be it intentional or accidental.

Programs like CERT's Common Sense Guide to Prevention and Mitigation provide a comprehensive outline for dealing with all aspects of insider threats, and are a useful starting point for organizations looking to build their internal defenses. Funded by Carnegie Mellon University's CyLab, CERT offers guidance on both the non-technological and technological security processes every organization should consider when combatting insider threats.

With the right cultural and technological tools in place, organizations can achieve a layered system that protects data equally against internal and external attacks. In fact, the right technology can protect against both – which is an important advantage when considering limited budgets.

wave®

Flexible but Comprehensive

The surest way to keep sensitive data from being breached would be to lock down enterprise resources completely – ban sharing, ban mobile devices of any kind, ban email, uploads, printing, external storage.

Since complete lock-down isn't feasible, data loss prevention (DLP) is one of the most important tools for an organization to have in its arsenal. A good DLP tool will offer customizable, data- and user-aware policies that prevent sensitive information from being shared in ways likely to expose it – email attachments on mobile devices, unsecured flash drives, wireless hot spots – but doesn't stop productivity. DLP, combined with good non-technical security protocols, will remind forgetful users of best practices and block malicious users from intentional mischief.

Add encryption for all endpoints (which is required for blocking external threats, as well) and role-based identity and access management (IAM), and you've gone a long way towards successfully protecting against insider threats.

Following the guidance of advisory organizations like CERT will help organizations ensure they have all the right boxes checked. Complementing an organization's compliance with CERT's non-technological process guidelines, Wave's solution enables organizations to:

- Consistently enforce policies and control
- Know its sensitive assets
- Implement strict password and account management policies and practices
- Institute stringent access controls and monitoring policies on privileged users
- Enforce separation of duties and privilege
- Institutionalize system change controls
- Use logs to monitor and audit employee actions
- Implement a secure recovery process
- Close the doors to unauthorized data exfiltration

Defending Against Insider Threats with Wave

Wave protects your organization against insider threats in the following ways:

Data Loss Prevention

Featuring a single console/single agent architecture and comprehensive, customizable policies, Wave's Data Protection Suite maps, tracks, and prevents leakage of sensitive data. Comprised of seven products that work independently or in combination, the Data Protection Suite is an award-winning DLP solution used by global companies in all major verticals. Policies are created by IT and enforced by the Data Protection Suite based on customized, pre-identified keywords and user roles. For instance, if an employee tried sending a spreadsheet with customer credit card data to someone outside the organization, they would receive a pop-up that their action had been blocked. If they tried sending the same spreadsheet to an approved user, but the recipient attempted to open the spreadsheet on a mobile phone or other unapproved device, he or she would receive a notice that they had been sent confidential data that could only be viewed from a secure endpoint.

For insider threats, consider the following elements of the Data Protection Suite:

- **INSPECTOR**
  Inspect, classify, filter and block leakage of sensitive content and data
- **PROTECTOR**
  Prevent sensitive data leakage through physical ports, external storage media and devices (USB, DVD, Firewire).
- **MOBILE PROTECTION**
  Limit sharing of data on mobile devices with content-aware, role-based policies.

Encryption

In addition to complying with data protection regulations, encrypting all data on all devices gives organizations control over data wherever the endpoint goes – if a disgruntled employee walks off with a laptop, you can remotely perform a crypto-erase on that laptop's hard drive next time the employee connects to the Internet. Hardware encryption also cannot be turned off locally, meaning that employees cannot bypass security measures.

Wave offers several types of fully-managed encryption, enabling the organization to choose the one that best fits its needs. Whether based in hardware or software, on 30 endpoints or 300,000, Wave's encryption options provide easy compliance with data protection regulations and the peace of mind that comes with knowing data is protected wherever it goes, inside the organization or out.

ERAS FOR SELF-ENCRYPTING DRIVES

Wave's EMBASSY® Remote Administration Server (ERAS) provides complete, remote management for the industry's most secure, easy-to-use, and cost-effective encryption method – the self-encrypting drive (SED). Chosen increasingly by organizations of all sizes, the SED automatically encrypts all data written to the drive, providing complete protection for data. Because encryption takes place in the hardware of the drive itself, the performance of the operating system is not affected, and the user is not frustrated by a slow computer. SEDs are sold by all major drive manufacturers and are comparable in price to drives without encryption. When managed by ERAS, SEDs provide best-in-class encryption with remote deployment, management, decommissioning, and secure audit logs. Government and government-affiliated organizations should consider using CAC/PIV card authentication to provide user access to SEDs.

WAVE CLOUD

The only cloud-based encryption management service of its kind, Wave Cloud provides much of the same functionality of ERAS, but does not require the maintenance of on-site servers. Wave Cloud also manages software encryption tools native to the operating system, such as BitLocker and FileVault. Scalable, always up-to-date, and available on a subscription basis, Wave Cloud is the fast and easy way for organizations to comply with regulations and deploy best-in-class encryption.

ERAS FOR BITLOCKER®

ERAS offers complete management for Microsoft's native encryption feature BitLocker. By storing encryption keys in hardware, BitLocker is more secure than software encryption alone, but not as strong as complete hardware encryption like the SED. For organizations looking to strengthen security using what they have, BitLocker is a good choice, and Wave's ERAS product makes it a complete solution with remote deployment, management, and audit logs.

wave®

Using a Layered Approach to Secure Against Insider Threats

Identity & Access Management

One way to minimize the exposure of sensitive data is to allow access only to those who need it. This is an important distinction to make, but equally important is how it is enforced. How do you determine if the person requesting access has the required authorization? Many security-minded organizations use two-factor authentication, meaning some combination of something you have, something you are, and something you know (i.e. a smart card/token, a biometric, and a password). Passwords alone are unfortunately still the primary authentication method for many organizations, which not only makes these companies more vulnerable to hackers, but also makes unauthorized access inside the organization easier. Whether sharing passwords without permission or stealing them (shoulder-surfing, key logging, post-it theft), authenticating with passwords alone can all too often lead to employees gaining access where they shouldn't.

- **WAVE VIRTUAL SMART CARD**
  Even if passwords are still a part of the authentication story, organizations would be well-advised to follow best practices and deploy multi-factor authentication. Unfortunately, this can be expensive and complex - imagine acquiring, distributing and maintaining enough smart cards, tokens, or fingerprint readers to account for every employee, plus some extra when the new hardware is lost. Wave Virtual Smart Card, however, transforms the device into the token or smart card, meaning there is no new hardware to be purchased; it's significantly harder to lose (users have to lose the entire laptop); and the authentication process requires no user interaction, speeding productivity. The end result? IT knows who is accessing sensitive resources, with what device, and they can prove it with secure audit logs.

- **WAVE ENDPOINT MONITOR**
  Malware can be planted and go unnoticed for weeks, causing damage to the network, stealing sensitive information, key logging passwords, and destroying hardware. Using the same secure hardware as Wave Virtual Smart Card, Wave Endpoint Monitor ensures endpoints are healthy and free of malware each time they boot up. Wave Endpoint Monitor collects and compares data from secure hardware storage locations as the machine boots, and alerts IT when it detects anomalies in this data that could indicate the presence of a rootkit or malware. Analyzing the data in pre-boot means IT can stop infected machines from loading and compromising the network.

Collaborating for Security: Working ***with*** Employees, Not ***Against*** Them

For every employee that poses a threat to an organization's security, there are many more that don't. Creating an atmosphere of roadblocks and distrust isn't in anybody's best interest. Wave's encryption and IAM products are silently in place at all times, enforcing policies without disrupting work flow. Wave's DLP products are designed to alert users when they are attempting a potentially risky action, and block the action if necessary, which reinforces user awareness of security best practices.

Although in many ways they present a liability, an organization's employees are also its biggest asset. Wave offers technology that, when partnered with the right no-tech policies, can protect organizations from the inside out.

Wave Systems is a leading provider of client and server software for hardware-based information security, enabling organizations to know who is connecting to their critical IT infrastructure, protect corporate data, and strengthen the boundaries of their networks.

For further information please visit www.wave.com or contact us at sales@wave.com.

03-000380/version 1.01 Release date: 01-17-2014

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238
(877) 228-WAVE · fax (413) 243-0045
www.wave.com

wave®