opentext™

Flash Point Paper

Breach Defense: Keys to Keeping Data Safe

Data breach impacts are devastating. Not only do you lose business and the trust of your customers, you can take an enormous direct financial hit.

While actual costs vary by organization, analysts estimate the cost at $148 per record breached.* Those costs escalate dramatically the longer a breach goes undetected. Such was the case with the recently discovered Marriott Starwood reservation system breach that had been compromised for four years, during which time 5 million guests' personal data had been exposed.

To protect your organization, it's helpful to understand the typical steps cybercriminals take to carry out a data breach. First, they research their target, looking for weaknesses in the environment they can exploit. Next, they stage the attack. This step can take on many forms with multiple attempts over a long period of time until the attacker gains the desired access to the network. It might include a range of social engineering efforts, such as phishing, malware spam, deceptive phone calls, and more. Those efforts could be combined with direct attacks on infrastructure weaknesses using a variety of methods, such as SQL injections, session hijacking, and vulnerability exploitations. Once attackers successfully gain access, they quietly steal personal data and other valuable confidential information until discovered and stopped.

The best breach defenses include four key protective capabilities:

- Automated patching
- Endpoint security

- Encryption
- Mobile security

Automated Patching

The more you can minimize and eliminate vulnerabilities in your infrastructure, the harder it becomes for attackers to breach your environment. Cybercriminals often seek the path of least resistance by trying to exploit well-known vulnerabilities. You can easily block those efforts by following the well-known best-practice of keeping all your systems and software patched with all the latest security updates.

** Ponemon Institute. "2018 Cost of a Data Breach Study." July 2018.* **www.ibm.com/downloads/cas/861MNWN2**

The Best Breach Defenses Include Four Key Protective Capabilities:

- **Automated patching:** *Automatically detect, inventory, and give you the patch vulnerability status of every laptop, desktop, and server connected to your network with a auto-discovery solution.*
- **Endpoint security:** *Enforce centrally managed security policies on each of your endpoints with strong firewalls, application controls, removable media governance, and protection against potentially infected downloadable files.*
- **Encryption:** *Use full disk encryption that includes support for (FIPS) 140-2 Level 2 and Level 1 encryption modules, centralized key management, transparent encryption, background encryption and decryption, and centralized pre-boot authentication override in case users forget their passwords.*
- **Mobile security:** *Simplify your mobile security efforts with strong centrally managed controls can significantly bolster your breach defense strategies.*

But too often organizations don't keep their environments protected with the latest available patches. Usually, this is because without the right tools, patching every system and piece of software in a timely manner can be a complex ongoing and time-consuming undertaking. To eliminate the complexity and time drain, you need an auto-discovery solution that can automatically detect, inventory, and give you the patch vulnerability status of every laptop, desktop, and server connected to your network. Next, you need a patch management solution that can quickly and automatically update each of those endpoints with the appropriate and most recent security patches. That includes also being able to report back to you the success or failure of those patch efforts, so you can be certain that every endpoint has been successfully patched and protected.

Endpoint Security

Since attackers often focus on end-user interactions as a common breach point, it makes sense that a key aspect of breach defense is to bolster endpoint security. This includes having centrally managed security policies enforced on each of your endpoints with strong firewalls, application controls, removable media governance, and protection against potentially infected downloadable files. Endpoint protection needs to be at the driver-level, so you have the power to restrict access to those parts of the system with the highest level of privileges.

Encryption

Despite your best efforts, your organization can still become victim to a data breach. When this happens, one of the best ways to make sure your data doesn't get compromised is to leverage full disk encryption on your endpoint devices. Full disk encryption renders your confidential data unreadable to unauthorized individuals. If you're not proactively encrypting end-user devices ahead of a breach, you should at least have a remote web-based management capability to encrypt your users' devices when a breach is detected. A few things to look for in full disk encryption include support for (FIPS) 140-2 Level 2 and Level 1 encryption modules, centralized key management, transparent encryption, background encryption and decryption, and centralized pre-boot authentication override in case users forget their passwords.

Mobile Security

Enforcing security on mobile devices can be a challenge. That's why they can be a favorite attack vector for cybercriminals. A solution that can simplify your mobile security efforts with strong centrally managed controls can significantly bolster your breach defense strategies. In today's BYO environments, a mobile application management (MAM) solution lets you balance your need to secure your corporate assets while minimizing the impacts those necessary controls have on your mobile users' productivity and experiences. This requires a solution that enforces security controls at the application level in a way that creates a separation between the user's personal assets on the mobile device and the corporate assets on the device using technology such as containerization.

Bolstering Breach Defense

To avoid the financial and reputational devastation that cybercriminals can inflict, OpenText™ ZENworks solutions unify the key capabilities you need to strengthen your data breach defenses while minimizing your effort in employing those defenses. OpenText™ ZENworks Patch Management automates the process of discovering, monitoring, and updating the patch state of all your Windows laptops, desktops, and servers. OpenText™ ZENworks Endpoint Security Management gives you fine-grained, policy-based control over all your Windows laptops, desktops, and servers, including advanced firewall protection, application controls, wireless security, port controls, and robust storage device controls. OpenText™ ZENworks Full Disk Encryption makes it easy to automatically protect data stored on your laptops and desktops. OpenText™ ZENworks Mobile Workspace gives you a best of breed MAM solution that empowers you to secure and control corporate data and applications on users' personal devices without impacting those users' personal use and files.

For more information on how OpenText™ can unify, simplify, and strengthen your data breach defenses, visit **www.microfocus.com/en-us/products/zenworks-endpoint-security-management/overview**.

Learn more at
www.microfocus.com/opentext

Connect with Us
OpenText CEO Mark Barrenechea's blog

opentext™