Data Security for the Way People Work

How to achieve data protection and threat prevention while enabling productivity, collaboration and a great user experience
Data security is at the top of the priority list for most organizations, as well it should be. Threats have never been more numerous, more varied or more dangerous. Phishing attacks, malware, ransomware, BIOS attacks and advanced persistent threats (APTs) are multiplying relentlessly (see sidebar). The dangers of data loss, extortion and identity theft are real. The global average cost of a data breach is $3.62 million USD, according to Ponemon Institute⁠¹.

The climate of increasing regulation reinforces the imperative to keep data safe. Failure to do so can result in severe penalties. In health care, for example, fines for violating the rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), a U.S. privacy act, routinely range from tens of thousands to multiple millions of dollars. Meanwhile, the General Data Protection Regulation (GDPR) of the European Union (EU) went into full effect on May 25, 2018. As of that date, organizations that fail to protect the personally identifiable information of EU citizens are subject to fines of €20 million or 4% of global turnover, whichever is greater.

The way people work magnifies the risks of security threats. Mobility is the norm for employees of all kinds, who expect to labor productively and collaborate with co-workers wherever they happen to be. The devices carried by members of a mobile workforce may be laptops, tablets or smartphones. A device in the wrong hands can lead to devastating losses of personal data and intellectual property. And users aren’t shy about sharing information, whether on e-mail or personal cloud services: 72% of employees are willing to share sensitive, confidential, or regulated information⁠², a practice that can easily expose data to bad actors.

In this challenging climate, IT leaders must implement security strategies that keep data safe while enabling productivity and collaboration without compromising the user experience. Security policies and solutions that are cumbersome, such as complex and arduous authentication methods or lengthy virus scans, will discourage employees from using their devices – or will lead them to circumvent the security measures entirely. In fact, 41% of employees say they will go around security methods that get in their way⁠³.

Current defenses fall short

In the quest to keep data safe and in compliance, there are many defensive measures – and many security products – that organizations might employ. It is possible to purchase each of these from a different provider. In 2017, 25% of security professionals said they used products from 11 to 20 vendors, and 16% said they used products from 21 to 50 vendors⁠⁴. That approach, however, is Continued on page 4

---

1 Cost of Data Breach Study, Ponemon Institute, 2017.  
4 Cisco 2018 Security Capabilities Benchmark Study.
inefficient at best. Different products must be licensed from different parties, then deployed, maintained and updated from separate management consoles. It’s a costly and time-consuming process that could result in the use of products that are out of date, which could in turn expose an organization to attack.

**Endpoint security**

In any network, endpoint protection is critical — research has found that 95% of breaches begin at endpoints. Because of the vulnerability of mobile devices and the willingness of mobile users to share data, today’s mobile workforce makes endpoint protection even more important — and more difficult to achieve. Authentication, encryption and advanced malware prevention are three pillars of endpoint security.

- **Authentication.** Single-factor authentication such as a password is typically not sufficient; two-factor authentication is essential. Typically, two-factor authentication utilizes two of these three factors: Something known to the user, such as a password, something the user has, such as a hard or soft security token, and something personal to the user, such as a fingerprint or other biometric.

- **Encryption.** Although the use of encryption technology is widespread, not all implementations are equally effective. File-level and dual-level encryption have distinct advantages.

  - File-level encryption, as the name suggests, encrypts files individually with a separate encryption key, rather than encrypting an entire hard drive with a single key. In case of theft, hackers would have to decrypt thousands of files, each with a different encryption key, rather than utilizing a single key to unlock all the files. Also, when files are sent from one location to another — via email, for example — they remain encrypted with file-level encryption. This is not the case with disk-level encryption.

  - Dual-level encryption is the practice of encrypting data twice. For example, a file could be encrypted with two different keys. This practice multiplies the effectiveness of encryption protection. Even if hardware-level encryption should be compromised, the second layer of encryption will protect the data, significantly decreasing the probability of a data breach.

- **Advanced malware prevention.** Traditional anti-malware solutions have relied on signatures, or telltale byte sequences, to identify malware. Signature-based anti-malware software can grow to enormous size as it accumulates new malware signatures. The very size of the program causes it to degrade overall system performance, something that users can ill afford as they strive to remain productive.

---

5 Verizon Data Breach Digest, 2017.
Ransomware, WannaCry

Organizations are under siege from ransomware and other threats

Data security threats are widespread and constantly evolving to higher levels of sophistication. Malware that was once easy to spot is increasingly difficult to detect. Phishing attacks continue to deliver a number of different kinds of malware from bad actors who send email messages containing clickable links to unsuspecting users. When they click on the links, malware is installed on their systems. Even knowledgeable users are misled by some of the newer attacks. Social engineering, for example, attempts to lure users into exchanging information that can be used to breach a system and install malware. Often, social engineering methods appear to be legitimate, even to the trained eye, because they incorporate valid information relating to a user found elsewhere.

BIOS attacks can be especially pernicious. By infecting the core software of a computer, such an attack delivers the device to the complete control of a bad actor. And because the malware resides in the BIOS, it evades virus scans and can survive even after the device's operating system is wiped clean and re-installed. It is possible for malware to be introduced into the BIOS at some point in the microprocessor supply chain, making manufacturing integrity particularly important.

Lately, there has been a surge in ransomware, which encrypts data until ransom is paid by the victim. Ransomware attacks are predicted to occur every 14 seconds by the end of 2019. Damages go far beyond the ransom payments themselves and are expected to total $11.5 billion in 2019 due to loss of data, downtime, lost productivity, reputational harm and other factors. In the case of the WannaCry outbreak of 2017, ransomware was implanted by a network worm which spread rapidly, infecting hundreds of thousands of Windows systems.

For example, a user giving a presentation could suffer unacceptably slow performance should the anti-malware initiate a scan in the midst of the talk. Advanced malware prevention overcomes the problems of signature-based anti-malware by using artificial intelligence (AI) and machine learning to detect threats before they execute. This approach has very little impact on PC performance, freeing users from potential interruption and enabling users to remain productive. Perhaps most important, users will not be tempted to disable anti-malware programs that degrade performance.

Conclusion

Faced with a growing array of daunting threats and the challenge of enabling the mobile workforce, IT leaders must implement a multifaceted security strategy that focuses on the way end users work. End users are highly collaborative and frequently mobile, which exposes their systems to a wide array of security threats.

Data security is a daunting challenge. Costly data breaches are increasing in number and sophistication, and a growing list of regulations mandate that personal data be protected. At the same time, security technologies must not impede user productivity by creating cumbersome obstacles or slowing performance. If not, users might be led to disable or circumvent them.

6 Cybersecurity Ventures, Nov. 14, 2017
Since the vast majority of breaches begin at endpoints, a focus on endpoint security is critical.

A robust security strategy that includes authentication, encryption (both file-level and dual-level) and advanced malware prevention, utilizing AI and machine learning, enables an organization to keep data safe while enabling the way people work.

For more information, please click DellEMC.com/DataSecurity

Dell Data Security
The right security partner
IT leaders should look for a single provider of security technologies that both protect data and prevent threats. A vendor's portfolio should include products that:

• Protect data at work and on the move through file-based encryption.
• Control access through policy-based access control.
• Monitor data activity so administrators can easily identify unusual usage patterns or data movements.
• Protect against the latest forms of malware.

A valued partner should implement both hardware and software protection. For example, a hardware provider should, where appropriate, embed security into the devices and software it produces. And the provider should take care in the design, manufacturing and delivery processes to mitigate the risk of counterfeit parts or malware introduction.

Dell's innovative security solutions are made for the way people work, enabling efficient and secure collaboration and a better employee experience. Dell provides both hardware and software protection, reducing the number of different security vendors an organization must use. Dell incorporates its own intellectual property as well as the technology innovations of strategic partners into its products. In addition, Dell leverages its PC heritage to bring security to the hardware layer through such features as BIOS protection.

The Dell Data Security portfolio includes these products and features:

Dell Trusted Devices
• Dell offers the world's most secure commercial PCs, powered by Intel® Core™ vPro™ processors with industry-leading endpoint security solutions that include BIOS protection, data encryption, advanced authentication and next-gen malware protection options7.
• Rigorous supply chain assurance processes and procedures are architected into every commercial PC to minimize risks and help ensure product integrity.
• Dell exclusive off-host BIOS verification, available with Dell SafeBIOS, provides the ability to confirm the BIOS hasn't been tampered with and altered, which could be a sign of a highly technical and invasive attack.
• Dell also provides additional BIOS security features to ensure the BIOS, at the heart of every PC, stays protected. Should BIOS become corrupted Dell PCs have BIOS Recovery which allows a clean BIOS reinstall so the end user is back up and running.

Dell DataSafe
• Protect. Data is secure, even though it is shared via email, cloud services, FTP and portable storage devices, by employees, contractors, vendors and partners.
• Control. Administrators define parameters for who has access to what data and when, as well as how the data can be used.
• Monitor. Dell Security Management Server performs analytics on data access, activity and location, enabling administrators to spot potential security risks.

Dell Encryption
• File-centric encryption encrypts the important data on the hard drive at the file level.
• Optional dual-level capability encrypts data twice for greatly enhanced security.
• Certified by the National Information Assurance Partnership (NIAP) for use in national security systems.

Dell SafeGuard and Response powered by Secureworks
Comprehensive threat management with intelligent and prompt security decisions powered by endpoint telemetry and validated by dedicated security experts can:

• Prevent 99% of endpoint threats from contaminating your environment8.
• Detect non-malware threats already lurking in the environment and obtain an action plan for focused remediation.
• Respond to cyber incidents quickly and efficiently or even prepare in advance for the unthinkable.

© 2018 Dell, Inc. ALL RIGHTS RESERVED. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Dell, Inc. (“Dell”). Dell, the Dell logo and products — as identified in this document — are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.