Amp up your endpoint data security

Prevent threats and protect your data with Dell Data Protection | Endpoint Security Suite Enterprise

Introduction

In recent years, the number and virulence of cyberthreats have increased dramatically as attackers develop innovative ways to penetrate traditional security defenses undetected. As organizations of all sizes and industries look to strengthen their defenses, they often focus on the endpoint, with good reason: 95 percent of successful cyberattacks start with an endpoint exploit.[1]

Most endpoint protection products base their defenses on remediation, also called "clean and quarantine." This reactive approach assumes that cyberthreats will penetrate the network and therefore seeks to isolate them and minimize the damage. However, today's cyberthreats can create havoc in just minutes, so any penetration can be catastrophic. In addition, traditional defenses rely on signatures to identify threats, a method that is ineffective against zero-day threats by definition.

Security planners need a way to stop malware before it can execute. Any new technology solution must provide that protection while streamlining management.

Your organization can block malware and reduce complexity with Dell Data Protection | Endpoint Security Suite Enterprise. The solution identifies and stops zero-day and advanced persistent threats as well as commodity malware before they penetrate the network. You can simplify your endpoint security by managing advanced threat prevention, data encryption and authentication, all from a single pane of glass.

Endpoint security on life support?

If endpoint security were a hospital patient, the attending physician would be concerned. Why? Because the patient's vital signs are not encouraging:

- The **speed of successful attacks** has been increasing to the point where, in 60 percent of the cases studied, it took only minutes to compromise the victim.[3]
- At the same time, the median **time to detect an intrusion** is 205 days.[4]
- More than three-quarters of organizations say they are very likely or certain to have been infected with **web-borne malware that was not detected**.[5]

The constantly evolving threat landscape requires a level of security that far exceeds the effectiveness of the solutions currently deployed throughout enterprises, governments and institutions worldwide.

Ratcheting up the security challenge

Data breaches have become one of the most vexing problems today. You don't have to be a CEO to appreciate the damage a high-profile breach can inflict on customer loyalty, employee morale, marketplace competitiveness and brand reputation, to say nothing of your organization's bottom line. IT executives need effective endpoint security solutions to relieve their fears of a major data breach and reduce the time and money they expend on security issues.

In general, cybersecurity vendors have not met the challenge. Most solutions are based on detecting patterns and behaviors of known malware — the security equivalent of preparing to fight the last war. These legacy defenses can identify and quarantine traditional malware, but they are powerless against zero-day and new or altered exploits. Unfortunately, many vendors have adopted a defeatist mentality: Threats are going to get in no matter what, so we'll focus on remediation and do what we can to minimize the damage.

Dell strongly disagrees with that conclusion. In fact, you can stop 99 percent or more of threats from entering your network.[2] You can protect your data from expropriation in the event of a lost laptop, smartphone or tablet. And you can spend less time managing security without compromising your organization's security posture. Effective endpoint security is not only possible, it's available today from Dell.

Making the case against signatures

Reactive measures have inherent limitations: The weeks or months between infiltration and detection are open season for cybercriminals, allowing them to prowl the network using stealthy behaviors that avoid conventional detection methods. In some high-profile incidents, the actual data exfiltration occurred slowly, over days and weeks.

Defenses based on spotting suspicious behaviors are by definition reactive and after the fact: If you're observing behavior, then the threat is already causing damage. The best such approaches can do is to limit the damage; they cannot stop it entirely. Even when they do detect a zero-day threat, signature-based solutions fall short. The reason is the gap between discovery and response: When a new or improved threat is identified, it takes time to create the signature and push it out to users — time that cyberattackers can exploit to your disadvantage. The reality is that traditional signature-based solutions are ineffective against zero-day threats, advanced persistent threats and targeted attacks such as spear phishing and ransomware.

Avoiding accidental and intentional data leaks

The enterprise world is a mobile world. Employees increasingly choose when and where they do their jobs — but that freedom creates new risks. Even though security teams work to protect sensitive corporate data from theft through cyberattacks, their efforts can be thwarted by a single employee who accidentally leaves an information-loaded laptop at the local coffee shop.

Theft poses another risk. Most device theft is opportunistic, with three-quarters of all incidents occurring either in the victim's work area or employee-owned vehicles.[6] Not surprisingly, information loss is most damaging in the public sector, healthcare and financial services — industries in which personally identifiable information (PII) has the highest intrinsic value.

Given the ever-expanding number of mobile and remote workers in the typical enterprise today, lost and stolen laptops and tablets are just a fact of life. No matter who winds up with the information or what they do with it, the consequences of a lost mobile device are enormous. Unless you can certify that the lost data was protected with robust encryption, your organization may have to notify customers, face regulatory fines and deal with negative publicity. The need to satisfy compliance and privacy legislation with enterprise-class encryption is just as important to security as preventing malware.

Preventing attacks and avoiding expenditures

You can prevent cyberattacks from affecting end users, data and business with Endpoint Security Suite Enterprise. Dell advanced threat prevention, integrated into the suite, stops more than 99 percent of incoming threats.[7] This preventative approach stands in marked contrast to traditional anti-virus software, which reactively catches a mere 45 percent of malware attacks, according to a leading industry expert.[8]

Dell advanced threat prevention also addresses an important gap in traditional anti-malware software: the BIOS. The BIOS is nearly invisible to traditional anti-malware solutions, making it difficult to detect when the BIOS has been compromised. Each time the system boots, Dell advanced threat prevention compares the current BIOS with a known good copy. The verification occurs in a secure cloud location, removing the potentially compromised PC from the verification process. If the BIOS has been altered in a way that might indicate a compromise, the suite alerts the administrator so the problem can be addressed before it does significant damage.

By helping to prevent attacks and identifying issues before they become widespread, Endpoint Security Suite Enterprise helps organizations avoid the costs associated with remediation. IT technicians spend an average of eight hours per system reimaging the disk and reinstalling the software.[9] In addition, end users lose access to their computers for a day or two and then spend hours reinstalling applications, reloading data and resetting preferences — a substantial hit on productivity.

Securing the mobile workforce

Encryption holds the key to solving the mobile device problem. Mobile end users can continue to work when, where and how they want, knowing their data is protected by the strong, best-of-breed encryption in Endpoint Security Suite Enterprise. At the same time, IT can focus on business needs without fear of the next compromise or data breach, because information on an encrypted device is just a pile of useless bits to anyone but the authorized user.

IT staff can simplify security configuration using the default policy settings that were designed to work for most organizations. The management console highlights the few policies that must be edited to enable the desired protection, thus reducing the time to protection and compliance. The result is simple, granular, policy-based data protection that works automatically in the background to maintain IT and end-user productivity.

Streamlining security management

Enterprise security doesn't have to be difficult to manage. Instead of requiring administrators to jump back and forth between disparate management tools and vendor support organizations, Endpoint Security Suite Enterprise enables them to manage threat prevention, encryption and authentication across the entire enterprise using a single pane of glass. You can spend less time on day-to-day management and avoid the need for training on multiple, incompatible software tools.

In addition, achieving and proving compliance is easier with Endpoint Security Suite Enterprise. Organizations with limited in-house security expertise can quickly and easily configure their security using the smart policy settings that are standard with the suite. Compliance managers can use the predefined templates to generate reports that contain information needed for more common regulations and general internal status reporting. If you need a more tailored approach, you can easily edit the

Intelligence right at the endpoint

Endpoint Security Suite Enterprise puts intelligence where it's most needed: right at the endpoint. Instead of signatures, Endpoint Security Suite Enterprise uses artificial intelligence and dynamic mathematical models to identify suspicious files before they execute, stopping malware from even entering the organization. These algorithms rely on hundreds of thousands of markers extracted from careful analyses of millions of real-world exploits and known good files. Locating the intelligence at the endpoint eliminates the need for a cloud connection and frequent updates. Dell continuously improves the algorithms and identifies new markers to stay ahead of evolving threats.

Encryption: The key to data protection

Endpoint Security Suite Enterprise delivers a layered, multi-key approach to encryption that is unlike any other data protection solution available today. The suite automatically applies different encryption keys for different users and different types of data, ensuring that only the rightful owner can access sensitive information, even on multiuser systems. The suite also enables automated patch management and other system maintenance without requiring a separate process for encrypted systems. End users can work just as they always have, while the data stays secure from the device up into the cloud. Encryption keys always remain within the enterprise network so IT and executives can know their corporate data is protected.

report templates and save them as custom reports that satisfy your business needs.

Simplifying endpoint security

Many organizations prefer to buy solutions from multiple vendors, while others prefer a more integrated approach to simplify security. The industry is increasingly moving toward the latter; a recent survey found that over 60 percent of mid-sized to large enterprise companies prefer purchasing hardware and endpoint security from a single vendor.[10]

You gain the flexibility to choose your preferred approach with the Dell suite because Dell integrates enterprise-class solutions into the suite to satisfy those who want best-of-breed products as well as those who want integrated simplicity. You can deploy hardware-agnostic Endpoint Security Suite Enterprise as stand-alone security software on your choice of hardware. Or for a more integrated approach, purchase Endpoint Security Suite Enterprise preinstalled on commercial Dell Latitude, OptiPlex, Precision and select XPS systems.

Conclusion

Traditional approaches to security are no longer enough. The twin imperatives today are to prevent threats from getting a foothold and to encrypt data to satisfy compliance legislation. As employee usage of laptops and mobile devices grows, security managers are asking how they can protect their information against today's stealthy, persistent threats in a mobile world.

More and more organizations will find the answer in Endpoint Security Suite Enterprise. You can dramatically reduce the risk of harmful data breaches thanks to the solution's proactive, best-of-breed data protection and advanced threat prevention. At the same time, you can streamline system administration, avoid remediation costs and simplify compliance. Better protect your organization from threats while supporting new initiatives and new ways of working — all without adding management complexity.

Learn More

For more information on Dell endpoint solutions that help you protect data and prevent threats, visit: Dell.com/DataSecurity

[1] Verizon, "2015 Data Breach Investigations Report," 2015, www.verizonenterprise.com/DBIR/2015/.
[2] Results from Cylance Unbelievable Demo Tour, Austin, Houston and Dallas, Texas, May 2015.
[3] Verizon, "2015 Data Breach Investigations Report," 2015, www.verizonenterprise.com/DBIR/2015/.
[4] FireEye Mandiant, "M-Trends 2015: A View from the Front Lines," February 2015, https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf.
[5] Verizon, "2015 Data Breach Investigations Report," 2015, www.verizonenterprise.com/DBIR/2015/.
[6] Ibid.
[7] Ibid.
[8] Brian Dye, senior VP for information security at Symantec, quoted in "Antivirus software is dead, says security expert at Symantec," The Guardian, May 6, 2014.
[9] CS-Solutions, "Business Case Analysis for Federal Agency," February 2, 2011, www.ezfts.com/wp-cs-solutions.pdf.
[10] Dell commissioned survey by Sentier Strategic Resources, March 2015.

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.