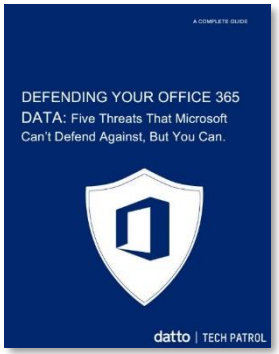
FUNDAMENTALS OF ENDPOINT SECURITY:
ANTI-MALWARE PROTECTION

ENDPOINT ANTI-MALWARE PROTECTION

The Fundamentals:

Endpoint Anti-Malware Protection actively works to prevent malware from infecting a users computer. However, there are millions of different kinds of malware out in the global world of the internet, ensuring that your organisation has strong protocols to fight these malware attacks is crucial and can be challenging. This ebook will be covering antimalware protection and how endpoint security technology can prevent malware from infecting and-user computers and corporate networks.

Other Resources You May Be Interested In



ANTIMALWARE PROTECTION AND THE FUNDAMENTALS OF ENDPOINT SECURITY

INTRODUCTION:

Endpoint antimalware protection actively works to prevent malware from infecting one of your users computers. There are a lot of solutions which the security technology extends to virtual desktops and mobile devices, as well as workstations and laptops. What is a Malware? – Common types of malware that affect, not only, your organisations computers but also mobile devices can be things like viruses, Trojan horses, worms, spyware, rootkits and the like. The term endpoint used with antimalware usually implies a product is designed for use within an organization, referring to small business, branch office, midsized company, government agency or enterprise.

With Cyber Attacks on the rise and with millions of different malware in the wild, one hyper-critical issue for organisations of any size is ensuring strong protection against malware.

THE BEAUTY OF ENDPOINT ANTIMALWARE PROTECTION SOFTWARE

Part 1:

Endpoint antimalware protection must be able to prevent malware attacks; this means protecting users when they are exchanging emails, browsing the web or connecting devices; and stop the proliferation of any attacks that manage to succeed.

To meet those goals, today's endpoint antimalware protection suites provide layered protection in the form of robust antivirus functionality – with the ability to shield against new or otherwise unknown threats or zero-day threats – such as antispyware, email inbox protection, host-based firewalls, data loss prevention, warnings when visiting websites that could pose safety risks and much more.

The beauty of such antimalware suites is that a single package with multiple functionalities presents a cohesive defence between external malware and internal systems and data. This type of in-depth defence uses different methods to stop….

THE BEAUTY OF ENDPOINT ANTIMALWARE PROTECTION SOFTWARE

Part 2:

malware, so an attempted attach or intrusion is unlikely to succeed simply by making its way through a single layer of protection. Plus a suite is easier for IT to manage than a collection of different applications from different vendors.

Think of your computer or device with endpoint antimalware protection installed as a heavily fortified castle with thick walls, a moat, steel gates and drawbridges. Guards, inside and out, constantly watch for suspicious activity, ready to block or slay the dragons.

CHARACTERISTIC FEATURES OF ENDPOINT ANTIMALWARE PROTECTION

[Typical features found in endpoint security suites]

- Antivirus: Malware writers go to great lengths to create malware that can avoid detection and resist removal. Today's antimalware products typically combine signature-based scanning with heuristics technology and cloud-based global threats intelligence to recognize and root out malware on systems and to prevent infections in the first place. Heuristics is the practice of identifying malware based on previous experiences, obs-ervations of malware behavior and typical points of attack. This combinati on of antivirus technologies is also effective against zero-day threats, whic h have historically posed major challenges to IT security teams.
- Antispyware: A malicious spyware infection is probably easier to pick up t han a common cold, and it's a major threat to protecting sensitive or conf idential data. Antispyware software runs constantly in the background to block spyware installation, regardless of the source.

CHARACTERISTIC FEATURES OF ENDPOINT ANTIMALWARE PROTECTION

[Typical features found in endpoint security suites]

- Data loss prevention (DLP): The technologies involved in DLP aim to protec t data that leaves the security of the internal business network, whether it' s via email messages, USB drives, on a laptop or mobile device, or uploade d to the cloud.
- Integrated firewall: Although a network should always be protected by a fir ewall, running a second firewall on the endpoint provides another layer of defense against malware that finds any cracks in the armor.
- Device control: Malware can infect a computer that isn't connected to a ne twork or the internet. Connecting a USB device to a computer or installing software from a CD or DVD always runs the risk of transferring an infected application to the target machine. Device control enables IT to restrict or b lock user access by setting and enforcing device access rules.

CHARACTERISTIC FEATURES OF ENDPOINT ANTIMALWARE PROTECTION

[Typical features found in endpoint security suites]

- Email protection: This component of antimalware suites attempts to filter out p hishing emails, spam and other messages that could carry malicious or otherwi se suspect content.
- Website browsing protection: Also referred to as reputation technology, most a ntimalware protection suites consult some type of ratings database that indicat es whether a website is safe to browse or not. With such protection in place, w ebsites reported as unsafe will not be opened. Users will receive warning messa ges instead

In addition to the preceding features, some endpoint antimalware suites roll in antir ansomware technology, intrusion detection and prevention functionality, applicatio n control, and network access control. Some packages also perform patch assessme nt and management, in which system threats are assessed and the most critical pat ches are applied first, in addition to vulnerability assessments and full-disk encrypti on to protect stored data.

DEPLOYING AND MANAGING ENDPOINT ANTIMALWARE PRODUCTS

Typically, endpoint antimalware products require an administrator to install a management cons ole on a server to help manage clients, product licenses and logs, or to use a web-based console that's part of a cloud service. This step also creates a database containing settings, privileges, eve nts and security policies. An organization that's very large or that has multiple sites may need to i nstall additional management servers for performance reasons, as well as to replicate data.

The next step is to install software (sometimes referred to as an agent) on client computers and devices, either directly or across the network. Regardless of the approach taken, clients must be configured for client software updates (automatic or pushed from the server) and virus definitio n updates, at a minimum. Overall, endpoint antimalware protection is an important and necessar y element in any organization's security infrastructure, though it shouldn't be the only element o rganizations implement. Before diving in, IT managers and security specialists should assess their environments to determine what specifically they need to protect, and they should look ahead t wo to three years at how their environment is expected to change. It's also a good idea to resear ch several highly rated endpoint antimalware packages to see how their features compare, deter mine which packages are most suitable to the organization's size and needs, and keep an eye on costs to get the best product for the budget.

ABOUT TECH PATROL

Tech Patrol is a market leader in providing advanced IT solutions to Australian and international businesses. We are the missing link in providing the technical experti se to reputable businesses who have limited internal IT resources.

As a platinum IT company we provide a corporate level of service with the impecc able customer service of a boutique business. This also means we are well regarde d for providing highly secure, reliable and best-of-breed technologies.

TechPatrol is a team of skilled and committed professionals who have distinguishe d IT expertise. We ensure our clients' current IT solutions are thoroughly maintain ed through our comprehensive monitoring, regular IT health checks and system au tomation. This guarantees we are constantly looking for ways to improve and maxi mise productivity while reducing overheads for our clients.

Founded in 1998 TechPatrol is a well-established industry forerunner in the latest t echnical solutions. We pride ourselves in our ability to control costs, integrate syst ems, increase staff productivity, reduce downtime and maintain disaster preventio n, for our clients.

Diogo Correa

Head of Sales and Marketing

"Thank you for taking the time to read this ebook on Endpoint Security. Hope yo u found it insightful. If you need any further informati on feel free to reach out to our team."

E: Sales@techpatrol.com.au
P: (02) 9363 5665
M: +61 411 046 016
W: www.techpatrol.com.au