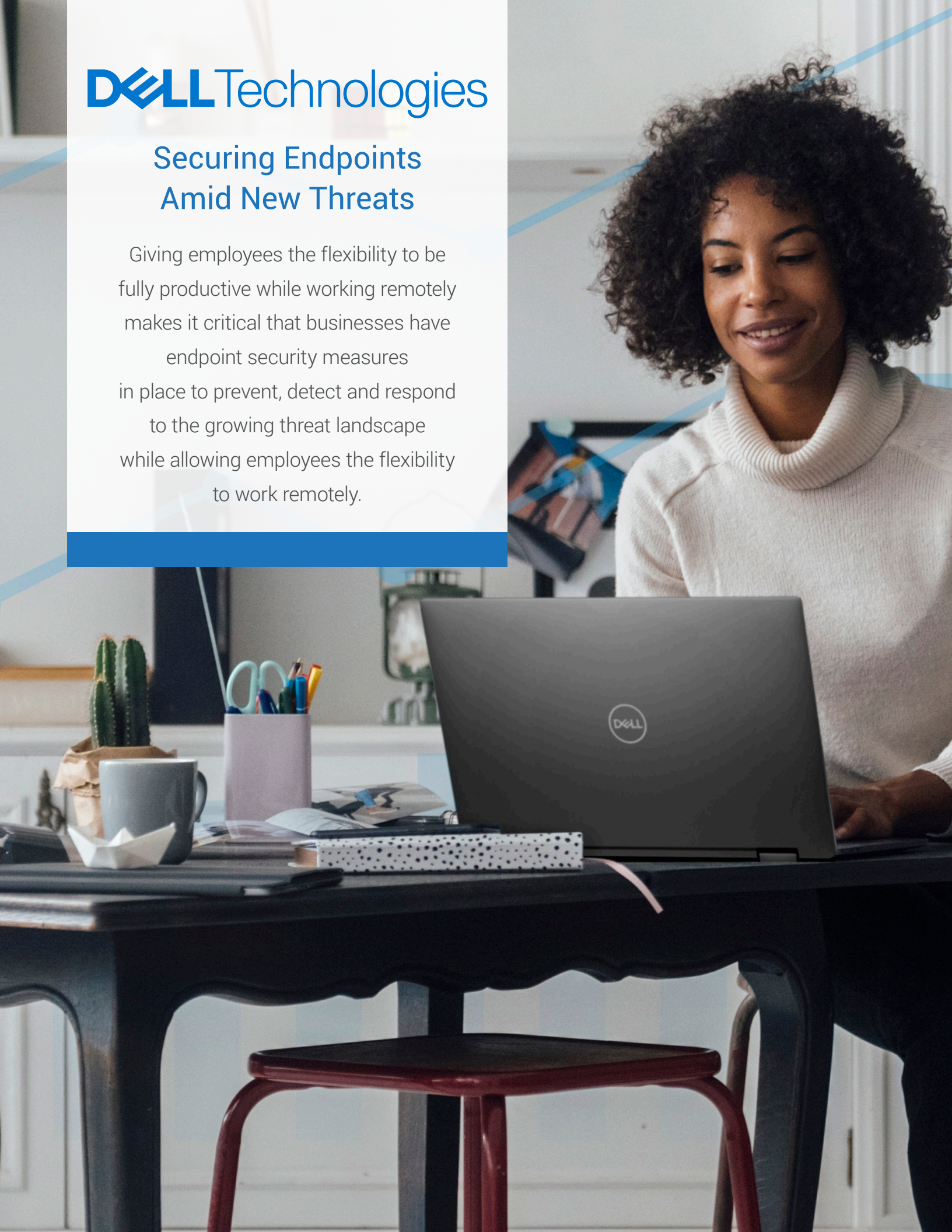
DELL Technologies

Securing Endpoints Amid New Threats

Giving employees the flexibility to be fully productive while working remotely makes it critical that businesses have endpoint security measures in place to prevent, detect and respond to the growing threat landscape while allowing employees the flexibility to work remotely.



As IT leaders scan the horizon for the end of the COVID-19 pandemic, many are planning on a new normal with a far higher number of remote workers than ever before. While many companies and their employees will benefit due to higher productivity and a more flexible work style, a price must be paid in terms of protection. The spike in remote work due to COVID-19 has made defending endpoints more difficult – 84% of IT leaders say protecting a remote workforce is harder.[1] One likely explanation is the 148% increase in ransomware attacks on global organizations amid the pandemic outbreak.[2] What makes this a sobering statistic is that home office workers rely on email as their primary means of business communication, which has led to a 350% increase in phishing attacks.[3]

Ongoing cyber security trends

The sudden shift to remote work takes place against a backdrop of many troubling cyber security concerns, which are taxing the expertise of cyber security professionals. These include:

1. BIOS-level attacks – exploited vulnerabilities in hardware or silicon. When the BIOS is compromised, the attacker often remains hidden while the device has credentialed access to the network and data. Sixty-three percent of companies have experienced a data compromise or breach due such attacks.[4]
2. Advanced Persistent Threats (APTs) – sophisticated threats that often lurk silently as they gather behavioral information as a prelude to siphoning off valuable data. Victims may not realize for a long time – 108 days on average[5] — that a silent attack has occurred.
3. File-based and fileless malware
   - File-based malware – usually file types with familiar extensions such as .DOCX and .PDF – the kind employees need to do their jobs. When a user opens the file, embedded malicious code is executed.
   - Fileless malware – usually a legitimate program that infects a computer. When the user launches such a program from an email, the fileless malware infects the computer and potentially the network, successfully evading many security technologies.
4. Nation-state-based attacks – typically from China, North Korea, Russia, and Iran. With the technological expertise and financial backing of such nation-states, attacks are often sophisticated and very damaging. However, many of these attacks exploit systems that lack the latest updates and patches. The FBI's CISA unit sends out advisories regularly.

The sudden shift to remote work takes place against a backdrop of many troubling cyber security concerns, which are taxing the expertise of cyber security professionals.

1. "The State of DLP 2020," Tessian.
2. VMware Carbon Black Blog, Patrick Upatham and Jim Treinen, April 15, 2020.
3. Google report, as cited in PCMAG.com, March 30, 2020.
4. "Match Present-Day Security Threats with BIOS-Level Control," A Forrester Consulting Thought Leadership Paper commissioned by Dell, June 2019.
5. The 2018 U.S. State of Cybercrime Survey.

5. Cloud-based attacks – increasing as cloud-based collaborative and productivity applications replace desktop applications. With the use of more than 2,400 cloud services in the average enterprise, 93% of organizations are moderately or extremely concerned about cloud security.[6] Protection must include data loss prevention (DLP) and threat protection in the cloud. In addition, user authentication must be protected against spoofing, and data must be encrypted to and from the cloud.
6. Compliance regulations – aimed at protecting personally identifiable information (PII). To prevent PII from falling into the wrong hands and ultimately being used for identity theft, some industries have adopted stringent regulations carrying stiff penalties. These include HIPAA in health care, PCI-DSS in financial services and retail, and GDPR for companies doing business with European citizens.
7. Crippling risk – resulting from $6 trillion in cybercrime losses predicted in 2021, an increase from $3 trillion in 2015. Losses are due to damage and destruction of data, stolen funds, lost productivity, intellectual property theft, personal and financial data theft, post-attack disruption, reputational harm and more, according to Cybersecurity Ventures.[7]

Rethinking endpoint security

Endpoint security: part of enterprise security
Faced with a larger population of remote workers than ever, many of whom must handle sensitive data to do their jobs, IT leaders should assess the current state of endpoint security at their organizations. But rather than looking at endpoint security by itself, they should consider it as an integral part of enterprise security to implement protection in depth – and they should look beyond the endpoints to include storage, networks and cloud-based services. A holistic approach to creating "trusted devices" within the enterprise must take into account these factors:

Built-in security
Rather than rely solely on software to protect endpoints, a comprehensive approach calls for the use of trusted devices – end-user computing devices that implement security within the devices themselves. Such devices protect PII and play an important role with regard to regulatory compliance, should a device be lost or stolen. End-user devices should also include privacy screen technology, which limits the ability of coworkers and office visitors to view confidential information on a computer screen.

IT leaders should consider endpoint security as an integral part of enterprise security.

6. Cybersecurity Insiders Cloud Security Reports, 2018, 2019.
7. Cybersecurity Ventures, 2020.

Protection above and below the OS

Above the OS. IT needs visibility, monitoring, and data security, as well as threat prevention, detection and remediation. On-device encryption is also very important to meet compliance requirements, however, should not slow down performance to degrade user productivity.

Below the OS. IT needs BIOS protection as well as chip authentication due to the frequency of attacks on firmware and hardware. A compromised BIOS can provide attackers with access to all data on an endpoint, including credentials, enabling attackers to move within an organization's network and attack the broader IT infrastructure.

AI and ML

With today's increasingly sophisticated attacks, the use of artificial intelligence and machine learning in detection and remediation is essential for endpoint protection. By observing behavioral patterns, AI and ML algorithms can detect unusual activity that could indicate and prevent a breach.

Secure Supply Chain

In the manufacturing process, it is possible for bad actors to introduce compromised components to enable a backdoor attack. Once embedded in a manufactured product, such components might enable a breach that could be extremely damaging and difficult to detect. It is therefore critical for both suppliers and manufacturers to implement stringent security measures at critical points along the supply chain.

Dell Trusted Devices

Dell builds security into each PC with these technologies:

SafeBIOS with BIOS Indicators of Attack (IoA) – provides visibility to BIOS changes to prevent tampering. Dell maintains a protected image off host to verify BIOS integrity. SafeBIOS is now integrated with VMware Carbon Black Audit and Remediation, which increases visibility to attacks through automated reporting and enables remote access in order to remediate BIOS corruption.

SafeID – provides chip-based authentication. End-user credentials are verified using a dedicated security chip, rather than relying on software which is less secure.

SafeScreen – protects screens that might expose sensitive information to office co-workers, visitors, maintenance workers, or other unauthorized persons.

SafeGuard and Response. Powered by VMware Carbon Black and Secureworks technologies, the Dell portfolio includes:

VMware Carbon Black — A cloud-native endpoint protection platform that combines the intelligent system hardening and behavioral prevention needed to keep emerging threats at bay, using a single lightweight agent and an easy-to-use console.

Trusted devices protect PII and play an important role with regard to regulatory compliance, should a device be lost or stolen.

Secureworks Managed Services — collects and correlates telemetry from cloud, network and endpoint to identify threats across the enterprise. Providing industry-leading incident response, Secureworks Managed Services are integrated with the VMware Carbon Black platform as well as many other platforms.

SafeData. Collaboration, always a hallmark of successful organizations, takes on added importance in the era of intensified remote work. Today's workforce collaboration requires data security both on-device and in the cloud that does not slow down the end user. Dell partners with Netskope and Absolute to deliver holistic endpoint security.

Netskope. Taking a data-centric approach, Netskope technology protects data created and exposed in the cloud. By providing IT with real-time visibility, access to the cloud, monitoring and data loss prevention, Netskope redefines cloud, network and data security. Teams are empowered with the right balance of protection and speed, enabling them to secure their organization's digital transformation journey.

Absolute. Dell embeds Absolute technology in the firmware of every device, giving every endpoint a self-healing link to the cloud-based Absolute dashboard. This enables managers to track, manage and secure endpoints and the data on them, even when they are off the network. Absolute technology:

- Locates and manages devices.
- Provides VPN and security software persistence.
- Implements an air-gapped solution to enable recovery from attacks
- Includes multi-cloud data protection solutions that can be either software-defined or appliance-based.

Today's workforce collaboration requires data security both on-device and in the cloud that does not slow down the end user.

Conclusion

The spike in remote work due to the COVID-19 pandemic increases danger across an already threat-filled cyber security landscape. A new, holistic approach to endpoint protection is needed. Rethinking endpoint protection starts with trusted devices that are protected both above and below the OS. Such a strategy also looks beyond the endpoints themselves to take an enterprise view of cyber security that includes servers, networks, cloud-based services and regulatory compliance. The Dell Trusted Devices portfolio embodies such a comprehensive approach. Dell endpoint protection spans the enterprise to include multi-cloud data protection solutions that can be delivered as software-defined and/or appliance-based solutions. Above all, Dell Trusted Devices enable users to remain highly productive by defeating increasingly sophisticated attacks in the new remote work paradigm.

For more information, please see:
https://www.dell.com/en-in/dt/endpoint-security/index.htm