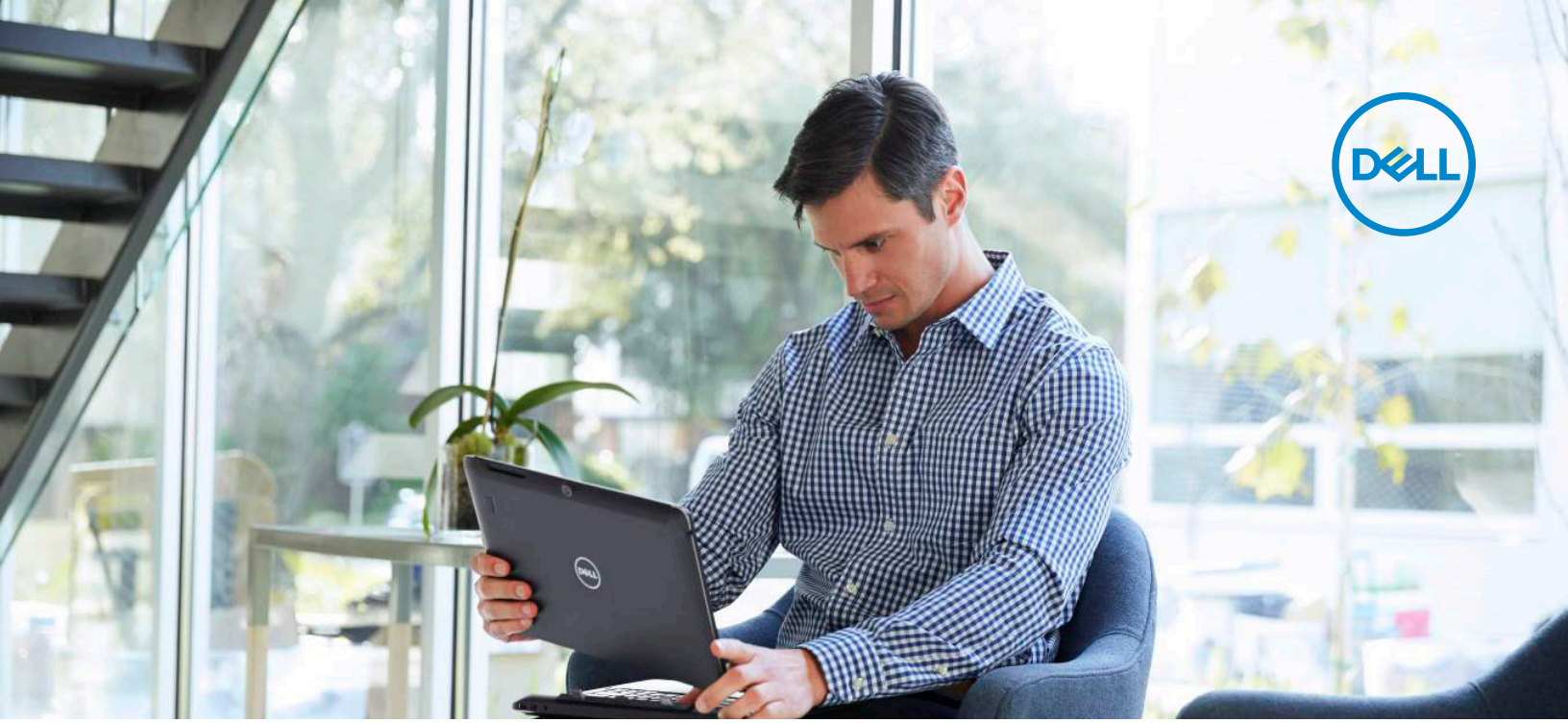

## Vorteile des erweiterten Bedrohungsschutzes

- Beispiellose Effizienz: Unsere Lösung stoppt 99 % aller Malware-Bedrohungen bereits vor der Ausführung und liegt somit weit über der durchschnittlichen Effizienzrate von 50 % der führenden Virenschutzlösungen.[1]
- Die Vermeidung von Malware-Angriffen reduziert die Problembehebungskosten sowie die Ausfallzeiten für Endbenutzer deutlich.
- Schützt physische PCs sowie virtuelle Desktops und Server.
- Dank der niedrigen Prozessor- und Arbeitsspeichernutzung steigt die Systemleistung und der Computer bietet wieder Leistung wie am ersten Tag.
- Durch die lokale Bedrohungserkennung ohne kontinuierliche Verbindung mit der Cloud können mobile Endbenutzer arbeiten, ohne dabei Kompromisse eingehen zu müssen.
- Der Bedrohungsschutz basiert auf künstlicher Intelligenz sowie mathematischen Modellen. Damit werden Fehlalarme (False Positives) praktisch eliminiert. Da keine kontinuierlichen Signaturaktualisierungen nötig sind, steigt die IT-Produktivität.
- Unsere Lösung erfüllt die PCI DSS, HIPAA HITECH und Microsoft Vorgaben für Virenschutzersatz und reduziert so die Gesamtkosten für die Absicherung Ihrer Daten.

[1]Ergebnisse von der Cylance Unbelievable Demo Tour, Austin, Houston und Dallas, Texas, Mai 2015

# Dell Endpoint Security Suite Enterprise

## Blockieren Sie ausgeklügelte Angriffe, vereinfachen Sie die Endpunktsicherheit und übertreffen Sie die Compliance

Endgerätesicherheit und -Compliance sind für jede Organisation entscheidend – unabhängig von ihrer Größe. Einerseits müssen sie die physischen und virtuellen Endgeräte samt der auf ihnen gespeicherten Daten absichern, andererseits die Endbenutzeranforderungen im Hinblick auf Datenverarbeitungstrends wie BYOD (Bring Your Own Device), die Datenfreigabe in öffentlichen Clouds sowie Mitarbeitermobilität erfüllen. Herkömmliche Datensicherheitslösungen versuchen, auf diese Bedürfnisse einzugehen, doch stellt die Verwaltung mehrerer Clients und Konsolen IT-Teams mit begrenzten Ressourcen vor Schwierigkeiten – insbesondere wenn sie nicht über interne Sicherheitsexperten verfügen. Die meisten Lösungen für Endgerätesicherheit sind schwer bereitzustellen und zu verwalten, und nicht für alle Geräte und Speicherorte geeignet, die Mitarbeiter für ihre Daten verwenden. Außerdem beeinträchtigen sie die Systemleistung und die Endbenutzerproduktivität. Das Datensicherheitspaket von Dell bietet zahlreiche Vorteile, darunter:

- Vertrieb und Support für Ihre physischen PCs sowie Ihre virtuellen PCs und Sicherheitslösungen aus einer Bezugsquelle.
- Schutz für heterogene Umgebungen mit vollständigem Support für Dell Hardware und Hardware anderer Hersteller sowie für virtuelle Desktops, die auf Citrix oder VMware ausgeführt werden
- Automatische Bereitstellung und Provisionierung bei werkseitiger Installation auf kommerziellen Dell Geräten
- Einen einzigen integrierten Client für vereinfachte Bereitstellung und Aktualisierung sowie die nahtlose Zusammenarbeit aller Komponenten Ihrer Datensicherheitslösung
- Unkomplizierte Compliance-Verwaltung und -Überwachung mithilfe vordefinierter Berichte und einer intuitiven Verwaltungskonsole, über die Sie schnell jedwedes Problem identifizieren können

Endpoint Security Suite Enterprise gewährleistet starke Datensicherheit und schützt Daten, Systeme sowie den guten Ruf Ihres Unternehmens. Die Suite bringt einen integrierten Client für erweiterten Bedrohungsschutz und Verschlüsselung der Enterprise-Klasse mit. Alle Elemente werden zentral über eine einzige Konsole verwaltet, sodass Unternehmen die Kosten und die Komplexität ihrer IT-Verwaltung reduzieren können. Dank konsolidierter Compliance-Berichterstellung und flexibler E-Mail-Benachrichtigungen können sie Compliance-Vorgaben unkompliziert für alle ihre Endgeräte durchsetzen und deren Einhaltung auch nachweisen. Vor allem die integrierten Sicherheitsfunktionen wie die vereinfachte Richtlinienkonfiguration mit intelligenten Standardeinstellungen ("Smart Defaults") und vordefinierten Berichtsvorlagen sind Organisationen zum Schutz von Endbenutzern und Daten eine große Hilfe.

# Erweiterter Bedrohungsschutz

Das Bedrohungsspektrum verändert sich heute kontinuierlich und erfordert ein Maß an Sicherheit und Effektivität, das die bisher in Unternehmen, Behörden und Institutionen weltweit eingesetzten Lösungen bei Weitem nicht bereitstellen können. Herkömmliche verhaltens- oder signaturbasierte Viren- und Malwareschutzlösungen sind von Grund auf reaktiv ausgelegt, da sie zur Angriffsidentifizierung ausschließlich auf bereits bekannte Verhaltensweisen oder Muster zurückgreifen. Aufgrund ihrer reaktiven Konzeption sind sie zunehmend ineffektiv gegen Zero-Day-Bedrohungen, ausgeklügelte moderne Bedrohungen und gezielte Angriffe, wie Spear Phishing und Ransomware.

Endpoint Security Suite Enterprise löst dieses Problem mittels Integration eines revolutionären erweiterten Bedrohungsschutzes mit unerreichter Effektivität gegen Zero-Day-Bedrohungen, moderne ausgeklügelte Bedrohungen sowie gängige Malware. Die Lösung nutzt einzigartige künstliche Intelligenz und dynamische mathematische Modelle, um Dateien bereits vor ihrer Ausführung zu analysieren und zu bestimmen, ob sie sicher sind. Malware hat so keinerlei Chance, Schaden anzurichten. Der Dell Ansatz basiert auf Zehntausenden Markern, die durch die sorgfältige Analyse von Millionen von real genutzter Exploits und als unbedenklich bestätigter Dateien extrahiert wurden. Er ist nicht abhängig von Signaturen, die auf bekannte Verhaltensweisen oder Muster scannen und daher regelmäßig aktualisiert werden müssen, um mit der Weiterentwicklung der Bedrohungen Schritt zu halten. Dies ermöglicht uns den Schutz vor Bedrohungen, ohne dass eine durchgehende Verbindung zur Cloud oder häufige Aktualisierungen erforderlich sind. Die Threat-Intelligence ist in das Endgerät integriert, unabhängig davon, ob es sich um ein physisches Gerät oder eine virtuelle Maschine handelt. Dell ergänzt diesen erweiterten Bedrohungsschutz durch BIOS-Überprüfungen, die beim Start aller kommerziellen Dell Systeme durchgeführt werden und Administratoren bei potenziellen BIOS-Manipulationen umgehend warnen.

## Web-Schutz und hostbasierte Firewalls

Durch die zunehmend wachsende Angriffsfläche benötigen Organisationen eine tiefgestaffelte Sicherheitsarchitektur. In der Endpunktsicherheit ist der Schutz der Benutzer vor verschiedenen Angriffsvektoren von wesentlicher Bedeutung. Zusätzlich zur vorausschauenden mathematischen Darstellung, die bereits einen Großteil der Bedrohungen an der Ausführung hindert, bietet die Suite auch zusätzlichen Schutz vor Angriffen aus dem Internet sowie hostbasierten Firewalls für zusätzlichen Schutz des Geräts vor Malware, die in den Firewall-Perimeter vorgedrungen ist. Die Web-Schutzfunktion bietet eine reputationsbasierte Websitebewertung. Mit reputationsbasierten Websitebewertungen für über 106 Millionen URLs deckt sie 95 % der häufig frequentiertesten Websites ab. Die Funktion "Hostbasierte Firewall" bietet im Vergleich zur nativen Windows Firewall herausragenden Schutz. Sie ist zudem funktionsreich und anwendungssensitiv. So kann ein- und ausgehender Datenverkehr mittels Regeln und der optionalen Global Threat Intelligence Reputationsbewertung kontrolliert werden.

## Verschlüsselung

Die Verschlüsselungslösung von Dell stellt auch einen datenzentrierten und richtlinienbasierten Ansatz zur Verschlüsselung dieser Daten bereit (unabhängig davon, ob sie auf physischen PCs oder virtuellen Desktops gespeichert sind), ohne dass davon IT-Prozesse oder die Endbenutzerproduktivität beeinträchtigt werden. Die speziell mit Blick auf einfache Bereitstellung, Endbenutzertransparenz und problemlose Compliance konzipierte Lösung bietet ein Höchstmaß an Schutz, gewährleistet eine schnelle Neutralisierung kritischer Sicherheitslücken und hilft Ihnen, Verschlüsselungsrichtlinien für mehrere Endgeräte und Betriebssysteme zu verwalten – alles von einer zentralen Verwaltungskonsole aus.

Dell bietet eine starke Verschlüsselung und Verwaltung von Microsoft® BitLocker sowie Schutz von Daten auf externen Medien, selbstverschlüsselnden Festplatten, Mobilgeräten und in öffentlichen Cloud-Diensten. Die Lösung ermöglicht IT-Administratoren die einfache Durchsetzung von Verschlüsselungsrichtlinien, unabhängig vom Speicherort der Daten und ohne Eingriff des Endbenutzers. Unsere Verschlüsselungslösung bietet zahlreiche Vorteile, darunter:

- Detaillierte, unternehmensweite Berichte zum Verschlüsselungsstatus, mit denen Sie teure Geldbußen und Rufschädigung vermeiden, wenn Geräte verloren gehen oder gestohlen werden
- Keine Notwendigkeit für spezielle Vorbereitungs- oder Defragmentierungsschritte auf den Datenträgern vor der Verschlüsselung
- Verschlüsselung für Systemdatenträger und externe Medien in einer einzigen Lösung
- Integration in vorhandene Prozesse für Authentifizierung, automatisierte Patch-Verwaltung und mehr
- Softwareverschlüsselung mit FIPS 140-2 Level 2-Validierung
- Verschlüsselung aller Daten (außer Dateien, die wichtig für den Start des Betriebssystems sind) oder vollständige Festplattenverschlüsselung, abhängig von Ihren Präferenzen
- Erweitertes Portsteuerungssystem zur Verhinderung von Datenlecks

## Technische Daten

Endpoint Security Suite Enterprise kann in Umgebungen mit Systemen mehrerer Anbieter eingesetzt werden, die die nachfolgend aufgeführten Anforderungen erfüllen.

**Unterstützte Client-Betriebssysteme**:

- Microsoft Windows 7 Ultimate, Enterprise und Professional Edition
- Microsoft Windows 8 und 8.1 Enterprise und Professional Edition
- Microsoft Windows 10 Education, Enterprise und Pro Edition
- Microsoft Windows Server 2008 R2 und 2012 R2
- macOS 10.9+, 10.10+, 10.11+ und 10.12+

**Auf von Dell ausgewählten PowerEdge VDI-Servern unterstützte VDI-Umgebungen**:

- Virtuelle Windows 10 Desktops

**Wird auf folgenden Hypervisoren und Verbindungsbrokern ausgeführt**:

- VMware vSphere 6.0 Update 2 und VMware Horizon 7
- Microsoft Hyper-V 2012 R2 und Citrix XenDesktop 7.11

**Die folgenden Internetbrowser bieten Unterstützung für die Remote-Verwaltungskonsole und Compliance Reporter**:

- Internet Explorer 11.x oder nachfolgende Versionen
- Mozilla Firefox 41.x oder nachfolgende Versionen
- Google Chrome 46.x oder nachfolgende Versionen

**Erfahren Sie mehr unter Dell.com/DataSecurity und Dell.com/wyse/shield**