

Making Healthcare Digital Transformation A Reality

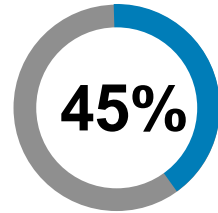
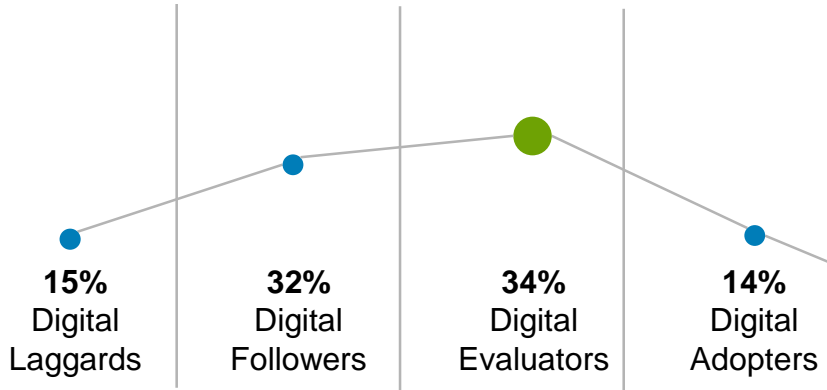


DELLEMC

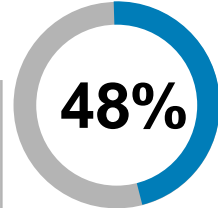
On the journey to digital transformation

In this digital world, businesses & industries are being disrupted everywhere

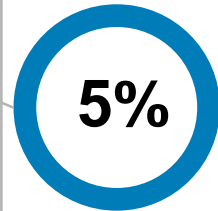
Business leaders have the opportunity to leap ahead from **digital evaluators** to digital leaders



Fear becoming obsolete in 3-5 years



Unaware of what their industry will look like in 3 years



Are classified as Digital Leaders

Source: [Digital Transformation Index](#)

DELL EMC

The new digital era of care – making it real

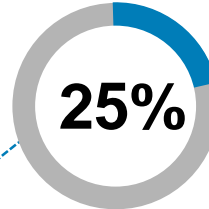
Game changers that are driving digital transformation



Multi-clouds

Worldwide, healthcare providers spent \$8.9 billion in industry cloud solutions in 2017, by

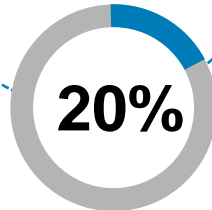
2021, they will spend \$17.6 billion on healthcare clouds



Consumerism

Of data used in medical care will be collected and shared with healthcare systems by the patients themselves ("bring your own data") by the end of

2020



Big data & analytics

By **2021**, 20% of healthcare & 40% of life-sciences orgs will have achieved 15–20% productivity gains through the adoption of cognitive/AI technology



Commitment to Security

By **2018**, there will be a doubling of ransomware attacks on healthcare organizations

Addressing drivers of change: our focus on four transformation pillars



**Health IT
Transformation**



**Precision Medicine
Transformation**



**Connected Health
Transformation**



**Security
Transformation**



DELLEMC

Pivotal™

RSA™

SecureWorks®

virtustream

vmware®

Essential infrastructure solutions for healthcare needs

Making Digital Transformation a Reality



Health IT Transformation



Precision Medicine Transformation



Connected Health Transformation



Security Transformation



Clinical Application Optimization



Multi-Cloud Portfolio



Healthcare Cloud



Clinical Genomics & HPC



Big Data & Analytics



Machine Learning



Innovative devices



Healthcare IoT & Telehealth



Patient Engagement



Data Protection



Threat Detection



Identity Access

Case Study – Large Teaching & Maternity

3,500 Staff
300,000 Out Patients

70,000 ED
8,000 Births

“Only last week we had a nurse who had to attend court because her name was on the Triage form, even though someone else had undertaken the Triage.”

Clinical Nurse Manager

“It is a typical chicken and egg scenario, Staff won’t use the system because it takes to long; other staff spend time inputting the data later.”

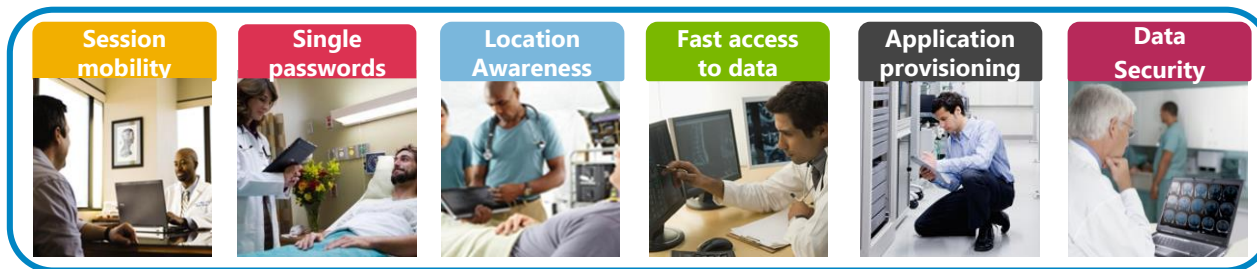
Consultant

“When I have to log in and out about fifty times a shift, the forty seconds each time adds up.”

Staff Nurse ED

“The multiple windows lock you out, and when you try to switch, they freeze. This causes delays in checking information for patients”

Mobile Clinical Computing



Mobile Clinical Computing



Providing healthcare professionals with the ability to roam with applications and sessions following the user



Data Security

- Information stored in the data center – not the endpoint
- Role-based delivery of apps/ data

Clinical Efficiency

- Single Sign-On and application auto launch
- Session Transfer
- Follow-me printing

IT productivity

- Dynamic provisioning
- Patch management
- Standardisation and simplification

Clinician - drivers



Head of IT - drivers



CxO Level - drivers



Mobile Clinical Computing is designed to:

- **REDUCE** security concerns by removing sensitive data from client systems
- **DRAMATICALLY** improve worker productivity
- **ENSURE** simple, fast, efficient access to data
- **REDUCE** application provisioning from hours to minutes
- **ELIMINATE** the need to memorise multiple passwords
- **LOWER** the overall cost of computing
- **IMPROVE** the computing experience of all users
- **ENABLE** clinicians to provide better patient care



1) Shared Working Environments - “Follow-Me Desktop”



Station Desktop



Wireless Device



Laptop / Remote Location

- **Fast and convenient desktop access**
 - User authentication (fingerprint, tap ID badge, etc.)
 - Single sign-on to eliminate all application logons
- **User roaming desktop**
 - “Follow-Me” desktop throughout the building
 - Automatic desktop lock when user roams
- **Location awareness**
 - Printer mapping (follow-me printing)
 - Application location context (tie user location to applications)
 - Desktop location context (which applications to show in which locations)

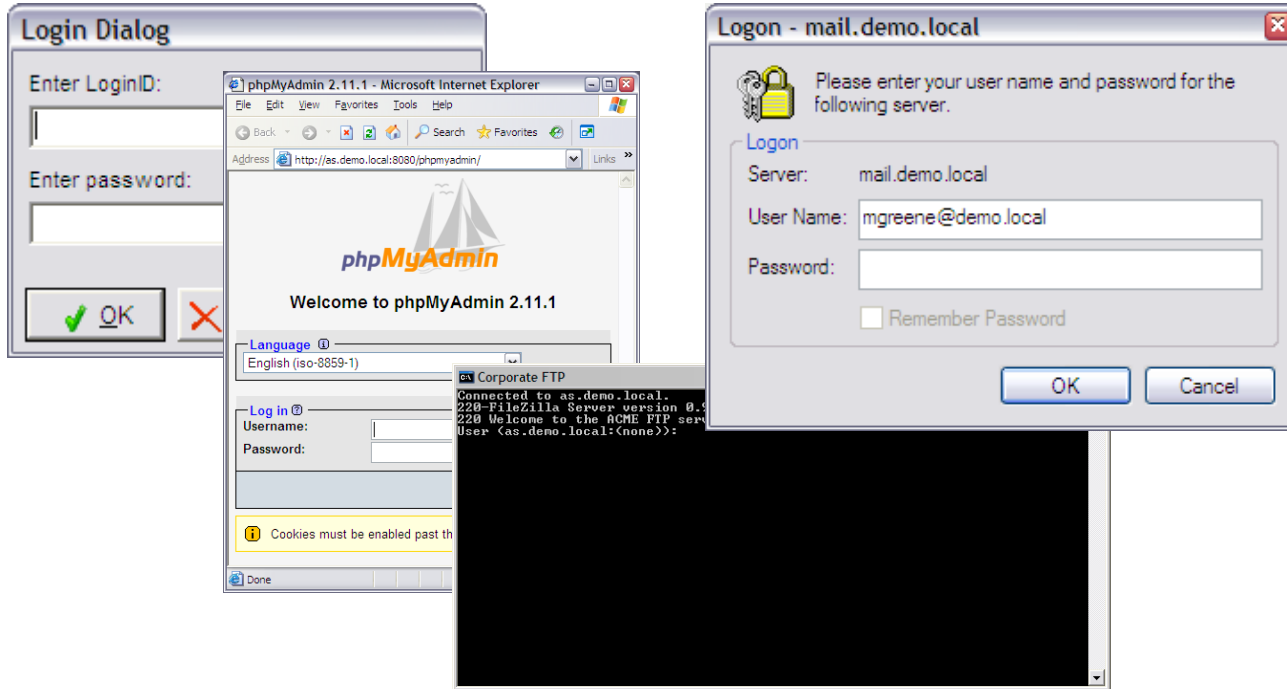
2) Protect Unattended Desktops - “Secure Walk-Away”

- Provides real-time visual detection to identify an already authenticated user in front of a workstation
- Automatically locks the desktop upon their departure
- Provides instant re-authentication when they return
- Tracks user for the duration of the session and requires no user interaction required – fully automated & transparent



3) Single Sign On - Logs you in...

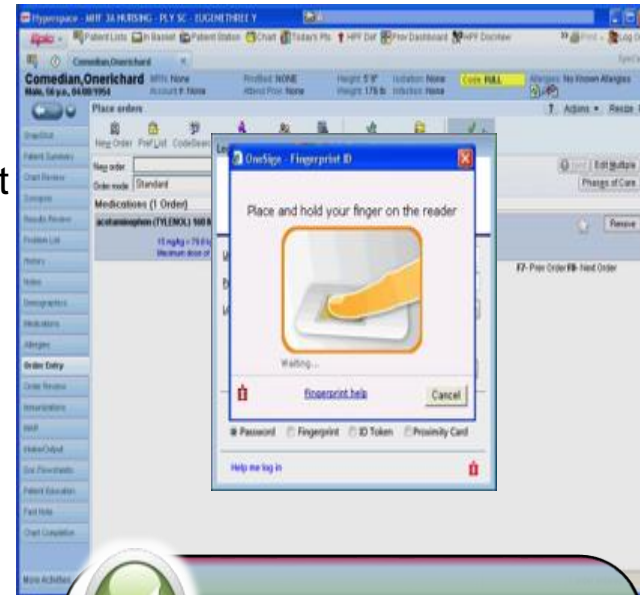
Any type of application, Web, Legacy, Java, Windows.....



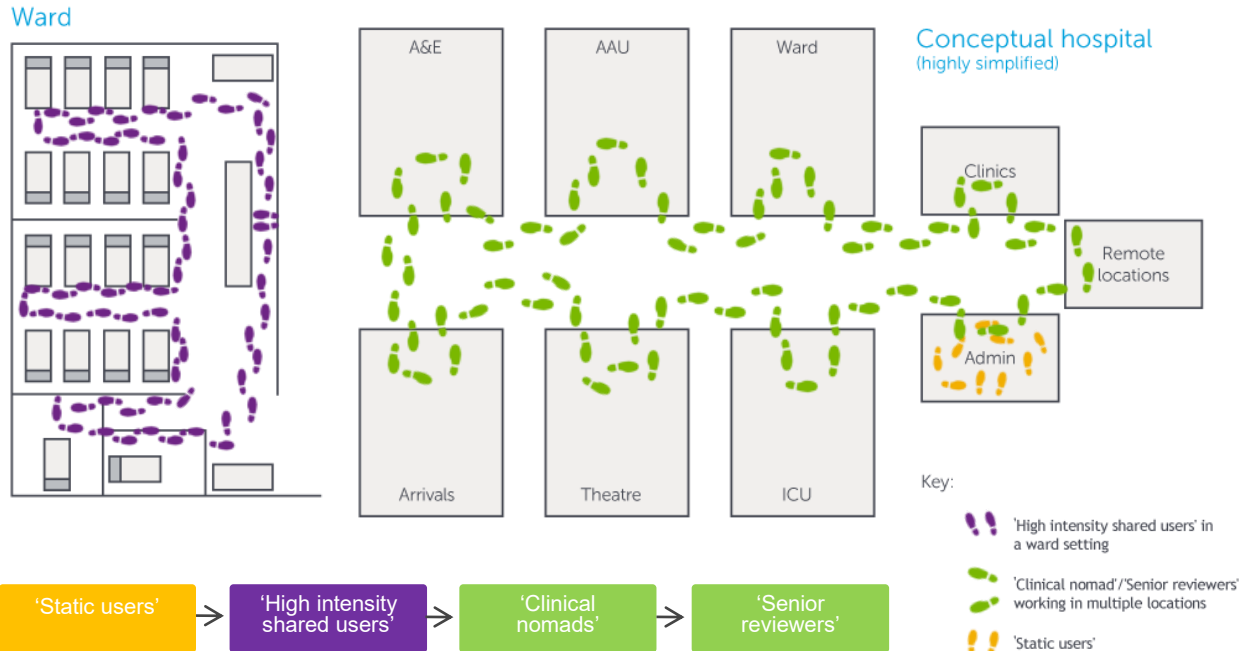
4) Application and/or Transaction Re-Authentication

ProveID

- Facilitates secondary re-authentication for target applications
- Introduces user verification at any point in a target application or operational workflow
- Supports username / password and strong authentication options



User profiles studied in the MCC trial



Case Study – Large Maternity Hospital

- Improved patient confidentiality (28% Desktops Shared)
- Clinical Governance (Audit of who accessed system)
- Compliance with data legislation (Data is Secured)
- Improved access for clinical staff (From 38 seconds to 4)
- Reduction in time spent logging into and out of applications (67% Improvement)
- Improved access & utilisation of devices (27% Increase in Shared Device Usage)

“It now takes them less time to have access to the clinical data needed to treat a patient. This means that the clinicians are able to focus more on what is important – the patients”.



Summary Conclusions

Clinical Use

Improved Productivity & Staff Satisfaction

Up to 215+ mins/week/person (9% productivity gain) *

Patients Benefit

Reduction in information access related delays & faster informed decisions

Enhances rather than disrupts Workflow

Helps existing systems align with workflow

Appropriate Security

Delivers appropriate, information security that's workable for users

MCC Solution

Session Mobility

Persistent Session which can roam from device to device as needed

Swipe in – Swipe Out

RFID card swipe or single key stroke suspension of session

Single Sign On

SSO access to core clinical and other applications**

Faster Start Up

Av 83%** faster app start up on shared computers. From minutes to seconds

IT Management

Simplified Management

Provisioning, Support and User Device optimisation potential at

Optimised Devices

Device types optimised for task & user population.

Workstation availability

Reduction of Workstation monopolisation and time required for interactions

Improved Security

Removal of the need for shared/generic logins. No data on devices.

* Extrapolation from trial results. Trial findings ranged from 6mins to 117mins

** Average time saving (UHB Trial 92% E4B and 94% MAU, OLVG 77% and COL 71%)

Mobile Clinical Computing Executive Summary

Executive Summary Proposal – Mobile Clinical Computing



XYZ NHS Trust LOGO HERE

1. AS-IS XYZ NHS Trust Background

Current issues:

- Having all of the relevant information at the point of care
- Speed of care, information sharing
- Multiple logins required for desktop and applications
- Generic workstation login
- Shared application credentials
- Mobile devices create security and support issues

Current initiatives and Strategy

- Trust 2010 Annual Report states it must "use technology to deliver faster, better care"
- New systems include:
 - Monitoring patient 'journeys' Trust-wide
 - Speeding up test requests and results
 - Electronic patient notes to speed up care
 - New technology in state-of-the-art facilities

Current Constraints

- Budget limitations following the NHS Comprehensive Spending Review

2. Scope & Key Assumptions

Scope

- 1000 access devices
- 800 concurrent users (see assumptions)
- 30 different applications to be installed within the environment
- 10 applications to be scripted for Single Sign-On
- Existing Chip/PIN smartcard and reader is to be used
- Technical training for support staff
- No remote access required

Key Assumptions

- 70% of 3000 staff will require MCC across a 3 shifts per day = 700 users + additional 100 user to allow headroom
- Existing AD, RADIUS Server and Wireless infrastructure
- Existing client devices to be re-processed
- All applications that require roaming either utilize Windows printing or have a method within the application that MCC can utilize to reset printing as end users disconnect and move to new devices
- Existing network infrastructure is resilient
- All user communications will be the responsibility of XYZ

3. XYZ NHS Trust Input into Process

- Attendance at an initial workshop to agree clinical settings in scope, assessment approach, communication plan, deliverables and timescales
- Participate in the completion of a MCC discovery matrix for each setting
- Contribute to stakeholder analysis and engagement for each setting
- Provide input to the benefits realisation, identification of benefits, baseline measures and indicators
- Provide input to the current state workflow assessment and gap analysis
- Attendance at 3-4 workshops to verify the content of the MCC matrices for the relevant business settings
- Ready all server hardware in readiness for configuration. This includes the provision of network access and shared storage where required

4. High Level Plan

- Kick-off workshop
- Complete MCC discovery matrix for each setting
- Stakeholder analysis for each setting
- Identification of benefits, baseline measures and indicators
- Workshops to verify content for each setting
- Develop current and future state workflows for validation of MCC workflows across the trust
- Design and Integration planning
- Integration and SSO profiling of agreed applications
- Infrastructure build and integration
- User Acceptance Testing
- Production client deployment

5. Discovery and Analysis

- Analyse data captured in the Discovery Matrix and document findings, collating volume of applications, devices, issues, risks and constraints for the MCC deployment
- Validate findings with XYZ and incorporate any changes
- Create MCC Technical Design
- Create 5 current state and future state workflows for validation of MCC workflows across the trust
- Assist XYZ to develop 5 additional future state MCC workflows
- Create Outline Deployment Plan

MCC Discovery Matrix



6. Dell Knowledge Base and Best Practices

Information-driven decisions through an established, repeatable process



7. XYZ NHS Trust Deliverables

- Workshop to help communicate benefits of MCC to facilitate clinical engagement/adoption
- MCC Technical Design incorporating infrastructure build and configuration guides, application integration and single sign-on profiling, and test plans
- Clinical Discovery Findings Document
- 5 documented current and future state workflows to validate MCC across the trust
- Outline Deployment Plan
- Fully built and tested MCC infrastructure
- Technical support to integrate the installation of client components within XYZ's existing Software Distribution Toolset
- End User Support provided by 'Floor walking' Technical consultants made available to undertake basic end user training and troubleshooting activities

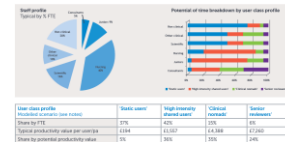


8. Benefits to XYZ NHS Trust

- Reduction of time consuming login processes
- Users able to more efficiently use shared PC's gaining greater asset utilisation
- Reduction or elimination of time spent by clinicians waiting for a PC (particularly when there is high contention for shared devices)
- Reduction or elimination of the need for clinicians to print patient records, record information manually and then log into the nearest available device and then facing the access challenges mentioned above
- "Session Roaming" enables anytime, anywhere access to patient and related information via MCC enabled devices
- Maintain all relevant patient or other data on a user's own "virtual desktop" allows clinicians to reconnect and continue a session from any MCC enabled device, irrespective of location
- Considerable time saving and productivity benefits for highly mobile clinicians
- Rapid and simplified access to patient data improves patient safety (access to latest patient information) and patient experience (avoidance of delay)
- Improved security of patient data
- Easier replacement of faulty devices (hot swap rather than repair)
- Reduction of password reset fault calls (thanks to Single Sign On)

9. Financial Justification

Using the Business Value of IT (BVI) methodology for assessing the operational and strategic impacts generated through the use of IT, the performance indicators and value dials that represent the most likely monetizable benefits all relate to increase in productivity :



Dell EMC Healthcare Partners

accenture

AGFA
HealthCare

aridhia

Allscripts

Atos

BARCO

Carestream

Cerner

CHANGE
HEALTHCARE

Datadobi
ASK YOUR DATA

Deloitte

dimension
data

DXC.technology

eClinicalWorks

edico genome

Epic

EY

GE Healthcare

FUJIFILM

Hyland
creator of OnBase

IBM Watson Health

illumina

Information
Builders

inovalon

inspirata

intel

Intelrad
Distributed Radiology Solutions

InterSystems
Health | Business | Government

IRON MOUNTAIN

JOHNS HOPKINS
MEDICINE

leidos

MACH7
TECHNOLOGIES
Unlock. Unleash. UnPAC.

MEDITECH

Medical
INFORMATICS

Microsoft

NEXTGEN
HEALTHCARE

NTT DATA

ORION
HEALTH

PHILIPS

Predixion
Software

SAP

SECTRA

seven10
STORAGE SOFTWARE

SIEMENS

SUNGARD
AVAILABILITY
SERVICES

tgen

UNISYS

DELL EMC



Better security means “better business”

Staff & Patient Experience
Improved Asset Utilisation
More Secure Environment
Accelerated Decisions
Greater Compliance
Faster Workflows
Lower costs
Less Risk

Privacy by Design

The inclusion of data protection from the onset of the designing of systems

The controller...

... “shall hold and process only the data absolutely necessary for the completion of its duties.”
(data minimisation)

... “shall.. implement appropriate technical and organisational measures.. in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects.”

... “limit the access to personal data only to those needing to act out the processing.”

Encryption is stated as being an essential “technical” measure as “it renders the data unintelligible to unauthorised parties in cases of data loss”



Our Position

Data is the lifeblood of a company

Data has to be fluid to propel innovation and raise productivity.

But, data must be SECURED and PROTECTED as it flows.

We must PREVENT THREATS from malicious outsiders.

And PROTECT DATA from trusted insiders

Starting with Endpoints

The end-user is the most vulnerable part of the security chain because we are humans – we are curious, we want to collaborate and we want to communicate.

45%

of corporate data is stored on the endpoint

95%

of data breaches originate at the endpoint

1M

new malware variants every day

Dell Data Security

integrated solution to protects your business, data, systems, users and reputation

Authentication

- Smartcards
- Fingerprint readers
- Multi-factor

Encryption

- Encrypt local drives & external media
- Full Disk Encryption, BitLocker & SED management
- Mac Encryption & external media
- Server Encryption
- Cloud and office documents where ever they go

Advanced Threat Prevention

- Revolutionary AV replacement
- Stops Zero-day threats before they can run
- Unparalleled efficacy of over 99%

Simplified management

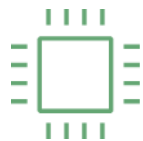
Single pane of glass

Consolidated status and compliance reporting

Virtual console options



Dell's Endpoint Solution for Healthcare



Advanced Threat Protection built-in, seamless to IT and End Users



Effective prevention against threats designed to circumvent traditional defences, firewalls, IPS/IDS even when offline, dark, remote.



Employs machine learning and artificial intelligence to accurately protect and prevent.



Endpoint and End Users – weakest link and where data is created - protect user & data. Extending EPS to protect the business and comply with regulations through policy control



There is no antidote to ransomware...currently.



“The ransomware is that good...To be honest, we often advise people just to pay the ransom”*

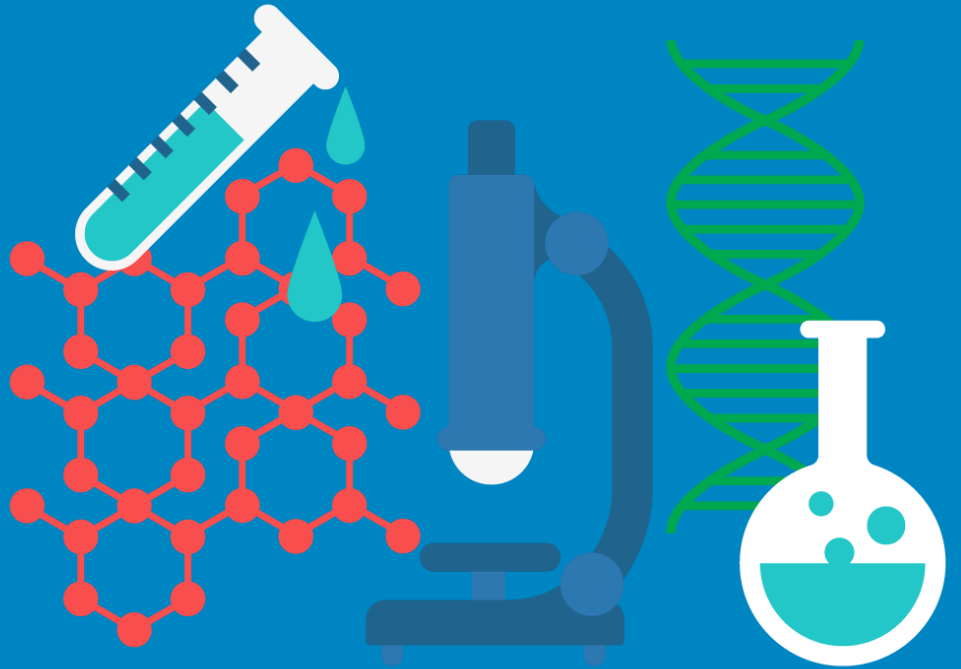
*Joseph Bonavolonta, Assistant Special Agent in Charge of the Cyber and Counterintelligence Program in the FBI's Boston office

Dell Advanced Threat Protection

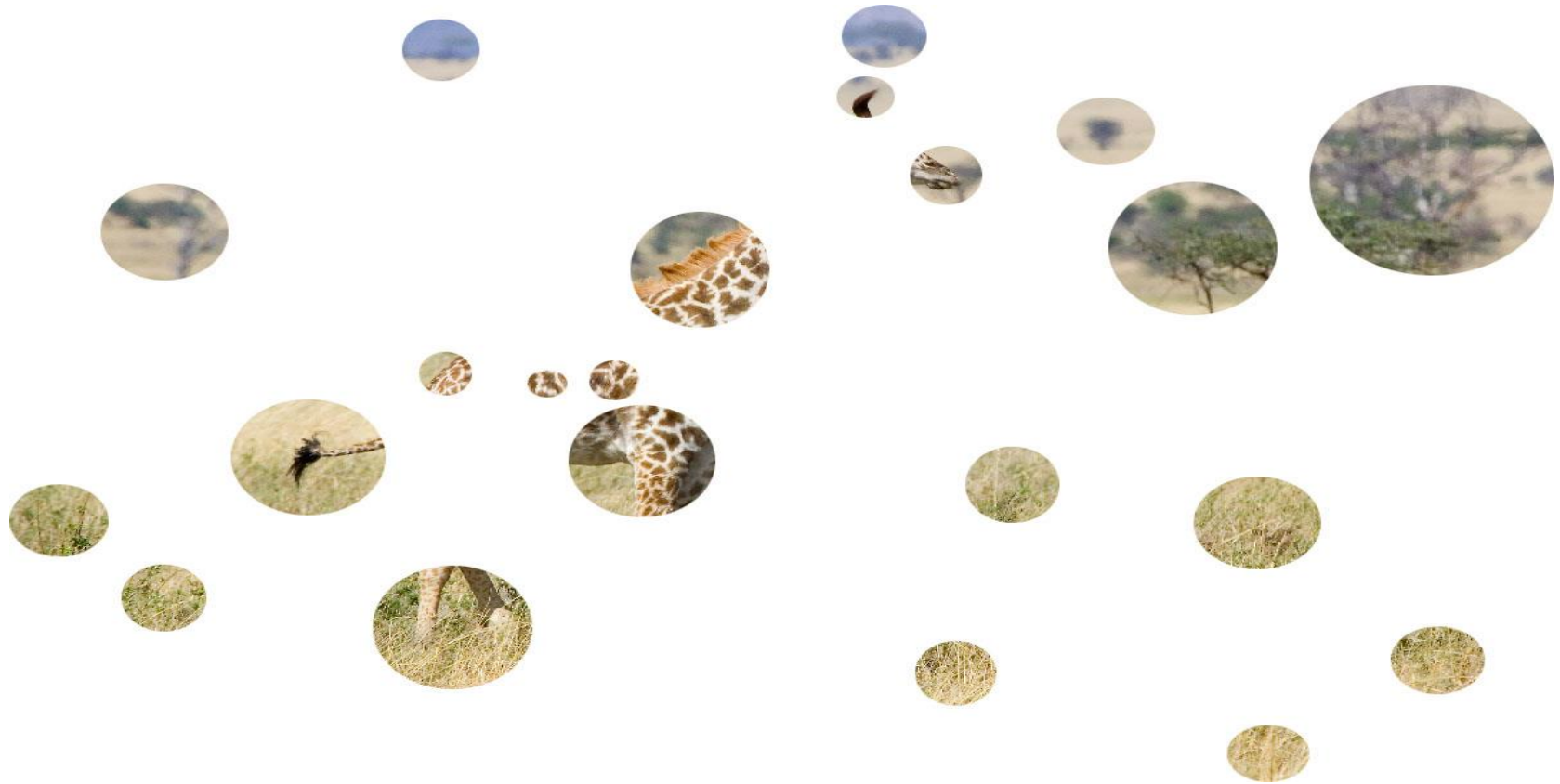


The cure for malware

Dynamic mathematical models & Artificial Intelligence unlock the DNA of advanced threats



Feature-Detection





What is Advanced Threat protection

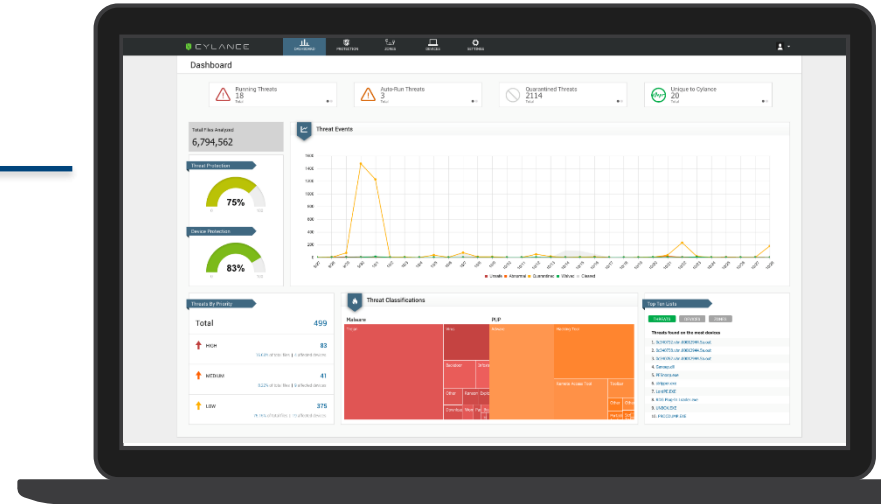
Powered By cylance

Unrivaled Threat Prevention & Protection

- ➔ PREdicative
- ➔ PREventative
- ➔ PRE-Execution
- ➔ PRE-Zero-Day

Enterprise Ready

- Microsoft Approved AV
- Windows and Mac OSX
- Web-based Console
- PCI-DSS Compliant
- HIPAA HITECH Compliant



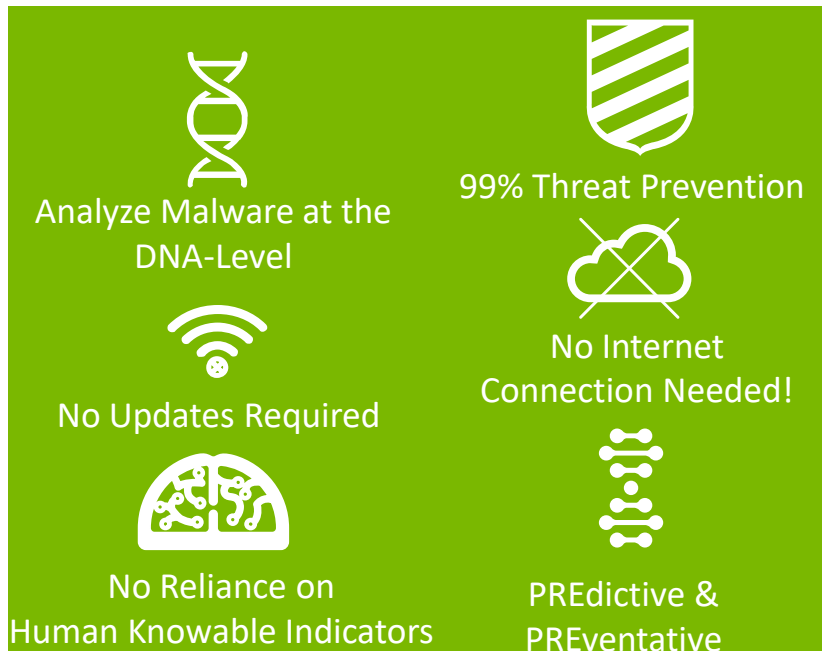
Lightweight & Flexible

1-3% CPU / ~60 MB Memory Footprint

The Capabilities of Advanced Threat protection

Powered By cylance

What we do:



Analyze Malware at the DNA-Level

99% Threat Prevention

No Updates Required

No Internet Connection Needed!

No Reliance on Human Knowable Indicators

PREdictive & PREventative

What we don't do:



Rely on Human Classifications

Signatures

Heuristics

Wait for Threats to Execute

Behavioral Analysis

Require Frequent Updates

Micro-Virtualization

Sandboxing

Dell Data Guardian



Data protected, at every step in it's journey

Encrypt my data



Define data use



Control access



Keep track of my data



Ensure data is not susceptible through encryption on the go

Digital rights management enables detailed policy control

Control who can access the data, where, and when with contextual access

Simplified data visibility

Dell Data Summary



The result: better security, better business



Protect

outside in and inside out –
efficiently and proactively



Comply

with regulations and
achieve consistent,
reliable governance



Enable

Users to do their work and
the enterprise to embrace
new technologies faster



Thank You

fergal.murray@dell.com