Dell Cyber Security Services Overview: Massachusetts Technology Collaborative

Ryan Reilly, MBA-Cybersecurity Advisory Consultant / Strategic Partnerships
March 9th, 2023
Ryan.Reilly@Dell.com
Agenda

➢ Healthcare security breaches and impact
➢ Security threats are increasing
➢ Cybersecurity Services - NIST
➢ Dell MDR Solution
➢ Dell IRR Services
Healthcare organizations are desperate to stay out of the news

$10M
Average cost of a healthcare security breach in IBM

34%
of attacks in 2022 involved an insider verizon

69%
of respondents not confident in ability to recover DELL Technologies

82%
of employers report a shortage in cybersecurity skills CSIS
Security threats are growing…

- 148% spike in ransomware attacks on global organizations¹
- 1.3x y/y uptick in confirmed data breaches in 2022²
- $10.5T estimated cost of global damages from cybercrime by 2025³
- 84% of IT leaders report data loss prevention is more challenging with a remote workforce⁴
- 48% of employees say they’re less likely to follow safe data practices when working from home.⁴
- 76% of IT security decision makers say their organization’s use of endpoint devices increased since the beginning of the pandemic⁵


…and remote work is intensifying complexity.
Security threats are growing

Endpoints are an expanding attack surface

<table>
<thead>
<tr>
<th>44%</th>
<th>62%</th>
<th>82%</th>
</tr>
</thead>
<tbody>
<tr>
<td>of organizations reported at least one hardware level or BIOS attack in 2020(^1)</td>
<td>of network breaches in 2021 attributed to supply chain vulnerabilities(^2)</td>
<td>of breaches were driven by individual error, e.g., phishing attack(^2)</td>
</tr>
</tbody>
</table>

**Unsafe Hardware**
- Replication through removable media

**Supply Chain Compromise**
- External remote services

**Social engineering**
- Valid Accounts

---

\(^1\)Futurum Research, 2020 \(^2\)Verizon DBIR Report, 2022
Dell Cybersecurity Services Overview
Holistic approach: NIST Cybersecurity Framework

Mature programs incorporate secure technologies with the people and processes to increase cyber resilience.

IDENTIFY
- Asset discovery & management
- Cybersecurity Assessment
- Business Impact Analysis
- Resiliency Strategy

PROTECT
- Endpoint
- Identity & Access Management
- Communications & Collaboration
- Data & Applications

DETECT
- Managed Detection & Response

RESPOND
- Incident Response & Recovery

RECOVER

Cyber Recovery Solution

Continuous learning and skills validation
Dell Trusted Workspace

- **Manufacturing**
  - Advanced Secured Component Verification (SCV)

- **Assembly & Customization**
  - BIOS & Firmware Verification
  - NIST Drive Sanitization
  - Pre-Imaging
  - BIOS Secure Configuration

- **Shipping & Delivery**
  - Tamper Evident Packaging Options
  - Device Tracking Option via Absolute
  - BIOS Verification
  - Indicators of Attack (IoA)
  - Firmware Verification (e.g., Intel ME Verification)

- **Built-in Solutions**
  - Built-on Solutions
  - Built-in Solutions

- **Built-with SafeSupply Chain Security Capabilities**

---

**Dell Technologies Offerings**

- **End User Lifecycle**
  - Dell Trusted Device
  - Secure Digital Fulfillment & Dell Verified Components Secure & Sustainable Device Retirement

- **Device Discovery**
  - Intel Integrations
  - Threat Telemetry
  - Authenticated BIOS Interface
  - Advanced Secure Component Verification
  - Intel Device Threat Telemetry
  - Dell Device Threat Telemetry

- **Automation | Prioritization | Orchestration**

- **CSO & CTO Dashboards**
  - SIEM Integrations (e.g., Splunk)
  - Ticketing & Alerting (e.g., Service Now)

- **Other "Top Quadrant" Leaders**
  - Microsoft
  - VMware

- **Other Top Vendors**
  - Carbon Black
  - Netskope

- **Security**

---

**Dell Solutions**

Holistic portfolio that simplifies endpoint management

---

**Dell MDR**

**VMware**

**Built-on Solutions**

**End User Lifecycle**

**Device Discovery**

**Automation | Prioritization | Orchestration**

**CSO & CTO Dashboards**

**Other "Top Quadrant" Leaders**

**Other Top Vendors**

**Security**

---

**Dell Solutions**

Holistic portfolio that simplifies endpoint management

---

**Dell MDR**

**VMware**

**Built-on Solutions**

**End User Lifecycle**

**Device Discovery**

**Automation | Prioritization | Orchestration**

**CSO & CTO Dashboards**

**Other "Top Quadrant" Leaders**

**Other Top Vendors**

**Security**

---

**Dell Solutions**

Holistic portfolio that simplifies endpoint management
Dell Managed Detection & Response Services
Dell MDR Solution – People, Processes & Technology

People and Process
- Threat Hunting
- Threat Engagement Manager
- Isolate or take actions on devices
- Certified and Experienced Analysts

Managed Detection and Response
- 24/7 Global SOC
- Usage of Additional Tools
- Remediation (40 hrs / qtr)
- Expertise to identify attack patterns
- Incident Response (40hrs / year)
- Quarterly Reports
- Noise Reduction / Tuning
- Perform Complex Investigations

Technology
- Artificial Intelligence
- Machine Learning
- Use Cases
- Tactics Engine

Data Ingestion – XDR Cloud
- Carbon Black
- CrowdStrike
- Fortinet
- SonicWall
- Palo Alto
- Azure / O365
- Cisco
- Juniper
- Symantec
- Amazon AWS
- Okta \ ZScaler

Endpoints
- Antivirus
- EDR

Network
- Secureworks XDR (Extended EDR)

Cloud

Endpoint security evolution
Dell Managed Detection & Response Service with Incident Response & Recovery
Accelerate security initiatives and become more resilient

Providing strategy to full-scale implementation by incorporating secure technologies with the people and processes to secure organizations

Skilled in threat investigations, threat hunting, endpoint security, incident management and security consulting

Analysts are certified with a wide range of industry certifications including GIAC SANS, CEH, CISSP's, CompTia etc.

Microsoft Advanced Specialization in Threat Protection and Identity and Access Management with numerous competency achievements including Information Protection and Governance, Cloud Security, and more.

97% success rate in helping customers recover after experiencing a cyber event

Over 20 Years of business resiliency innovation

750+ Cyber Recovery Services customers

1Based on Dell analysis of service requests from June 2019 to July 2021 in North America.
Prioritizing your next steps toward cyber resilience

Focus on how your organization would detect, respond and recover from a cyber attack

Managed Detection and Response

Cyber Recovery Solution

Incident Response and Recovery

Managed by Dell Technologies Services

Incident.Recovery@Dell.com