Enhance your vulnerability management program, prepare against ransomware attacks, and map your Zero Trust Initiatives

Gain a clear view of your current state and what it takes to meet your goals

Dell Cybersecurity Advisory Services

With the increasing digitization of businesses and the value of the data they generate, organizations need to better understand their cybersecurity strategy. From vulnerability management to ransomware readiness and recovery after a cyberattack, having the people, processes, and technologies in place to better protect the business and become more resilient is essential to ongoing operations.

Vulnerability management is a key part of improving cyber hygiene, but also presents challenges for many. Organizations need to rely on advanced tools to help discover, assess, and remediate vulnerable IT assets across the business. However, due to the number of known vulnerabilities, this is challenging and requires understanding the context around those vulnerabilities by applying relative risk to the business and other key metrics to drive prioritization.

2021: Over **20,000** known vulnerabilities

or

an increase of **10%** over 2020[1]

Beyond managing vulnerabilities, organizations have also highlighted a general lack of awareness and shortage of skills associated with preparing and defending against a ransomware attack. With the average cost of a ransomware attack costing $4.54 million*, the economic, legal, and reputational impacts of a ransomware attack throughout the initial disruption, and at times, prolonged recovery are a top of mind issue for many organizations- big or small.

In addition to this, organizations also struggle with defining a cybersecurity strategy which considers gaps, opportunities, and business risks to clearly prioritize initiatives. Without a clearly defined path to improving cybersecurity posture, experts within the organization are jumping from project to project without a clear top-level goal to unify the organization around the broader objective of reducing risk to the business. There must be a better way!

Key benefits:

- Scan for vulnerabilities and prioritize action
- Advance your vulnerability management program with expert advice
- Assess your readiness to counter ransomware threats and receive recommendations to enhance your security posture
- Gain a roadmap for achieving your Zero Trust goals by aligning your existing investments with a long-term vision, documented in a detailed deliverable

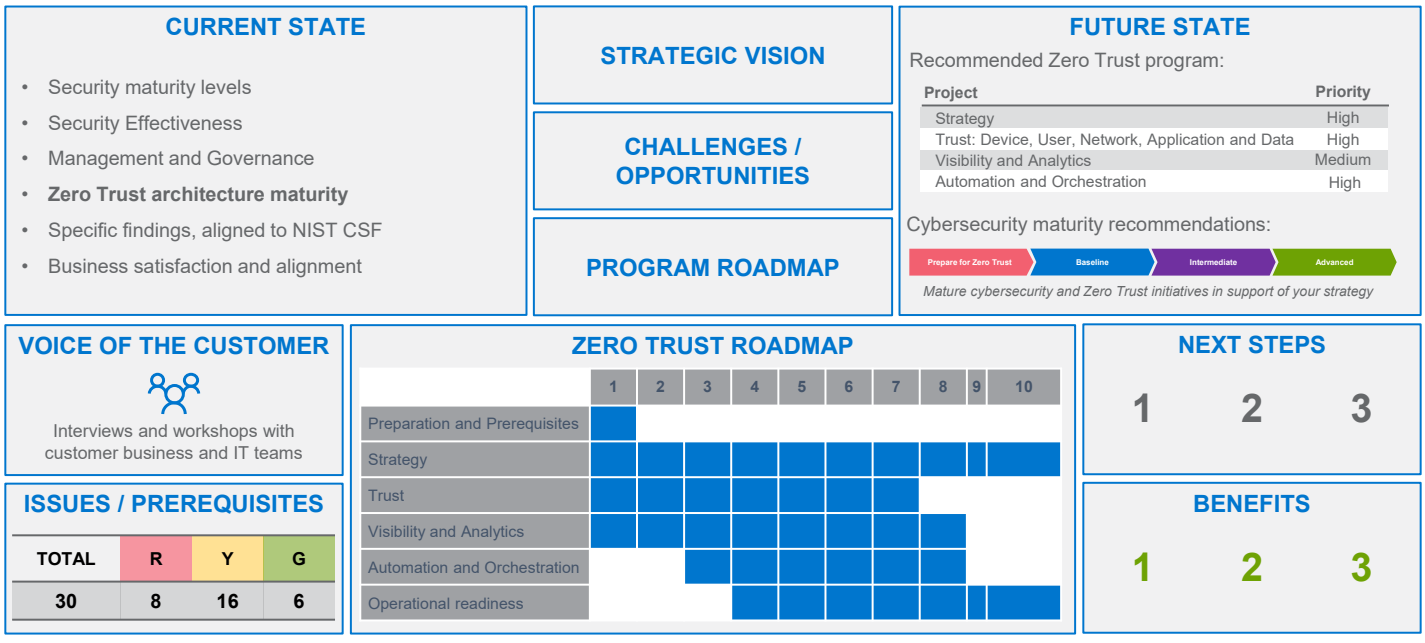
The Dell Cybersecurity Advisory Services facilitate a plan for beneficial and lasting change. Our cybersecurity consultants work with you to determine how to build maturity in your vulnerability management program, prepare against a ransomware attack and chart a path to achieving your Zero Trust goals. Our services are designed to help assess your cybersecurity planning and advise you on the best course of action based on the needs of your business.

We work with you to evaluate your IT assets, scan and prioritize exposures and identify threats and risks. Our consultants use advanced tools which apply context to individual vulnerabilities and inform prioritization. This is essential in better understanding what to address first, not only relying on the merits of the individual exposure, but also on potential impacts to your business based on the technologies you're using. The vulnerability scan results are detailed in actionable documentation and reviewed with your teams during an advisory session where we make recommendations based on vulnerability management best practices.

In our Cybersecurity Advisory Core Service, we build on top of vulnerability scanning and recommendations to assess your organization's tools, technology, and processes, and ability to defend and mitigate the impact of a ransomware attack. Our Service is delivered across 5 weeks, where we analyze and assess your existing cybersecurity policies and compare these to established cybersecurity best practices. In doing so, you will receive an assessment score along with recommendations under different assessment domains on how to enhance your security posture and mature your readiness for a ransomware attack. Our Ransomware Readiness Assessment, which is tightly aligned to the NIST Cybersecurity Framework, offers a holistic service so that your organization can feel confident in your ability to identify, protect, detect, respond and recover from a ransomware incident.

In the Cybersecurity Advisory Plus service, we build on top of the vulnerability scanning and ransomware readiness assessment and recommendations with a workshop focused on Zero Trust and advising on policies, technologies and how to best align your organization. We understand that you're already on the path to Zero Trust and have investments across IT which enable various aspects of Zero Trust. This workshop is all about aligning where you are today with a vision for the future with actionable steps to better secure your organization. The Dell Technologies approach to Zero Trust is tightly aligned with National Institute of Standards and Technologies (NIST) and Department of Defense (DOD) standards for achieving Zero Trust. This model enforces trust across devices, users, sessions, applications and data through centralized policy management and driven by deep analytics and visibility and automation and orchestration across the stack. This is all documented on an easy-to- understand view showing current state, a program roadmap and the future state including risk optimization and return on investment (ROI) analysis.

Actionable deliverables clearly chart your path



For details contact your Dell representative or visit **DellTechnologies.com**

[1]Vulnerability Visualizations: National Institute of Standards and Technology https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time. IBM, 2022. For more information: https://www.blackfog.com/the-true-cost-of-ransomware-attacks/#:~:text=According%20to%20IBM's%20latest%20data,that%20play%20in%20ransomware%20recovery.