Dell Technologies

Channel Secure Podcast

Episode 2: Total Chaos Requires Zero Trust

Telemarketing Script

Given the cyber security threats customers face, they need you to be a Trusted Advisor. Dell and Microsoft will help that happen. This script covers important topics from Episode 2. Our goal is to make complex security topics clear so you can approach customer conversations with confidence. Use this script to talk with customers by phone or video conference. Follow up with a quick email with links to informative resources such as infographics and white papers. Your customers will gain more insights and you can continue the conversations. You know your customers best! Tailor your communications to their needs and expectations.

Topic: Starting the conversation

Partner: *When purchasing servers, how much of a concern is cyber security for your business?*

Customer: *Very important…*

Partner: *You’re not alone. Businesses rank data privacy and cybersecurity concerns as the # 1 barrier to digital transformation. As servers become more critical in software-defined data center architecture, server security becomes the foundation of overall security.*

Customer: *Yes, it’s kind of overwhelming. I don’t know where to start….*

Topic: Factory Load

Partner: I’m happy to help walk through some great places to start.

Customer: *Yes, let’s do it.*

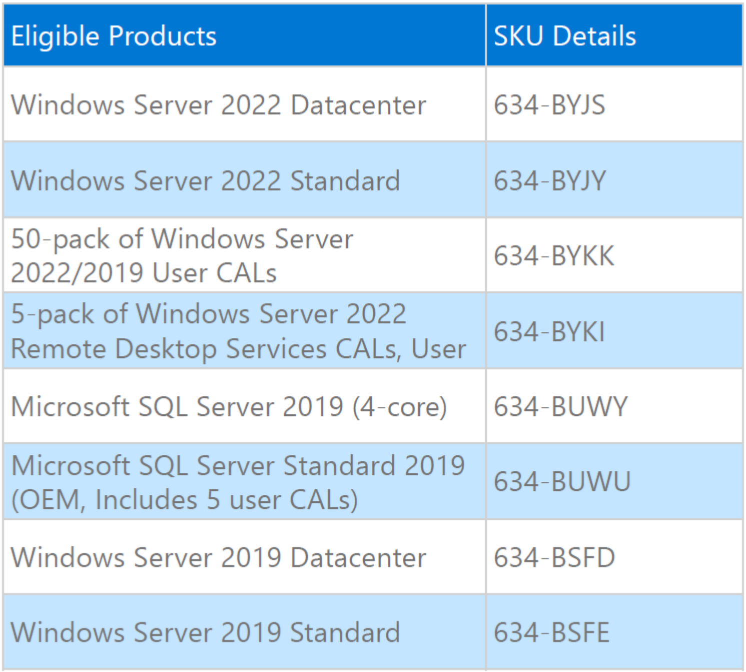
Partner: I’m hoping it can give you peace of mind that in this environment of cyber threats, Dell has created processes that help keep your servers safe. And a really good place to start is factory loading.

- Factory loading of options such as Microsoft Windows Server 2022 may be the easiest and safest thing you can do when buying a new server.
- In the past we thought of factory install as a time-saving convenience – which it is, but in this environment full of cyber threats, factory loading is a process that actually helps keeps your servers and data safer. So, I really recommend it.

Customer: *Sure, that’s something I can do if you help set it up.*

Partner: *I can definitely do that!*

TIP: Use this handy Dell SKU Quick Reference to help customers get Microsoft products like Microsoft Windows Server or Microsoft SQL Server factory installed on Dell EMC PowerEdge Servers.



Eligible Products	SKU Details
Windows Server 2022 Datacenter	634-BYJS
Windows Server 2022 Standard	634-BYJY
50-pack of Windows Server 2022/2019 User CALs	634-BYKK
5-pack of Windows Server 2022 Remote Desktop Services CALs, User	634-BYKI
Microsoft SQL Server 2019 (4-core)	634-BUWY
Microsoft SQL Server Standard 2019 (OEM, Includes 5 user CALs)	634-BUWU
Windows Server 2019 Datacenter	634-BSFD
Windows Server 2019 Standard	634-BSFE

Topic: Security Risks

Partner: *You mentioned earlier that cyber security can seem overwhelming.*

Customer: *It really is, and you hear about cyber-attacks all the time.*

Partner: *Yes, every day cyber-crime becomes a bitter reality for companies all over the world. Data's being used across many devices, on premise, and in the cloud, and high impact data breaches continue to mount.*

Customer: *It seems our risks are growing more complex every day.*

Partner: *Well, they are, and now you might have employees returning to the office with sloppy cybersecurity habits such as downloading unauthorized software.*

Customer: *Yes, that's a concern.*

Partner: *Plus, if we look at the really big picture, right now there's significant cybersecurity risks coming from the Russia-Ukraine conflict. I'd be happy to send you a* New York Times *article about it which also talks about what Microsoft is doing regarding this.* *https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html*

Customer: *Yes, can you email it?*

Partner: *Done. You may have also heard about what's called a "Multistage cyber-attack", which is really the way most cyber criminals operate today. Have you heard of it?*

Customer: *I've heard of it but not sure I understand the ins and outs of it.*

Partner: *Well, it's pretty sophisticated. A Multistage attack is breach that's accomplished through several different steps through a false sense of trust. Another word for it is "The Kill Chain."*

Customer: *Geesh! Can you walk me through an example?*

Partner: *Of course. Today, the criminals might access the email account of a cousin of a security guard's girlfriend. Then trick the guard's girlfriend to give them a piece of information they can use to get the guard's email address. The guard gets an email the next day that says "IMPORTANT CHANGES TO HEALTHCARE COVERAGE COMING SOON." The guard doesn't recognize the sender but he feels the urgency so he downloads the form, verifies some important personal information, and send back the form.*

Customer: *That can't be good.*

Partner: *You guessed it. They use the information to crack his work email password. Then the criminals watch and wait, reading his work mail. And nobody knows. Then they see an email that this weekend the company is renovating the vault and for one day they're leaving a side door open for maintenance crews.*

Customer: *Wow.*

Partner: *Yeah, the Kill Chain is accomplished through several different steps. They probe for ways to fool the system, to get it to trust things it shouldn't. This is what we mean by false trust.*

Customer: *Yes, this is why I'm overwhelmed.*

Topic: Zero Trust

Partner: *And that's understandable given these threats. The good news is there's an important concept from Microsoft and Dell that addresses this. I think once you hear about the approach, you won't feel overwhelmed. You* might even *feel confident.*

Customer: *OK! I'm all ears. Please tell me.*

Partner: *The concept is Zero Trust. In the multi-stage attack example, you remember that the criminals were able to establish a False Sense of Trust that allowed them to establish their Kill Chain.*

Customer: *Yes, that was pretty disturbing.*

Partner: *Well, Zero Trust is the opposite of that.*

Customer: *OK…*

Partner: *Zero Trust is actually both a mindset and tactics. First, let's talk about the mindset. There are 3 Principles. Would you like to hear them?*

Customer: *Yes, but how complicated are they?*

Partner: *Not as complicated as you might think!*

- *The first principle is to **Verify Explicitly.** This means don't assume anything. Verify across all data points.*
- *The second principle is to **Use Least Privilege**. This means limiting access to just enough access, making that access compartmentalized*
- *And the third principle is to **Assume Breach**. This is an important one in today's world, where you want automated threat detection and response.*

This may sound like a lot but Dell and Microsoft provide the manageability that automates this in practice.

Customer: *Yes, I could see how automation is a good thing.*

Partner: *Would you like me to send you Microsoft's white paper on Zero Trust? It will help you understand this mindset that is fundamental to modern cyber security.* https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT

Customer: *That would be great.*

Partner: *I'll also attach an Infographic that shows how Dell applies Zero Trust across all your data points – users, devices, network, data, and threat detection. This is the new standard in cyber security.*

https://www.delltechnologies.com/asset/en-us/products/servers/briefs-summaries/dell-zero-trust-architecture-infographic-infographic.pdf

Topic: Cyber Resilience

Partner: *So, the good news is Dell has a leadership position in server security to help your business grow with confidence. We talked about the Zero Trust mindset. It's a fundamental piece of Dell's End-to-End Approach to Cyber Resilience.*

Customer: *I've never heard the phrase "Cyber Resilience." What does it mean?*

Partner: *It truly is End-to-End and about being resilient. It's about protecting infrastructure, detecting threats, and also rapidly recovering from cyber-attacks when they do happen. It's a comprehensive path to secure server infrastructure. Dell and Microsoft have this covered. Cyber Resilient Architecture includes the embedded server firmware, the data stored in the system, the operating system, peripheral devices, and the management operations within it.*

I have both a Dell Infographic and a White Paper about Cyber Resilient Architecture I'd be happy to share.

- *Infographic: https://www.delltechnologies.com/asset/en-us/products/servers/briefs-summaries/dell-emc-poweredge-cyber-resilient-architecture-2-0-infographic.pdf*
- *White Paper: https://dellmicrosoftserver.com/wp-content/uploads/2022/03/common_dell-emc-poweredge-cyber-resilient-security.pdf*

Customer: *Yes, please send the assets. I'd like to learn more about it and get a sense of the framework.*

Topic: Make a plan to continue the conversation

Partner: *Once you understand Cyber Resilience and Zero Trust, you really will have a solid framework for how to approach modern cyber security for your business. Dell and Microsoft have established these processes. And servers are a foundation for overall security.*

As I mentioned before, a starting point is to have options such as Microsoft Windows Server 2022 factory loaded. Factory install is not only a time-saving convenience, it helps keep your servers and data safe.

Customer: *Yes, I'm feeling more confident already.*

Partner: *Great! Remember I'm here to help advise you on cyber security. Take a look at some of the Dell and Microsoft assets I emailed you, and let's talk more next week about the best security approaches and solutions for your business!*