# The Cybersecurity Readiness Podcast Series

| | |
|---|---|
| **Episode Title** | Preparing for the Future of Device Management |
| **Podcast Series** | The Cybersecurity Readiness Podcast Series<br>https://www.dchatte.com/podcast/<br>https://the-cybersecurity-readi.captivate.fm/ |
| **Host and Producer** | Dave Chatterjee, Ph.D.<br>https://dchatte.com |
| **Guest** | Mike McNeill, CEO, Fleet Device Management, |
| **Summary Pitch** | With the growing move towards a hybrid and remote work environment, more and more people are relying on their smart devices to get work done. Keeping track of all of these devices, and ensuring that they are being used in a very secure manner, can be a challenging proposition. A recent survey finds organizations unprepared and overwhelmed with managing thousands or hundreds of thousands of these endpoint devices. Mike McNeill, CEO, Fleet Device Management, sheds light on some of these critical security issues and addresses questions such as: How does an organization manage its devices? Do they know if their devices are compliant and secure? Do they have ways to query them to learn more about their status in real-time? Mike also offers recommendations on how to prepare for the future of device management. |
| **Time Stamps** | 01:28 -- Share with the listeners some highlights of your professional journey.<br><br>02:11 -- Let's talk about the motivation for the study.<br><br>03:54 -- The study is fairly recent; it was started on February 25, 2022. It was conducted online via Pollfish using organic sampling. And when |

| | |
|---|---|
| | I look at the industry is represented. It's pretty comprehensive. You all didn't leave out any sector. Am I correct?<br><br>04:52 -- Were you surprised by the survey findings relating to the state of device management?<br><br>06:48 -- Talking about managing the devices and keeping track of the devices, I read here that only a quarter of the sample population said that their devices are fully enrolled and upgraded. You know, that's worrisome. Why do you think organizations would allow that to happen?<br><br>07:54 -- So, if I'm understanding you correctly, the use of multiple operating systems and multiple platforms is part of the problem when it comes to tracking the devices, right?<br><br>08:33 -- Another finding that got my attention is that one of the best practices is to have a good Bring-Your-Own-Device (BYOD) policy. And to be more specific, 32% said, having a documented BYOD policy is a crucial best practice for their MDM (mobile device management) strategy. Can you expand on this?<br><br>09:57 -- BYOD, Bring Your Own devices, as an approach has its pros and cons. It was interesting to read that 32% of the respondents felt that having a documented BYOD policy is a crucial best practice for their MDM strategy. What are your thoughts?<br><br>11:49-- Another best practice documented here is measuring point-in-time compliance across all devices. Share with the listeners what you mean by point-in-time compliance or real-time compliance across devices.<br><br>13:56 -- How feasible is it to try and automate the patching process and thereby remove the responsibility (of patching) from the users?<br><br>17:51 -- Another finding that I find interesting is that multi-factor authentication becoming a top priority for 2022. The reason I find it interesting is I would assume that by now, multi-factor authentication |

| | |
|---|---|
| | would be a standard. I wonder why the delay in the adoption of a security mechanism that is universally accepted to be a very robust protective measure. What are your thoughts?<br><br>19:35 -- What were some unanticipated or unexpected findings?<br><br>20:59 -- I think the extent to which security and IT teams can work together and appreciate the significance of each other's work would make the development and implementation process more effective and efficient. What do you think?<br><br>23:12 -- What would you say to organizations interested in improving device management? How should they prepare themselves?<br><br>25:46 -- Going back to the report, where you're talking about preparing for the future of device management, you have several recommendations, one of which is to start managing containers. Can you expand on that?<br><br>28:21 -- Another recommendation in this report is to protect remote workers with zero trust, TLS, and multi-factor authentication. I'd like you to expand on this TLS when you suggest " move away from VPNs to granular proxies with TLS." Can you explain this?<br><br>30:38 -- Share some final thoughts with the listeners. |
| **Memorable Mike McNeill Quotes/Statements** | For endpoint security and risk management overall, you are starting to see more security engineers and security operations roles live in the IT department, and you're starting to see more IT engineering roles effectively taking on security challenges. And I think there's an argument to be made that in a couple of years, we're gonna see blended IT and security departments. So they will not be all that distinct anymore, other than the risk management aspect and crunching the numbers. |

| | |
|---|---|
| | I think your success then comes down to, can we take inventory of what we have, and look at this from first principles, like, what are we trying to achieve here? We have a security posture we want to get to, we need to have an accurate inventory, and we need to make sure that we're collecting the right data that we can empower our security team with to like go run and build what they need themselves without having to go ask IT for more and more data every time.<br><br>If you are pocketed in and are part of a big organization, look for ways to find portable formats and solutions that don't lock you into a particular future, and that can work for other people in your company, even if they do have to use a different set of tools. |