DELL EMC

Security for the modern worker

Empower employees to work their way while protecting your data wherever it goes.

Today data is constantly on the move, which poses new threats to security. IT must be able to address these new risks without restricting the flow of information—findings discovered in a recent Forrester report, *Evolving Security to Accommodate the Modern Worker.** Brett Hansen, Vice President of Client Software and General Manager of Data Security, shares his insights on the report and the solutions Dell provides to meet the needs of employees and IT.

Why is protecting data important?

There are three answers to this question. The first is that there are regulations that require protection of certain types of data. This is typically customer data, like patient information in healthcare or employee information. There are increasingly serious consequences if you don't meet these requirements. So at the very minimum, you're required to protect data.

Second, data is the lifeblood of companies today. Regardless of what industry you're in, data is the most important part of your business and having it compromised could be catastrophic to your company's health. The third is brand reputation. Being able to protect your company's data is an expectation that's universally shared. Whether it's complying with data protection laws, to recognizing the importance data has as the underpinnings of your business, to brand reputation, all three of these are essential.

> "Regardless of what industry you're in, data is the most important part of your business and having it compromised could be catastrophic to your company's health."
>
> **Brett Hansen,**
> Dell's VP of Client Software and GM of Data Security

The Forrester report states employees believe security makes them less productive. Why do you think this is the case?

Companies employ security solutions and set policy that's increasingly restrictive. If you take your data and lock it in an airtight environment where no one can get to it, it's a lot safer, but the whole point of having data is being able to use it. Employees want to mine the customer database for insights, collaborate with colleagues and share best practices. All of these things require the movement of data.

IT professionals aren't trying to make it more difficult for employees to do their jobs, it's just because they're using more traditional, legacy-based solutions. If you look at the policies and technologies deployed in the last year, it encumbers what people want to do with their data, which is to collaborate and drive business momentum forward.

How can we find a middle ground between IT and employees? Can IT tailor security solutions to different workers and occupations?

It starts with a conversation. Business professionals and the cyber security team have to sit down and ask, "What is our line of business strategy?" and "What are we trying to do from a people perspective?"

The next piece is knowing there's no one size fits all. Organizations and groups within that organization have different requirements. Policies and technology should reflect different needs. What typically happens is IT pushes a common security policy across everyone, versus being thoughtful about who these individuals are, their objectives and what tools they need to protect sensitive data.

How flexible can security be to address the needs of different types of workers?

It's a combination of policies and tools. You need to have the right policies, which are driven by a broader security strategy that informs employees what they can and cannot do. Employees want to be educated. They want to have these conversations and they want to be empowered. However, companies need tools to protect them because there are going to be threats from the outside and potential compromises. In regard to flexibility, the answer is simply yes it can be done, it just takes it back to "it all starts with a conversation."

You mentioned employees want to feel empowered. The Forrester report states workers are willing to manage their own security. Do you think they're equipped to handle this?

To answer the question simply, no. One of the findings from the Forrester report was that 62% of employees

say they're worried about being blamed for a security breach.* That's pretty shocking. Everyone is looking over their shoulder. There should be a sense of confidence that employees know what steps they need to take to protect their company's assets, and then include a set of capabilities to help them do that. Employees are people and people make mistakes and have accidents, but what you can do is align your trainings so employees have a sense of empowerment. They need to understand the types of security policies in place so they can embrace them, instead of fight against them. This approach, layered with security practices that give them the freedom to work their way, will bolster confidence and trust.

What's Dell's approach to protecting data? Which solutions do this best and how are we different from the competition?

There are a couple things that make Dell unique. We're newer to the security game than a lot of other companies. This is a good thing. Because we don't have a legacy portfolio that addresses outdated security problems, we're in a much better position to drive solutions that reflect today's workforce and today's challenges.

We consider the external attacker with Dell Endpoint Security Suite Enterprise (powered by Cylance), a machine-based learning, signature-less approach to detect malware and stop outside threats. We look at the

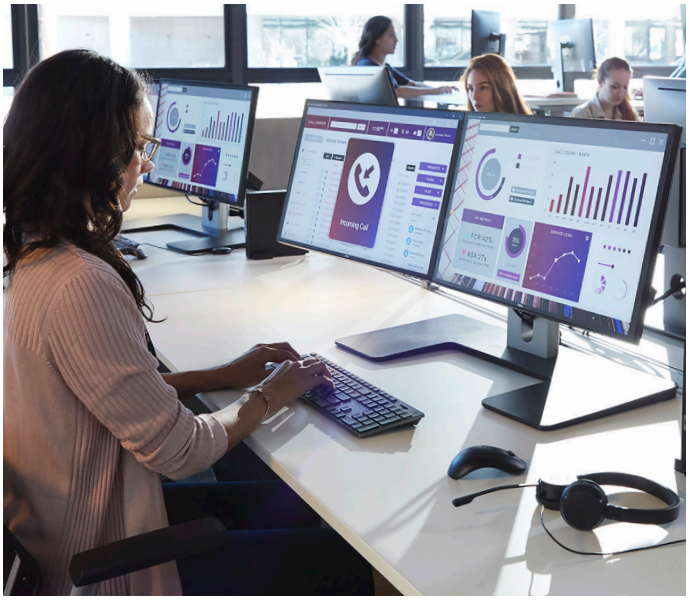
underlying code itself, so it's much more difficult for the attacker to disguise their intentions. And with machine-based learning, there is very little impact on the system as the machine scans files for potential malware—even when scanning hundreds of data points. Legacy solutions that scan for signatures will grind a system to a halt.

Lastly, we protect people from themselves. If policies prevent employees from doing their jobs, they find a way around it. They're not intentionally being malicious, they're trying to get their job done in the most efficient way possible. Rather than building walls and locking data down, our tools, such as Dell Data Guardian, let employees do their jobs and let IT protect, control and monitor files no matter where they are. Our process offers multiple facets of defense—we stop the bad guys, and then protect insiders from themselves.

> "If you create an environment where employees can work efficiently but still have a level of trust and capabilities to protect data, it's naturally going to be more productive."
>
> **Brett Hansen,**
> Dell's VP of Client Software
> and GM of Data Security

How can protecting and securing data encourage productivity?

If you create an environment where employees can work efficiently but still have a level of trust and capabilities to protect data, it's naturally going to be more productive. It goes back to the meeting between business and cyber



security. They need to have a conversation and set a strategy together.

In a perfect world, business and IT are aligned and have a strategy in place, but under a time crunch security has to move forward with policy. Regardless of where the business and security stand, there are tools Dell can provide that allow IT and employees to have the best of both worlds. Employees can stay productive without fear of creating a breach. Going back to that statistic—62% of employees are worried about creating a breach*—that's not a good environment. We want employees to feel confident they know what they're doing. Let's empower in a way that controls risk. The technology is out there, it just takes companies acknowledging this new paradigm and embracing these tools.

*Based on a study conducted by Forrester Consulting commissioned by Dell, *"Evolving Security to Accommodate the Modern Worker,"* October 2017.