FUTURUM.

FOUR KEYS TO NAVIGATING THE HARDWARE SECURITY JOURNEY

Ensuring enterprise-wide device security requires a shield, or security posture, that follows and protects devices throughout all aspects of the hardware journey, encompassing the external supply chain, internal implementation, and ongoing end-user operations and device management.

Q3 2020

DANIEL NEWMAN
Founding Partner + Principal Analyst

SHELLY KRAMER
Founding Partner + Senior Analyst

FRED MCCLIMANS
Research Director + Senior Analyst

Published: October 2020

IN PARTNERSHIP WITH

DELL Technologies

TABLE OF CONTENTS

Executive Summary

True security, or being secure, means having a shield or security posture that follows you through your journey, from the moment you place an order to the end of the device's life cycle. It protects you, your suppliers, your partners, and your users.

As security technologies have increased in sophistication for both threat actors and enterprises, cyber criminals have expanded their approach to focus on targets perceived to be less protected, many of which exist 'below the operating system' at the hardware level.

From lone individuals and groups to state-sponsored teams, the threats posed today and in the future are not and will not be confined to end-user or operational systems and will be felt throughout the entire ecosystem, from the first supplier to the final end user in software, hardware, and even the silicon itself.

This research, ***Four Keys to Navigating your Hardware Security Journey***, summarizes the highlights of a long-term research initiative begun in late 2019 and concluded in mid-2020.

This initiative was designed to better understand the level and type of threats encountered by organizations today, and the measures, practices, and policies these organizations employ to address these threats throughout the entire security journey.

Our research included an in-depth study involving over 1,000 technology and security professionals directly involved in the planning, implementation, management, or operations of security, risk, and compliance activities related to device-level security.

RESEARCH DEMOGRAPHICS

U.S. Federal Government (FED, 29%)
Including all federal agencies, departments and organizations.

State or Local Gov't & Education (SLED, 30%)
Including all aspects of state, local, county or municipal government including public and private education.

Defense Industrial Base (DIB, 17%)
Including defense-related organizations supporting aerospace; shipbuilding & combat vehicles; weapons, missiles & ammunition; technology (IT and electronics); and other related organizations.

Critical Infrastructure Sectors (CIS, 22%)
Including chemicals; commercial facilities; communications; manufacturing; dams; emergency services; energy; financial services; food & agriculture; government facilities; healthcare & public health systems; information technology; nuclear reactors, materials & waste; transportation; water & wastewater.

Commercial Industries (COMM, 2%)
Including businesses and organizations providing commercial products and services not directly related to government, defense, or critical infrastructure.

We're pleased to present this executive summary of four key insights derived from this research and invite you to explore deeper through this paper and our other related assets.

ONE: UNDERSTANDING YOU ARE THE TARGET

Security threats can come from all directions, both internal and external. They can be malicious or accidental. They can be found in both your end-user devices and throughout your partner ecosystem and supply chain. And they can be in software and in hardware.

> There's a common misperception that security threats are all about the software, and that smaller or less visible organizations are not often targets. This is simply not true.

In fact, two thirds of organizations say they've been the victim of a hardware-level attack in the past, with 44 percent saying it's happened during the prior 12 months (and for 16 percent, more than once). But the real story is that we believe those numbers are low, and that inadequate threat detection is hiding significant additional threats.

TWO: SECURITY IS BUILT FROM THE GROUND UP

There is no silver bullet for countering security threats. From improving advanced threat intelligence capabilities and verifying components in the supply chain to improving disaster recovery policies and isolating/ air-gapping resources within a network, enterprises are deploying a wide range of approaches to help secure their assets. And yet, 65 percent expect hardware vendors to provide platform security as part of their manufacturing and distribution process.

> Security and IT professionals that realize the significance of the threat have been laying the foundation for a stronger, more resilient security posture through a diverse range of initiatives and measures.

The challenge that we see today is for organizations to recognize the different stages of the journey that hardware and devices move through where each stage of the journey requires a tailored approach.

THREE: EVERY SECURITY JOURNEY NEEDS GUARDRAILS AND FRAMEWORKS

Established frameworks, such as NIST and MITRE ATT&CK, can allow an organization to focus beyond the hardware and software elements of security to the policies and procedures that form the foundation of an ongoing security discipline.

> Security must follow hardware and devices from A to B, and then to C and D, and it's critical to have a framework (or guardrails) to keep focused and on track.

And while these two frameworks are used often, over 30 percent of organizations say they don't use any security framework today, with over 20 percent indicating they don't plan to within the coming three years. This must change. Note that simply having secure hardware and software (or thinking that you do) does not replace the requirement for policies and procedures. Hardware alone isn't security, having the right policies and procedures in places is critically important.

FOUR: SECURITY PARADISE IS FOUND BY THE DASHBOARD LIGHT

From custom-built and internally-developed to commercial off-the-shelf tools, security dashboards are a critical component in the monitoring of the security journey. Organizations actively using one or more dashboards are twice as likely to report they've experienced a hardware-level security breach during the prior twelve months — you can't spot the dangers if you're not looking ahead.

> If security is a journey, it's the lights of the dashboard that illuminate the status of that journey and highlight both current and potential threats down the road.

ONE THE MYTH OF SECURITY

There's a common misperception that security threats are all about the software, and that smaller or less visible organizations are not often targets. This is simply not true.

Let's start our journey by breaking the Myth of Security that says, "It's all about software, and we're not a big target."

No, it's not, and yes, you are.

Security threats can come from all directions, both internal and external. They can be intentionally malicious or add an element of unexpected risk. The greater the number of devices or individuals within an organization, the greater the potential risk.

WE'VE BEEN HACKED!

44%

of organizations say we've had at least ONE Hardware-Level or BIOS Attack during the prior 12 months. External attacks are the most common, experienced by 56% overall. Who has been hit the most with external attacks? U.S. Federal government agencies top the list at 67%.

While malware, ransomware, data theft, phishing, and all manner of software or behavior-based threats that operate "above the operating system" get the major coverage, security threats that operate "below the operating system" (in hardware) can be equally difficult to detect and just as devastating. If basic principles such as intrusion detection, data integrity, or data theft can apply to software they also apply to hardware.

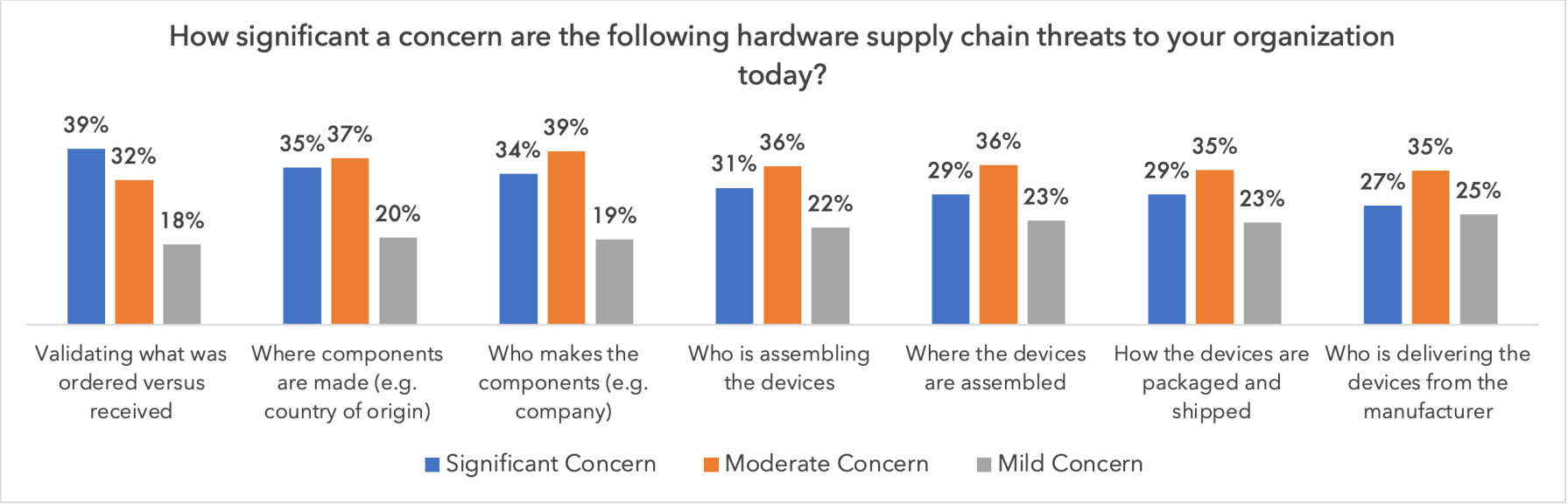
Security is a journey that begins in the supply chain.

It's important to understand the breadth of the security journey, and the requirement for organizations to develop and maintain a security posture that spans the entire journey, from the first component supplier to the ultimate end users.

While you may not believe you are a target, your suppliers, partners, or customers may very well be, and those threats can make their way into your organization. Maintaining an adequate security posture is an ecosystem-wide effort that must include all the various partners that hardware devices may transit along the way to your organization and again within your organization.

56% of organizations that are aware of data breaches during the prior twelve months say those attacks included external threats targeting their organization. Equally important are the 38% of organizations that say their data breach involved an accidental internal incident or user error.

When we talk about security in the supply chain, we're talking about a range of issues that need to be addressed at different stages of the journey, which we understand can be a challenge given the present forces disrupting global trade and the traditional supply chain model. But regardless of where a supply chain exists, there are certain waypoints on the journey that are consistent and can be addressed.



What are the top waypoints or concerns along the way? 39 percent of organizations cite the validation of what was ordered versus received as a significant concern (the top ranked significant concern). But concerns in the supply chain begin long before, including along the way:

- Individual component sources (country or manufacturer)
- Where devices are assembled (and the assembler)
- How devices (and components) are secured and shipped, including levels of tamper-resistance and physical security
- Storage facilities and warehouses during transit (including both physical locations and the organizations providing these services)
- Local delivery services
- Order integrity and verification (ordered vs received)

The key for any organization is to identify and assess the risks at the various stages of the journey that are relevant and important to their organization and the steps required to maintain an acceptable security posture.

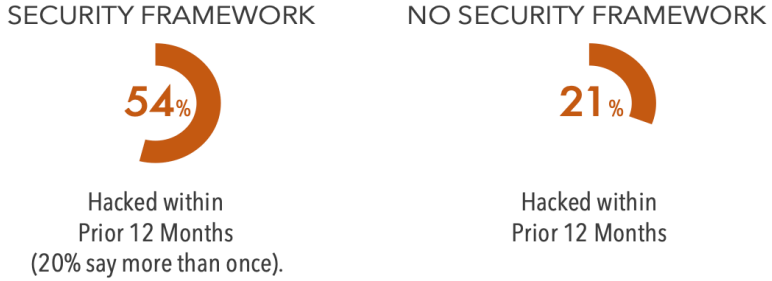
It's also important for organizations to understand that they themselves are part of the "supply chain" to their end users, and that security risks (and the steps required to mitigate them) don't stop at the arrival dock.

Threat detection begins with visibility and awareness.

While 44 percent of organizations say they've experienced an attack or breach during the prior twelve months, that number increases to 54 percent if the organization is using an established security framework and decreases to just 21 percent of those who do not employ a security framework.

IS IT A MATTER OF PERSPECTIVE?

Security breaches must be detected to be observed, and organizations with a security framework in place may be better prepared to identify (and stop) attacks.



To put it another way, you can't tell if you've been hacked if you don't have a policy or process in place to make sure you're looking in the right direction.

FUTURUM PERSPECTIVE

We take a broad view on the scope of security risks, spanning the intentional to the accidental, from theft to loss or corruption. If it impacts the performance of a device or process, we consider it a security risk — and the data on risks is clear. From our perspective, considering security risks is not so much a matter of asking 'was there a security breach' but rather 'when was the most recent event' and 'was it detected fast enough to mitigate the risk.'

Are organizations skilled at detecting hardware-level intrusions or attacks? Many are, but we're not convinced all are on the same level regarding visibility and awareness.

The security journey begins at the first component and requires a strong security posture that includes the ability of an organization to both understand and have visibility into the range of risks they face from the beginning to the present and ahead to the future.

TWO BUILDING A FOUNDATION FOR SECURITY IS A BROAD TASK

Security and IT professionals who realize the significance of the threat have been laying the foundation for a stronger, more resilient security posture through a diverse range of initiatives and measures.

Developing a strong security posture requires a broad foundation capable of addressing all the various waypoints along the hardware/security journey.

IT SECURITY INITIATIVES

53%

of organizations cite improving advance threat intelligence capabilities as the top IT Security Initiative. The use or implementation of cloud-based security services is #2 at 48% (and the top choice of state and local governments, including education).

There is no silver bullet for countering security threats. From improving advanced threat intelligence capabilities and verifying components in the supply chain to improving disaster recovery policies and isolating/air-gapping resources within a network, enterprises are deploying a wide range of approaches to help secure their assets. And yet, 65 percent expect hardware vendors to provide platform security as part of their manufacturing and distribution process.

The challenge that we see today is in organizations recognizing the different stages of the journey that hardware and devices move through and recognizing that each stage of the journey requires a tailored approach.

What are the most common efforts and initiatives organizations are taking to improve their security posture? It all starts with improving threat intelligence and detection, but that's only part of the complete story.

After assessing where an organization (or their hardware) is along the security journey, organizations need to ask several key questions:

- *What are the critical risks that are relevant to our organization?*
- *What is our true security status today? and*
- *Where do we need to be tomorrow?*

Not all devices or organizations have the same concerns or requirements. Answering these questions, and understanding this up front, is critical to assessing and prioritizing the steps that must be taken ahead. Only then can an enterprise answer the question of how they can best achieve their required security posture.

Where are our partners (and suppliers) in this journey?

Are they with you, behind you, or ahead of you? Not all partners and suppliers will be — or need to be — in the same part of the journey as your organization. But understanding where they are can help determine where the weak links may exist and how their risks, such as where and how devices have been assembled or shipped, may impact your ability to maintain a strong security posture.

How do we ensure that our own processes and distribution system supports (or integrates) with our incoming supply chain?

The same level of assurance you require from your suppliers must be available to your users and/or distribution partners.

What are the technologies, talent, and processes we need to develop and establish a viable security posture (and who are the providers and partners we need to help us along the way)?

When we look at the diverse range of initiatives that are being pursued within enterprise organizations today, it becomes clear that the breadth and depth of knowledge, technology, and processes can easily extend beyond the internal resources of even the most security-centric organizations.

For many enterprises, this goes beyond finding the right vendor, consultant, or advisor and leads directly to the decision to partner with a managed security services provider (MSSP).

In fact, the use of cloud-based security services and even the improvement of advanced threat intelligence can be provided through an MSS. Is this a trend? It certainly is a possibility, particularly in light of how rapidly both the supply chain and user requirements have changed over the course of the year.

THE GROWING ROLE OF MANAGED SECURITY SERVICES PROVIDERS

When asked to identify the top three initiatives organizations are taking today, the desire to leverage the skills of partners through managed security services breaks into the top three.

1. Improve Advance Threat Intelligence (45%)
2. Use/Implement Cloud-based Security Services (35%)
3. Use/Implement Managed Security Services (28%)
4. Verify Supply Chain/Source of IT Components (24%)

When it comes to supply chain security, organizations expect a lot from their vendors.

Over three quarters of organizations say they would prioritize supply chain security during vendor selection. But when it comes to the cost of supply chain security, 87 percent of enterprises say supply chain security measurements and standards are the responsibility of the device manufacturer and should be baked into the purchase price of equipment.

What are the top needs and expectations?

1. Firmware/BIOS Verification
2. Source/Origin Verification
3. Counterfeit Detection
4. Device Theft Prevention
5. Tracking (shipments and devices)

FUTURUM PERSPECTIVE

The one message that resonates throughout our research is that security initiatives, and maintaining a strong security posture along the journey, requires the commitment, collaboration, and partnership of an entire ecosystem — and that is a challenge for many enterprises. How do they build and maintain such a level collaboration across so many waypoints and risks?

THREE THE IMPORTANCE OF SECURITY FRAMEWORKS AND GUIDERAILS ALONG THE JOURNEY

If security is a journey that follows hardware and devices from A to B, and then to C and D, it's critical to have a framework (the rules of the road or guardrails) to keep focused and on track.

A security framework is essential in helping create the steps and processes necessary to implement a solid security posture. It won't specify the hardware or software used in a security system, but it will identify the behaviors of an attack, a common taxonomy to describe and identify threat behaviors, and the steps to remediate, and can be a significant aid in the improvement of an organization's security posture.

Security frameworks are also increasingly relevant to the evaluation and section of security providers, and that is key.

SECURITY FRAMEWORKS

30%

of enterprises use both NIST and MITRE ATT&CK during the evaluation of security providers.

Surprisingly, 31% use no framework at present. But while 23% say they are evaluating frameworks, 8% have no plans to ever adopt one (including 13% of US Federal agencies).

In fact, just over two thirds of organizations surveyed report using either the NIST or MITRE ATT&CK frameworks (or both) during the evaluation of security providers, directly impacting an organization's ability to create and maintain a solid security posture. Over the coming 18 to 36 months, we expect the use of both frameworks together to increase slightly, which makes sense, as the two are complimentary to each other.

From a practical perspective, the value of these frameworks can be found in the increased awareness of security issues they can foster. They allow an organization to go beyond the hardware and software elements of security to the more important foundation of the policies and procedures that form the foundation of an ongoing security discipline.

We believe that adherence to a security framework is key to knowing when (not if) you've been breached. To see the value of framework, or rules of the road, we can compare those organizations that do and do not utilize their value in establishing a security posture.

- 75% of enterprises that utilize a security framework say they have experienced a security breach in the past.
- 51% of enterprises that do NOT utilize a security framework say they have NOT been breached. Ever.

This increased awareness extends to other areas as well. When asked of supply chain measurements and standards are a key requirement in vendor selection, 51 percent of organizations that have adopted at least one framework would agree, compared to only 32 percent of non-adopters.

FUTURUM PERSPECTIVE

Based on our research, supply chain security is critical and while we can't draw a cause and effect, it does appear that those organizations that utilize a security framework are more security conscious and more likely to be aware of real-world threats.

> Security frameworks are essential in helping develop the enterprise-level policies that lead to a strong security posture. These policies, in turn, are critical in shaping the selection of the right vendors, technologies, and partners, including managed security service providers.

But frameworks are just that, frameworks. Key to successful implementation is how they are applied within an organization, and the successful translation of their guidelines into a set of policies and procedures that can help foster a strong security posture throughout the ecosystem and along all points in the security journey.

FOUR DASHBOARDS LIGHT THE PATH ALONG THE SECURITY JOURNEY

If security is a journey, it's the lights of the dashboard that illuminate the status of that journey and highlight both real and potential threats down the road

From custom-built and internally-developed to commercial off-the-shelf tools, security dashboards are a critical component in the monitoring of the security journey. It's not surprising that organizations that actively use one or more dashboards are twice as likely to report they've experienced a hardware-level security breach during the prior twelve months — you can't spot the dangers if you're not looking ahead.

DASHBOARDS

63%

of enterprises use one or more dashboards to view, monitor or manage the security of their enterprise devices (hardware or software). Of those that do, only 33% use just one while 20% use three or more.

Dashboard usage is fairly consistent across industries (with at least 60 percent in all sectors using two or more). Across all sectors, survey respondents indicated:

- Over half use a custom-built dashboard
- Over a quarter have developed a dashboard internally

Notably, enterprises utilizing dashboards are significantly more likely to have adopted both the NIST and MITRE ATT$CK frameworks as part of their security architecture (38 percent verses 15 percent who do not). In fact, 45 percent of enterprises without dashboard implementations report they have not adopted or utilized any framework at all.

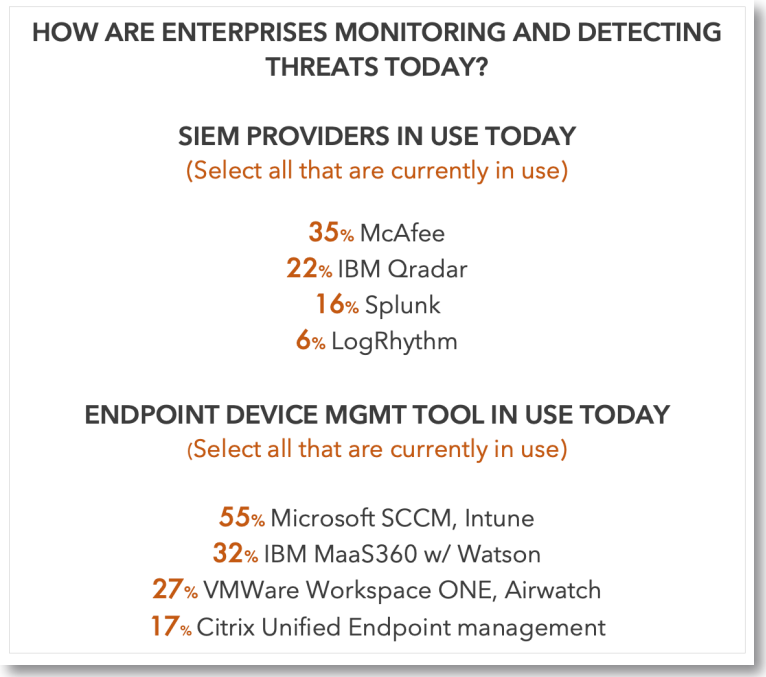
On the positive side, while only 63 percent of organizations report they are using dashboards today, 92 percent expect to be using at least one within 18 to 36 months.

Why the increase? Dashboards simplify threat intelligence.

Threat detection is all about data, massive amounts of data from sources such as Security Information and Event Management (SIEM) tools, Endpoint Detection and Response (EDR tools, and broader security alert and incident management tools.

Notably, 7 percent of US Federal organizations anticipate outsourcing dashboard functions entirely to a managed security provider. While we fully support the value an MSP brings to organizations, we also recommend enterprises maintain at least dashboard-level visibility into their provider's operations.

If security frameworks help define the rules of the road along the security journey, it's dashboards that provide the information necessary to monitor for security issues before they cause irreparable harm along the way. The information they provide is also used within the context of framework to properly apply the policies and procedures that enable a strong security posture.



Why the use of custom-built or internally developed dashboards? SIEM and Custom Need.

As organizations have become more digital over time, and as security threats have increased, security elements have often been added as they were needed or as the technology evolved. As a result, security systems have traditionally been very likely to be cobbled together, and include components from multiple, often competing, vendors.

This includes the development of custom tools themselves. While 61 percent of enterprises today say they've purchased a SIEM solution from a vendor, 23 percent (with some overlap) report they have developed a custom SIEM tool in-house.

For these organizations, custom dashboards were a necessity. From a practical perspective, we consider the use of a dashboard to be more important than the source of the dashboard.

Endpoint Detection & Response (EDR) is Still Emerging

In contrast to SIEM tools, the adoption of Endpoint Detection & Response (EDR) tools is still relatively low (in use by only 48 percent of organizations in our study). But within 12 months, 81 percent of enterprises expect to be on board, increasing to 92 percent within 24 months.

This is a high-growth market, with endpoint security rapidly shifting from a first-line of defense to a core defense role. As such, we anticipate less custom development. But this will place additional importance on the need for organizations to implement dashboard solutions to simplify security management.

ENDPOINT DETECTION & RESPONSE ADOPTION
TODAY vs 24 MONTHS (by sector)

SECTOR	TODAY	24mo
▶ US Federal	52%	89%
▶ State, Local, EDU	42%	92%
▶ Defense	46%	96%
▶ Critical Infrastructure	51%	94%

FUTURUM PERSPECTIVE

We believe dashboards are a critical component in successfully navigating the security journey and will become increasingly important (and less custom) across the enterprise.

But we're also concerned that unnecessary complexity and/or overlapping functions could lead to a lack of dashboard effectiveness. This is a real concern as organizations that have developed an internal SIEM are also likely to have developed a custom dashboard as well. While we're not opposed to custom development, we do encourage organizations to ensure an open, adaptable, and standardized approach to monitoring security risks.

CONCLUSION BEGINNING YOUR JOURNEY

Ensuring enterprise-wide device security requires a shield, or security posture, that follows and protects devices throughout all aspects of the hardware journey, encompassing the external supply chain, internal implementation, and ongoing end-user operations and device management.

The task of developing and implementing a journey-based security posture is not necessarily an easy one, but it shouldn't be difficult either. But it must begin with the recognition that need for security is created when the order is placed, and the need for begins with the first component and lives on through, and beyond, the use of a device or system within the enterprise ecosystem.

> Security risks don't go away just because a device or system is no longer actively in use. Data at rest on a device at rest is still risk until that device no longer exists.

Create a security posture that is both holistic and spans the entire ecosystem of suppliers, partners, employees, and users.

The responsibility for a strong security posture doesn't reside with just one individual, group, or organization. Security is the responsibility of all and requires a strong commitment to coordination, collaboration, education, and establishing the right partnerships to augment internal resources.

Security frameworks are essential to creating a strong security posture.

Identifying, countering, and overcoming security risks requires more than just the right technology, it requires the right policies, procedures, and partners. A strong security framework (or frameworks) can provide the basis for understanding the scope of the issue within an organization and help guide the selection of appropriate technologies, partners, and policies. This includes both internal operations and outsources security services management.

Threat visibility and awareness are critical to maintaining a strong security posture — you can't defend against what you don't know exists.

Dashboards, that simplify and present threat intelligence information from across the ecosystem, are the headlights on the highway ahead, providing advance warning of threats and the data necessary to take the right measures at the right time to protect your systems, your assets, and your employees. They allow you to be agile and adaptive in maintaining a strong security posture throughout the entire journey.

IMPORTANT INFORMATION ABOUT THIS PAPER

CONTRIBUTORS:
Daniel Newman
Founding Partner + Principal Analyst, Futurum Research

Shelly Kramer
Founding Partner + Senior Analyst, Futurum Research

Fred McClimans
Research Director + Senior Analyst, Futurum Research

INQUIRIES: Contact us if you would like to discuss this report and Futurum Research will respond promptly.

CITATIONS: This paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "Futurum Research." Non-press and non-analysts must receive prior written permission by Futurum Research for any citations.

DISCLOSURES: This paper was commissioned by Dell Technologies. Futurum Research provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

ABOUT DELL TECHNOLOGIES
Dell Technologies empowers countries, communities, customers and people everywhere to use technology to realize their dreams. Customers trust us to deliver technology solutions that help them do and achieve more, whether they're at home, work, school or anywhere in their world. Learn more about our story, purpose and people behind our customer-centric approach. For more information, visit DELL on the web at www.dell.com.

ABOUT FUTURUM RESEARCH
Futurum is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

DISCLAIMER: The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Futurum Research disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Futurum Research and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Futurum Research provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.

CONTACT INFORMATION

Futurum Research, LLC | futurumresearch.com | 817-480-3038 | info@futurumresearch.com | Twitter: @FuturumResearch