InteliSecure

At a Glance

- Information Security in a World Without Boundaries
- A Fundamental Shift: Different Operations, Different DLP
- Re-Thinking the Model for Critical Asset Protection
- What Really Matters in the Future—and What to Do Now?
- We Can't Face the Future of Information Security with Yesterday's Tactics
- Make the Case for Making the Shift

"Your future takes precedence over your past. Focus on your future, rather than your past."

—Gary Ryan Blair

INTELISECURE GUIDE

Future-Proofing Your Information Security Strategy

JEREMY WITTKOP, Chief Technology Officer

I don't often write about the broader topic of information security because there are large portions of the security space that I am not involved in. However, as a leader of the technical partnership strategy for my company's clients, I feel obligated to share some ideas with information security leaders and the larger information security community about what I believe the future will hold.

My responsibilities require me to travel the world and talk to a lot of people. I hear business leaders expressing growing concern about their ability to protect their information and businesses in the face of seemingly overwhelming security threats. My response is to offer a take on the message that Gary Ryan Blair expresses in the quote above: Don't look to past paradigms to protect your business. Instead, focus on what's ultimately important—and within your control—as you move into the future.

INFORMATION SECURITY IN A WORLD WITHOUT BOUNDARIES

Information security professionals I talk to readily admit that the "perimeter"—that imaginary protective wall around a business and its data—is dissolving. One major driver of this dissolution is the fact that we already live in a hybrid world today. Very few organizations store and use their data 100% on premises and very few are 100% in the cloud. As a result, on-premises security and cloud security are equally important today.

However, digital transformation has progressed to the point where the key question about data has changed. Instead of asking what data will go to the cloud and what will stay on premises, we should ask how long it will be before most organizations don't operate data centers at all.

Despite the wide recognition of this shift, organizations still try to apply perimeter concepts to a world without boundaries. For example, some organizations are deploying firewalls inside of Amazon Web Services. Why?

A FUNDAMENTAL SHIFT: DIFFERENT OPERATIONS, DIFFERENT DATA PROTECTIONS

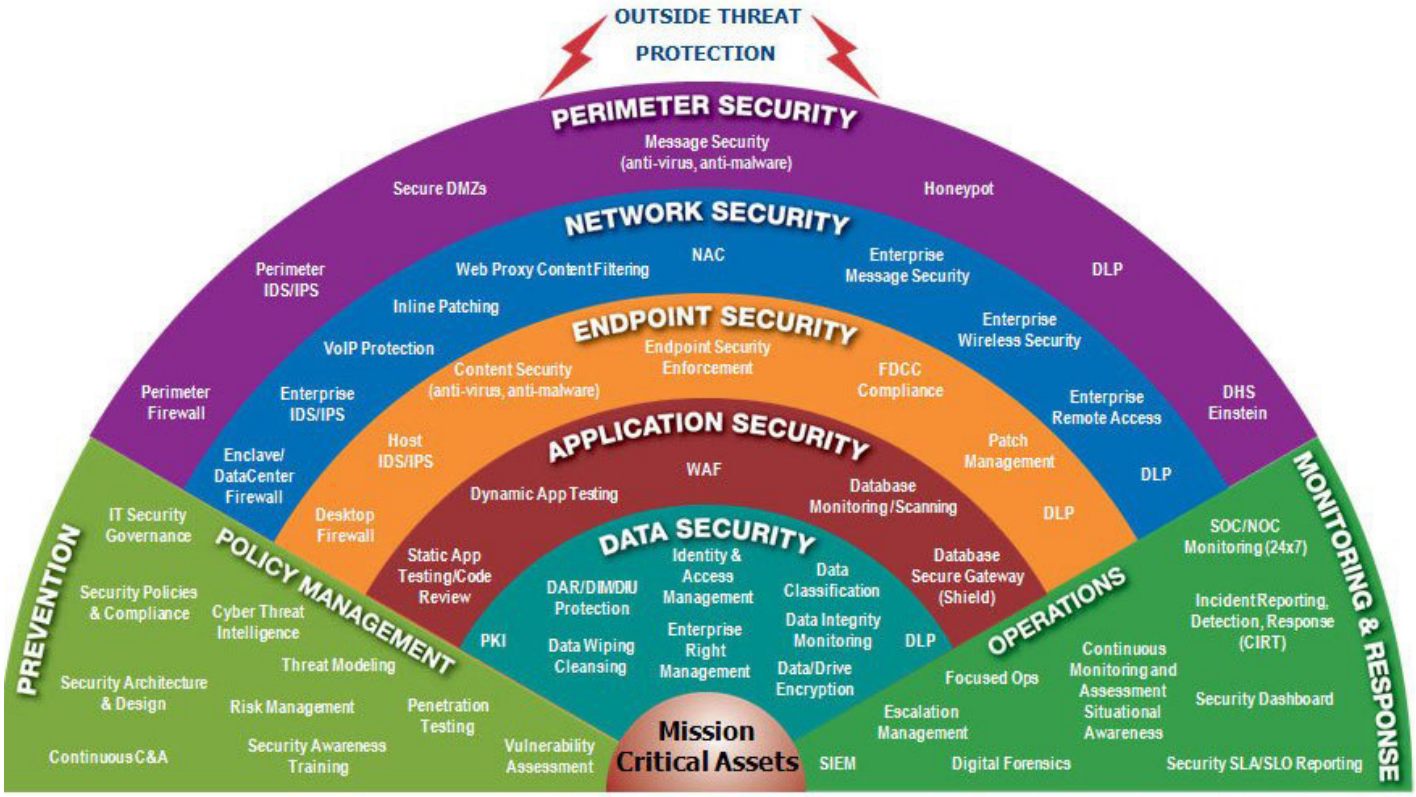
It's my job to look into the future—and the future holds some revolutionary innovations. Consider quantum computing, which offers orders-of-magnitude more processing power than any binary system ever could because a single qubit can operate in 256 distinct states, whereas a traditional bit has only 2. The potential power of this type of computing is staggering.

However, most organizations will never own a quantum computer; the operating environments for this type of technology is prohibitively expensive for most data centers, so it's likely that the primary model for its use will be Quantum Computing as a Service (QCaaS). Pair that with the rapid growth of Infrastructure as a Service (IaaS) that we're already seeing, and it's not hard to envision a world where all workloads are elastic and rented rather than static and purchased—and where the only organizations that own data centers are global governments and cloud services providers.

Many paradigms will change if such a world comes to fruition, but it is the most efficient way to operate and distribute resources. The shift will restructure many capital markets—and it will also challenge many security models.

RE-THINKING THE MODEL FOR CRITICAL ASSET PROTECTION

The Cyber Security Hub published this graphic detailing the disciplines of security and describing the products that fall into each bucket.



This model is helpful for understanding how we have navigated a crowded and confusing information security landscape. However, it is also useful for examining the future of security—and weeding out the sections we can no longer control.

- If you accept the premise that in the future you will rent computing power rather than own it, you will completely lose the ability to deploy the perimeter technologies in the purple section.
- Since you also won't own the network, all of the blue section goes away as well.
- The rise of bring-your-own-device (BYOD) strategies also renders the gold section obsolete to an extent because if you encourage your employees to use their home devices, or if they do so for convenience, it

becomes difficult to exert control over those devices.

- For Software as a Service (SaaS) applications, which are still the majority of cloud services, you will lose the red section as well—unless you use IaaS, in which case you will maintain that layer of protection.

What are you left with? Outside of policy management and limited operations, you are left with control over your data. If you look inside the teal bubble, you also have control over who you allow to access that data and the resources you rent.

Therefore, in this world, all that matters are people and data.

Most enterprise security strategies focus on implementing perimeter and network protections. Ironically, these are the security layers that organizations will have little control of in the near future.

WHAT REALLY MATTERS IN THE FUTURE—AND WHAT TO DO NOW?

I firmly believe we are moving at an accelerated pace towards the future I have described. I can't realistically predict exactly when we will get there. When skeptics express doubts about the pace of the digital transformation, I ask them a simple question: "What trends are you seeing that suggest a massive move back on premises for services that have gone to the cloud?"

I just don't see that trend going backwards. The elasticity, flexibility, and reduced barriers to entry into markets offered by cloud services is too appealing to ignore, especially for smaller and midsize businesses, which still form the majority of the economy. I can't imagine a new business starting today and borrowing capital to build a data center. It's difficult to imagine not utilizing SaaS and IaaS when those options allow you to be up and running in days instead of months or years.

Information security leaders should start pivoting now to emphasize the two elements of security that are not likely to be diminished: people and data.

- Design security programs with strong **identity and access management (IAM)**.
- Invest in **multifactor authentication (MFA)** and **identity governance**.
- Understand how to implement **Zero Trust Architecture** and know how you will enforce the **principle of least privilege (POLP)** and **need to know**.
- Gain an understanding for what data you have, what you must protect to establish international regulatory compliance, and what you should protect to **minimize risk** to the organization.
- Invest in technologies now that allow you to **secure Platform as a Service (PaaS), SaaS, and IaaS**.

Most important, begin re-skilling your workforce to address the problems of the future. It's fine to maintain legacy systems like Security Incident and Event Management (SIEM), firewalls, intrusion detection and prevention services (IDS/IPS), and endpoint protection, but don't make those the center of your strategy. If you do, you're likely to see diminishing security efficacy over time.

MAKE THE CASE FOR MAKING THE SHIFT

When it's time to future-proof your data protection strategy, you may still need to convince your leadership of the value of that change. Download the case study Making the Case for Critical Asset Protection and learn how a major cancer center implemented a Critical Asset Protection Program™ (CAPP) with InteliSecure and gained control of the flow of information inside and outside the organization.

WE CAN'T FACE THE FUTURE OF INFORMATION SECURITY WITH YESTERDAY'S TACTICS

If there's one thing digital transformation should have taught us so far, it is that business is going to move towards innovation, efficiency, and mobility as quickly as possible. The advantages that current and emerging technologies offer to business are essential to retaining a competitive advantage, and security leaders will not be able to slow or prevent the evolution.

We must prepare now so we can be ready to protect the business as it continues to innovate, rather than being dragged through digital transformation kicking and screaming. It's time to challenge our thinking and finally accept there is no perimeter and we cannot build a castle. The future of information security is asymmetrical, dynamic—and already a reality.

ABOUT THE AUTHOR

InteliSecure Chief Technology Officer Jeremy Wittkop is an information security leader dedicated to making the digital world a safer place to do business. With a varied background that includes defense, logistics, entertainment, and data protection, Wittkop brings rich experience to his role delivering comprehensive solutions to complex problems for client organizations around the globe. His passion and focus revolve around protecting the idea-based economy and the technological infrastructure on which the future is built.

ABOUT INTELISECURE

InteliSecure specializes in making data protection easy, fast, and cost-effective for companies of nearly every size. More than 500 clients with over 2 million managed users rely on our services and specialists to protect the integrity and safety of their sensitive information. With more than 15 years' experience and partnerships with some of the world's biggest names in cyber defense, we make data security and compliance easy by providing effective data protection at a lower cost, eliminating the strain on IT organizations and reducing the risk of confidential information getting into the wrong hands. Unlike other security providers, we focus on business outcomes—providing data and reports that make sense to business and security executives alike. InteliSecure serves clients globally with security operations centers in the United States and the United Kingdom.

InteliSecure

5613 DTC Parkway, Suite 1250 Greenwood Village, CO 80111 | + 1 (720) 227-0990 | sales@intelisecure.com | www.intelisecure.com

1 Lindenwood, Chineham Business Park Crockford Lane, Basingstoke, RG24 8QY, UK | +44 118 976 8960