CenturyLink® Business

WHITE PAPER

Revisiting the Cybersecurity Protection Myth

Practical Countermeasures for Threat Detection and Response.

An honest Cybersecurity professional will tell you they are spending more than ever on security tools and technologies to protect their critical business assets and IT infrastructure, but the bad guys are still getting in. Cybersecurity budgets are disproportionately spent on keeping the bad guys out. Protection alone is nowhere near sufficient, though. Extremely sophisticated and well-funded attackers relentlessly target your organization and will find new and creative ways to get in. In this environment, it's all about offense — how fast you can detect and respond to these threats. Yes, you still need to close the digital doors but you also have to add alarms and monitoring services in case they do get in — and they likely will. This paper revisits the protection myth and looks at practical countermeasures that deliver an economical but effective level of threat detection and response.

"We're going to need a bigger boat…"

Sheriff Brody in Jaws

Introduction

Cybersecurity has never been for the timid. You're dealing with bad guys who want to do bad things. The challenge in recent years is that they're getting a lot badder. And bigger. The threat environment has exploded in depth and intensity.

Think of it like this. If Jaws had been about Cybersecurity, you'd be Sheriff Brody, who, upon seeing the size of the shark he's up against, utters one of the most memorable lines in the history of the movies: "We're going to need a bigger boat." More security tools. More personnel. More budget. That fin in the water does look pretty huge. But, the truth is no boat will be big enough. The time has come to rethink the myth that the Cybersecurity tools and processes you've been using can prevent attacks. There's a limit to what a single security team can accomplish. This paper looks at the reasons the total protection approach is no longer viable and offers some thoughts on how to defend the most critical business and IT assets in a more proactive, efficient and therefore economical and effective way.

The End of the Protection Myth

While the Cybersecurity field has never held that 100% perfect defense is possible, many security programs have been based on the idea that a security team can devise countermeasures that protect all business and IT assets. This approach may have been valid for a time, but it no longer holds. The threat landscape is simply getting too vast and powerful to make pervasive protection a viable Cybersecurity strategy. The perimeter, which traditionally defined the starting point of protection policies, has begun to blur so much that it's difficult to know where to apply policies and countermeasures. Basic security methods alone cannot do it all.

Today's Threat Landscape

Threats are multiplying. Nearly 1 million malware threats are released each day. In 2015, a remarkable 169 million personal records were exposed in more than 750 data breaches in healthcare, education, financial and government institutions. That's 38% more security incidents than were detected in 2014. Attackers stay dormant within a network for over 200 days before detection. And, it's not just outsiders who threaten organizations. A SANS survey found that 74% of CISOs are concerned about employees improperly accessing restricted company data.

Organizations are also increasingly exposed to new styles of hacking. According to Wired, 2016 is shaping up to be a year full of more toxic extortion hacks, breakthroughs in hacking of security chips on credit cards and even the "Rise of the IoT Zombie Botnet." In this case, we may be witnessing the downside to the much hyped proliferation of smart devices on the Internet of Things (IoT). They can all be compromised, making the average connected thermostat into an instrument of Russian Military Intelligence.

Wired also cited a disturbing article from the respected government site, Defense One, which warned that new hackers are likely to change, rather than steal, data from important sources. For example, a hacker might penetrate a corporate ERP database and change all the logistics records, rendering them useless.

Worsening Threat/Perimeter Tension

The blurring of the perimeter compounds the challenges that arise with the escalation of threats. Today, with increasing adoption of the public cloud and standards based APIs, it's harder to know where your enterprise ends and someone else's begins. Add to this new classes of workers, some of whom don't actually work for you but have access to your most sensitive systems — and you are less able to mount a coherent defense.

The blurring perimeter is exacerbating the risk exposure inherent in the expanding threat environment.

38%
Feel they can handle an attack

81%
Of breach victims lack an intrusion detection system

52%
Believe they will be victims of a successful attack

Facing the Limits of the "Protect Everything: Orientation

As the threat landscape heats up, basic security techniques become less effective at protection. In the same way that installing doors, windows or a fence won't keep determined criminals out of your home, basic protective technologies like firewalls and anti-virus software are good first defenses but may not be successful when criminals have figured out how to get around them. More and more criminals are figuring this out and as a result, the quantity and types of threats we're confronting every day has gotten more intense.

In this context, security teams feel less prepared. ISACA, the body that certifies security auditors, found in a survey that only 38% of global organizations feel that they are able to handle a sophisticated cyber attack. Another survey found that 81% of data breach victims lacked a system to detect breaches. 52 percent of respondents to a CyberEdge Group survey believed that a successful cyberattack would occur in the coming year against their networks.

Shifting the Emphasis to Detection and Response

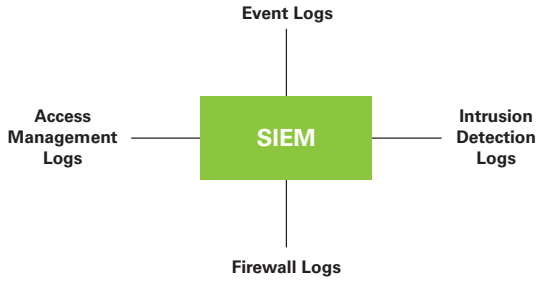
Daunting as the security challenges may seem, there is no reason to be pessimistic. As we said, Cybersecurity is not for the timid. However, it's time to shift the focus from protection to detection and response. Let go of the myth that we can protect everything and instead get better at detecting threats before they cause damage. Putting your Cybersecurity emphasis on detection gets you closer to attackers before they carry out malicious acts. The better you can detect, the better you can defend.

The first step is to identity the assets that need the most protection. Or, more likely, re-identify. Organizational changes brought about by mergers and partnerships may make certain information assets more vulnerable or valuable than they were originally thought to be. This might require doing a business impact "heat mapping" process described in the paper Moving to a More Efficient Cybersecurity Strategy. Once you have determined your most critical assets, you can build a detection-centric defense for them by concentrating on a few focus areas like log monitoring and SIEM. These focus areas are holistic and typically span multiple security technologies and professional disciplines. If you do Cybersecurity for a living, most of these focus areas will be familiar to you. However, the approaches we suggest, which are based on CenturyLink's extensive experience securing large enterprises, may give you some new insights into how to improve your overall security posture.

Security Log Monitoring and SIEM Technologies

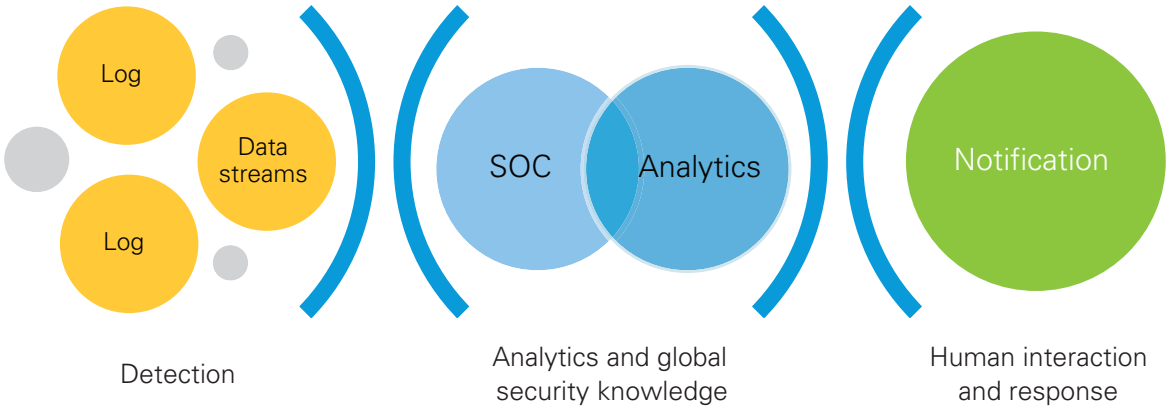
The emerging best practice for prevention-centric, holistic Cybersecurity countermeasures involves continuously monitoring the logs of your IT assets and business systems in a mode of correlation and deep analysis that can reveal hidden risk exposure. To perform this kind of deep analysis, many departments turn to security log monitoring and Security Information and Event Management (SIEM) solutions. Done right, SIEM today benefits from achieving what seems like an oxymoron — a fine-grained big picture of what's happening throughout your extended organization. They can help you detect possible threats based on correlation of event data and applied context data (like vulnerability data, threat intelligence, user and asset data, etc.)

The appeal of SIEM is easy to see, though its execution can get complex and costly. The effectiveness of the technology is only as good as its configuration and continuous upkeep. The effectiveness of correlation depends on expertise in data collection, the strength of the correlation rules established, and an understanding of the threat landscape, attack patterns and/or compliance requirements.



SIEM success requires intense configuration, continuous upkeep of systems and rules as well as skilled analysis.

It's a budget and resource-intensive process. The development of rules and new policies based on use cases and the changing security environment takes time and expertise. The ongoing maintenance and tuning of a SIEM is complicated. The results and read outs require careful analysis and continuous monitoring to be effective. All of this costs money and requires expert security staff. Even large organizations struggle with doing it all in house. According to 451 Research, less than 20% of Cybersecurity budgets are spent on SIEM technologies that perform log correlation and can identify possible security incidents on a proactive basis.



Proactive threat detection and notification requires sophisticated analytics and an SOC, followed up with risk-based alert process for administrators.

Proactive Threat Detection and Notification

Proactivity makes detection-centric security work most effectively. Being proactive means correlating multiple streams of data and pulling insights from both real-time events and asset risk profiles to detect threats at the earliest stages and reduce false positives. The best way to do this is with a 24/7 Security Operations Center (SOC) that performs continuous monitoring. Historical logs should also be available for analysis that can aid in investigation and provide deep context to threat trends.

As detection proceeds, the human connection emerges as another layer of vulnerability in and of itself. In order for a security team to take action on a threat, a person must receive an alert and decide on an appropriate response. As we all know, this sounds easy but is anything but. Too many false positives and vague warnings lead to alerts getting ignored. A proactive threat detection system must be accompanied by a sophisticated, risk-based alert process that combines automation with rigorous human review.

Incident Management and Response

Once you've detected a possible attack, how do you most effectively handle it in order to limit damage, increase the confidence of external stakeholders, and reduce recovery time and costs? It's your ability to swiftly and efficiently respond to incidents that make the difference between weathering them and incurring great damage to your business and reputation.

While most organizations do, in fact, have incident response (IR) plans in place, most organizations don't truly operationalize them, leaving the plans ineffective due to poor design or poor implementation, or both. Incident response is a notorious budget drain and distraction from other security duties but this is a critical area to focus on and get right.

The CenturyLink Approach

Some of these countermeasures can be done in-house. Others offer great value when outsourced, or with a hybrid mix of in-sourced and outsourced services. In deciding whether to keep detection-centric security in-house or outsource, one consideration should be staffing. Even if you want to implement SIEM and an SOC, you may not find the right people. In Georgia Institution of Technology's Emerging Cyber Threats Report 2016, Frost & Sullivan projects that the tech world will be short more than 1.5 million security personnel by 2020.

CenturyLink can be a resource for helping your department focus on the holistic focus areas described above. If you accept that you cannot prevent everything, that you do not likely have the time, personnel, tools or resources to mitigate all of your high-impact risks, consider how we can help. Our security services, honed over years working with some of the world's largest enterprises and by defending our own global organization, are designed to give you capabilities that would be difficult to create in-house.

We provide a unified system of security services that covers the entire IT stack. With this approach, we are able to reduce security and instability risks that arise from managing and integrating disparate technologies, services and SLAs across multiple vendors. It's a true ecosystem of security services that ranges from DDoS attack mitigation, to monitoring and management of basic protective devices like firewalls, to handling the entire lifecycle of an attack. Our approach incorporates macro threat intelligence, advanced analytics and SIEM technologies along with proactive detection, containment and incident response services.

CenturyLink is known for expert security consulting by specialized security and SOC pros. Our expertise goes into securing our millions of customers, 550k fiber route miles of global network and billions of dollars in business assets. We can evaluate your regulatory environment and suggest the tailored delivery of standard solutions. These can be easily added to CenturyLink hosting, cloud, network and colocation services.

Services can be fully managed or co-managed, available on-premises, hosted, or a hybrid mix of both. CenturyLink security clients get 24/7 continuous monitoring from our commercial SOCs, which are staffed by over 250 researchers, testers and GIAC Certified Intrusion Analysts.

Conclusion

As Brody learned in Jaws, there isn't going to be a bigger boat. He had to fight smarter to survive the shark attack. Cybersecurity teams are in a similar position. The idea that your team, on its own, can prevent any attack is getting harder and harder to put into action. The threat landscape continues to grow larger and more varied — to the point where adopting areas of holistic focus is the best approach.

By focusing on more proactive approaches that help you detect and respond to possible threats rather than react, it is possible to stop threats before they expose the organization to risk. Proactive threat detection and notification warn of attacks before they can inflict harm. Incident management and response planning completes the picture. Outsourcing of selected aspects of these focus areas can provide the best results. CenturyLink® Managed Security services offer a depth of capability while shouldering the burden of many time-consuming and complex security tasks.

About CenturyLink Business

CenturyLink, Inc. is the third largest telecommunications company in the United States. Headquartered in Monroe, LA, CenturyLink is an S&P 500 company and is included among the Fortune 500 list of America's largest corporations. CenturyLink Business delivers innovative private and public networking and managed services for global businesses on virtual, dedicated and colocation platforms. It is a global leader in data and voice networks, cloud infrastructure and hosted IT solutions for enterprise business customers.

For more information visit www.centurylink.com/enterprise.

Global Headquarters
Monroe, LA
(800) 784-2105

EMEA Headquarters
United Kingdom
+44 (0)118 322 6000

Asia Pacific Headquarters
Singapore
+65 6768 8098

Canada Headquarters
Toronto, ON
1-877-387-3764

868082616 - revisiting-cybersecurity-protection-myth-whitepaper-wp160508

CenturyLink® Business