Boosting your organization's cyber immune system.

Why it's time to think differently about cybersecurity

A white paper from Bell

What's inside

With cyber threats evolving at an accelerated pace and attackers becoming increasingly sophisticated, organizations will continually look to improve their security posture. The ability to keep pace with attackers, however, may be achievable only by thinking about the problem in a different way. This white paper describes how effective cybersecurity is similar to the way the human immune system anticipates, detects, adapts to and defends against threats – allowing the body to function at peak performance. Just like the immune system, in the cyber world there are also times when a coordinated, community effort is needed to protect against mass 'outbreaks' of threats, with Internet service providers ideally positioned to play an important part in this community-based defence.

Contents

Introduction

Escalating threats. A persistent stream of new vulnerabilities. Intensifying business impacts. As cyber attacks become more severe and diverse, organizations need not just new tools and techniques but also a new way of thinking about cybersecurity. When it comes to finely tuned and highly resilient systems that defend effectively without compromising core functions, one of the best models is extremely close to home: the human body.

If not for the immune system, we might each have to live in a bubble providing perpetual quarantine to protect us from disease. While such an approach would keep us healthy, it would also seriously impede us from interacting with and enjoying the world. The same is true about networks: in today's operating environment, a perimeter-only approach to defence is simply putting up walls that get in the way of doing online, data-intensive business.

The human body's immune system takes a different approach: a dynamic and learning approach. When it encounters threats it recognizes, it reacts in known ways to address them. When it encounters threats that are unfamiliar, that's when it intensifies its defences – and at the same time, acquires knowledge of how the threat behaves so it can take more effective action next time.

The business of the body is to keep functioning at as close to peak condition as possible. The business of an organization is to carry out its daily operations with maximum efficiency. Viewed this way, security is really a business problem rather than a purely technical one. Solving it means taking a holistic view of the corporate network's role in achieving business objectives and also drawing maximum value from existing security investments: two areas where an Internet service provider (ISP) can serve as a key partner.

The evolving threat landscape

Even with considerable improvements in modern medicine, viruses and illnesses are always adapting and evolving. So is the external environment. All of this requires continual enhancements to medical approaches. The same applies to the cyber threat landscape, which is evolving in ways that make it increasingly difficult for organizations to do what they need to do (such as embrace virtualization and the cloud, grow their online presence or handle exploding volumes of data) safely and securely.

Five key trends have given attackers the upper hand in recent years:

Expanded attack surface

As they continue to digitize their businesses, organizations are rapidly transforming their IT Infrastructures in the pursuit of greater business agility and productivity. More endpoints and devices, including legacy systems that are ill-equipped to handle modern threats, are moving in and out of the corporate network than ever before. (To illustrate, Gartner estimates 8.4 billion devices will have connected to the Internet by the end of 2017.[1]) At the same time, mobile and cloud platforms are becoming increasingly essential to daily operations. This gives attackers more options for infiltration and infection than ever before – and gives enterprises a much bigger potential attack surface to monitor and defend.

More complex attacks

It used to be that only Windows-based machines were vulnerable to attack. Today, viable malware is present for macOS, Linux, Android and iOS – and malware is now being designed specifically to target embedded devices such as routers and modems. Malware has also evolved to evade traditional signature-based defences, with attackers using previously unknown exploits, malicious code that never gets written to the victim's hard drive, malware that embeds itself in a device's firmware, and polymorphic malware that changes its characteristics every time it executes.

Attackers also have a much wider range of potential attack methods at their disposal. Organizations need to defend against malware that can give full access to their systems, ransomware that locks away critical files and data unless they pay the attacker, zero-day exploits that target specific vulnerabilities not previously known to software vendors, distributed denial of service (DDoS) attacks that take down websites or online services by overwhelming them with massive amounts of bandwidth, and breaches in which attackers steal sensitive personal or financial information.

These attacks can be carried out in many different ways, including phishing (malware delivery via legitimate-looking email), malvertising (malicious payloads injected into the ads of legitimate apps and websites), social engineering (tricking users into performing actions that give attackers access to important systems and assets) and more.

As attacks become more complex, they also take a longer to detect and are more expensive to remediate. The median time to identify an attack is 99 days[2] and the mean cost per stolen data record in Canada is $255.[3]

[1]Campus Technology. Gartner: 2017 will see 8.4 billion connected 'things'. Available from: https://campustechnology.com/articles/2017/02/09/gartner-2017- will-see-8.4-billion-connected-things.aspx

[2]FireEye. FireEye releases Mandiant M-Trends 2017 Report. Available from: http://investors.fireeye.com/releasedetail.cfm?ReleaseID=1017295

[3]Ponemon Institute. 2017 Cost of Data Breach Study. Available from: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

Growing volume of attacks

Attacks are not only becoming more complex but also happening in greater numbers, with attackers often combining multiple attack vectors and techniques to inflict the most harm possible. The number of successful attacks has increased by 46 percent over the last four years[4] – with the number of reported data breaches in the U.S. increasing by 40 percent in 2016 alone.[5] Attacks are getting larger, too. According to Bell network data, the largest DDoS attack in Canada was 202.5 Mbps and the longest attack lasted more than 16 hours. Globally, some DDoS attacks powered by Internet of Things botnets have exceeded 1 Gbps in size. With more attacks come greater costs: ransomware damages reached $5 billion in 2017, a 15-fold increased from just two years earlier.

Attackers are better organized

Today's attackers employ evolved tactics and techniques, leveraging a mature and rich supply chain of tools, services and infrastructure – such as the Dark Web – to fuel their cybercrime and facilitate their operations. Attackers have infiltrated the Apple App Store and Google Play Store, for example, to spread malware across a large number of apps, and have exploited retail point-of-sale systems to facilitate data breaches. The same tactics used by for-profit crime are also available to 'hacktivists' who target governments or corporations as a form of protest.

Attacks are cheaper and easier to conduct

The high availability and low cost of cyber crime tools encourages criminals to prey on enterprise data. Subscription services now exist where people can rent DDoS botnets or pay someone to launch an end-to-end attack on a target of their choosing. At a cost of only a few dollars per week, anybody with a credit card and motive can quickly and easily launch an attack. With the emergence of ransomware-as-a-service (RaaS), people with no programming or coding skills have access to this highly effective attack. Cybercriminals author the malicious code and then make it available for others to use, often for a small up-front fee or by taking a cut of the ransom (which, in turn, incentivizes more attacks and higher ransom requests).[6]

Regardless of how they are delivered, cyber attacks can be categorized into two major categories: attacks in plain sight and silent killers.

The business case for cyber crime

A stolen credit card account can be sold on the black market for as much as $20. If a breach yields 10 million records, even at a conservative dollar for every card, that attack is potentially worth $10 million.

Criminals can put together a strong attack package (i.e., malware source code, exploit kits, bulletproof hosting, malicious installs, zero-day exploits) for less than $500,000. That amounts to a return on investment in the range of 2,000 percent.

Part of the reason for the rise in ransomware is that they can provide a much faster payout than stealing credit card data – with a much lower risk of being caught due to the anonymity that comes with trading in Bitcoin.

Visit our blog to learn more about what your data might be worth to cybercriminals.

Like the common cold, attacks in plain sight such as DDoS, phishing attempts and the like can be easily detected. But other attacks are more like heart disease and cancer: multi-stage, multi-vector attacks that go unnoticed for long stretches of time before turning deadly. These silent killers include strategic breaches and advanced persistent threats designed to remain in the target system over the long term to facilitate data access and exfiltration. Defending against these attacks requires unwavering diligence to early detection and removal, which traditional cyber security methods may not be cut out to provide.

[4]Forbes. An "average" cyber crime costs a U.S. company $15.4 million. Available from: www.forbes.com/sites/moneybuilder/2015/10/17/an-average-cyber-crime-costs-a-u-s-company-15-4-million/#5dd7996032cb

[5]Cision PR Newswire. Data breaches increase 40 percent in 2016, finds new report from Identity Theft Resource Center and CyberScout. Available from: https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html

[6]Forbes. Ransomware-as-a-service: The next great cyber threat? Available from: www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat

Why it's difficult to maintain cyber health

When you walk into a room where people are coughing – say, the waiting area of a walk-in clinic – you're likely to avoid touching too many common surfaces and will wash your hands regularly to keep from getting sick. Acting on self-preservation instincts, you anticipate potential threats and act to minimize them.

Again, there's a parallel with cybersecurity, which has to do with keeping up a strong security posture. Yet as organizations race to transform their IT infrastructures and move more of their business to the cloud, many are inadvertently weakening that posture.

Every new system and application introduced to the corporate network increases the risk of zero-day vulnerabilities that could be exploited. Legacy standalone technologies, such as the supervisory control and data acquisition (SCADA) networks that operate power plants and other critical infrastructure, are suddenly becoming vulnerable as they connect to the Internet for the first time. They simply lack defences against the threats that come with open network connectivity. And with the ongoing adoption of cloud and mobile computing, information historically protected within the enterprise perimeter is now diffused across multiple locations.

In this context, organizations face two major challenges when it comes to protecting their data:

1. Lack of situational awareness

Just as in public health, where agencies monitor disease trends and population-level data to identify potential epidemics or 'hot spots' of disease activity, organizations need to understand the threat context in which they operate. Many today face digital threats without knowing it – and without appreciating the potential consequences until it's too late. Unfortunately, many lack the resources or capabilities to constantly monitor and act upon potential threats.

2. Keeping up with the security 'arms race'

Despite continually investing in and refreshing their defensive infrastructure, many organizations still can't keep pace with the rapidly changing IT environment. Introducing a new productivity application, cloud service or customer portal brings security implications that then require investments in new security solutions, adding even more complexity to the IT infrastructure – and further increasing the exposure and potential vulnerabilities that can be exploited by attackers.

In other cases, enterprises get caught in frequent hardware refresh cycles, struggle to maintain an adequate team of qualified IT professionals or find themselves burdened with high licensing costs for security technologies, all of which limit their ability to make the upgrades necessary to stay in front of attackers' capabilities. The resources organizations spend on keeping up with the arms race are resources they take away from delivering their core mission.

Addressing both of these challenges will require organizations to start thinking 'big picture' in terms of how they go about protecting their cyber immune system.

Taking a holistic approach to cyber immunity

Just as people who want to stay healthy will avoid smoking and junk food rather than waiting to treat symptoms of illness as they appear, organizations should be adopting a holistic, preventative approach to cyberhealth.

This starts with understanding the corporate IT environment as a whole. Because it's becoming increasingly difficult to protect every part of the business to the highest level possible, it's often necessary to prioritize security efforts. As such, enterprises need to assess where their vulnerabilities lie and what parts of the business most need protecting. In other words, they need to focus on risk. For businesses, the greatest risks are those to the bottom line, brand reputation and customer relationships.

Assessing risk from multiple perspectives

Traditional enterprise IT security risk assessments start from the defender's perspective: what is the threat, how vulnerable is the organization to it and what is the potential business impact of a breach? Weighing all of that helps determine how much to spend on which types of resources to block that specific form of attack.

But with more types of attacks coming from more places, this approach is no longer sufficient. Assessments must also consider the attacker's perspective. For example, by calculating the potential return on investment for an attacker, an organization can determine which of its data actually presents a lucrative target. By knowing how much its data is worth to an attacker, it can better allocate security resources to protect its most valuable data. It's like looking at it from the perspective of a contagious virus. If you were looking to infect somebody, how would you gain entry into the body? And what types of people would you be most likely to target?

As part of this assessment process, organizations should build up a thorough understanding of the strengths and weaknesses of the various protection methods available and leverage the strengths that best serve their organization's mission and effectively manage risks.

Organizations must also look at their supply chain to identify partners who can help them strengthen their security posture – and any who might pose a risk of compromising it.

Getting the visibility and insight to predict and prevent threats

Part of the big picture approach is adopting a systematic view of cybersecurity. This means looking at security as more than a firewall or other security appliance. Instead, it's important to consider how security can enable the organization's core mission while minimizing risk. Which approaches could provide optimal protection? What will have the least negative impact on the organization's primary business objectives – or even help the organization synergistically facilitate its core mission?

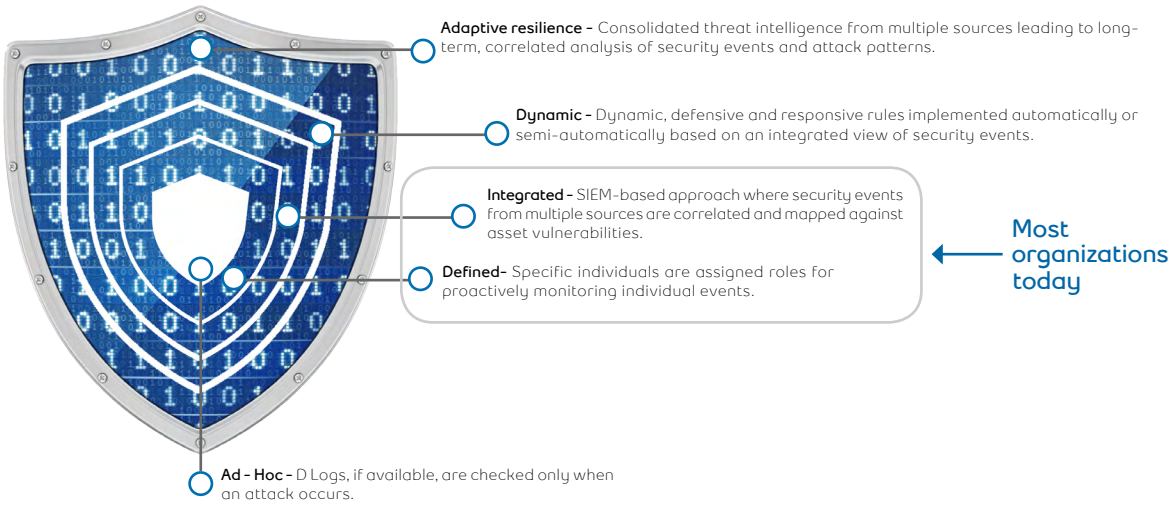
Enterprises can achieve this by improving their situational awareness and visibility into potential attacks, and by training staff to recognize and avoid cybersecurity hazards (e.g., through the use of proper email and password protocol to reduce the risk of phishing and other common attacks).

Achieving greater visibility into threats requires enterprises to leverage the power of their supply networks rather than relying purely on their own defences. By drawing on intelligence from across their region, industry and multiple other sources, they can identify emerging threats faster and better focus their defences.

It's the same principle used by the World Health Organization (WHO), which has established a model for what it calls "community-based health cooperation". The WHO gathers data from members around the world and uses its global perspective to identify epidemics, aggressive pathogens, carcinogenic substances and other health hazards, all with the aim of getting ahead of emerging health risks. And when severe outbreaks do occur, it helps analyze samples from Patient Zero – the origin of the infection – to accelerate vaccine development.

With improved understanding of potential risks, organizations can move beyond purely reactive approaches to focusing on prevention and pre-emptively stopping attacks before they happen. Most organizations aren't there yet – but by adopting techniques such as high-end cyber analytics, they'll be able to leverage insights gathered across their networks to detect threats earlier and with greater accuracy. Such tools will continue to evolve to incorporate more proactive and predictive measures, allowing most appropriate defensive measures to be put in place when necessary.

Figure 1. Situational awareness maturity model



The Bell approach

Just like how the WHO provides public health protection and promotion at the global level, ISPs and telecommunications carriers like Bell are ideally positioned to play a similar role in the cyber world. They see the macro activity of their entire network system. They're in a position to identify patterns, implement preventive measures and promote practices that foster good network health. Carrier-hosted network security solutions typically offer levels of scalability and flexibility that exceed the capabilities of individual enterprises alone and can be provided in a cost-effective manner.

Bell takes this approach a step further through its highly proactive approach to security, which offers a number of distinct advantages to customers with its various network security solutions:

Greater visibility and situational awareness

Bell carries most of Canada's Internet traffic volume – more than 10 petabytes of traffic every day – and reaches 99 percent of individuals and businesses. This gives Bell a commanding view of the Internet traffic flowing through public networks. With access to such a large amount of information, Bell can detect anomalous traffic patterns before anyone else and stop malicious packets before they can reach customers' networks.

Bell also maintains advanced, high-capacity security measures (such as anomaly detection and honeypots) throughout its national network and at peering points with other carriers to identify and understand emerging threats as they occur. Combining internal and external situational awareness from 24/7 security event monitoring and correlation, malware analysis, and broad collaboration with industry and government organizations, Bell is able to see vulnerabilities and threats that are simply not visible to most enterprises with the tools and limited information available to them today.

Applying a magnifying glass to Canadian Internet traffic

Bell uses what is known as cyber threat intelligence (CTI) to analyze data from a number of different sources and create actionable cybersecurity insights for its customers. Through its CTI platform, Bell correlates feeds from more than 150 data sources across its own national network infrastructure, customers, industry partnerships, major security suppliers, governments and the global security community. It then uses automation, machine learning, artificial intelligence, anomaly detection and other techniques to aggregate and analyze this vast set of cyber threat information.

In addition to enabling early threat detection, CTI also:

- Promotes greater understanding of an organization's threat environment (e.g., by providing context into which threats are targeted and which are more opportunistic in nature), allowing it to make better- informed risk-management decisions and optimize its security investment.
- Allows for cross-vertical and industry comparisons
- Provides the capability to rapidly recreate a forensic timeline for a security breach, reducing time- and cost-to-recovery and ensuring no residual backdoors are left behind

When aggressive new 'pathogens' emerge, we want to quickly identify the initial victim, analyze the source of the infection and synthesize an effective 'vaccine' to inoculate the community – in other words, to mount the right cyber response.

Preventative and predictive threat response

The cost and effort associated with maintaining, renewing and managing multiple layers of perimeter security – the 'classic' model – can be quite significant. But by leveraging a carrier's preventative and predictive security model, organizations can reduce costs and increase efficiency while at the same time increasing their overall security posture.

Bell helps deliver this model by taking on the first line of defence, offering a thorough defence-in-depth approach that consists of three layers of protection:

- **Network edge:** The first layer of defence is found at Bell's network peering points. Here, Bell leverages a number of core security features including filtering traffic from flagged IP addresses to prevent certain types of DDoS attacks and dropping traffic from flagged sources for a faster response to volumetric DDoS attacks. Bell also neutralizes large DDoS attacks that target specific network infrastructure protocols (such as NTP or DNS), governs traffic to prevent a customer's access circuit from becoming a 'transit' point for malicious traffic, and monitors IP address spoofing (a common vector for DDoS attacks).
- **Network:** In providing a gateway to the Internet, Bell develops and embeds security services in the network. Through its Network DDoS Security service, for example, Bell inspects the network pipe as traffic flows through it, looking for possible attacks.
- **Customer premises:** In the last layer, protection is provided at the edge of the customer network. Bell can deploy and manage many technology capabilities, leveraging the 24/7 monitoring available through its security operations centres as well as its centralized management to deliver additional insights in threat prevention.

In addition, Bell is currently expanding its portfolio of network services to provide turnkey protection for business customers, drawing on CTI for invaluable insight into emerging threats. Its network-perimeter-as-a-service approach, for example, will provide comprehensive, always-on, always up-to-date protection for businesses that use Bell as their gateway to the Internet. Like the WHO working to ensure community health, Bell is focused on keeping Canadian businesses safe and secure from cyber threats.

Bell is also working to further leverage the insights gained from inspecting the large volumes of traffic traversing its network, using CTI to rapidly detect and eventually predict attacks before they happen. This capability will allow all organizations, not just the victim of an attack, to proactively orchestrate defences across all three layers to counter the attack vector – ultimately reducing the cost of defensive infrastructure.

Together, these three elements mirror the human body's immune system, comprising an ecosystem in which every part works together to protect the whole.

Conclusion

With cyber attacks becoming increasingly common and complex, organizations need to shift the way they think about cybersecurity – away from firewalls and other 'boxes' and toward ISP-enabled solutions that offer greater visibility and situational awareness into potential threats. Doing so provides the insights to make smarter security decisions that boost the enterprise 'cyber immune system' while keeping mission-critical traffic flowing through the corporate network.

Bell is uniquely positioned to offer cyber threat intelligence and upstream network security that can simplify companies' defensive architectures and put more distance between malicious actors and their corporate assets. With its highly available network, 27 secure data centres and three scrubbing centres across Canada, Bell can sustain and respond to threats and attacks with speed and scale that few others can match. Backed by a team of highly qualified security experts, Bell delivers advanced threat detection, mitigation and prevention expertise to organizations across the country – with experience protecting banks, governments and other regulated industries that require the highest levels of security.

Contact your Bell sales representative to discuss the network security solutions that might be right for your business, or visit bell.ca/securitysolutions for more information.