A Frost & Sullivan Assessment

BlackBerry Secures 96% of the Enterprise IoT Threat Landscape

Powering clients to a future shaped by growth

FROST & SULLIVAN

Frost & Sullivan has assessed the cyberthreat landscape and the proportion that BlackBerry's suite of technologies can protect against. After quantifying the overall market in terms of number of attacks and categorizing those attacks as more preventable by network- or endpoint-based security, Frost & Sullivan determined that comprehensive endpoint-based security can protect upwards of 97% of attacks. The percentages are likely to grow because of the growing proliferation and importance of Internet of Things (IoT) devices. Frost & Sullivan also determined through independent research that BlackBerry is well positioned to secure all IoT endpoints, and upwards of 96% of all cyberthreats in the current landscape, proving a comprehensive, effective, scalable, and high ROI cybersecurity solution to modern businesses.

SECTION 1: UNDERSTANDING THE CYBERTHREAT LANDSCAPE

The digital transformation of society and economies has impacted all aspects of modern life. Businesses, governments, organizations and people have become accustomed to real-time information, communication, and action. This increased level of connectivity has allowed us to become more efficient, productive and resilient. For instance, because of the mobility that connectivity has enabled, millions of people during the COVID-19 pandemic were able to work, “socialize,” and stay informed remotely while sheltering in place. Never in history has this level of information and communication been so readily and easily available.

However, with connectivity comes risk. The same pathways that enable remote work, create smarter cars and homes, and improve production are the ones that can be leveraged by threat actors to impede and damage these activities. It would not be an exaggeration to say that cyberattacks are everywhere, and they vary in type, intent, and execution. The University of Maryland estimates there’s a new hacking attempt every 39 seconds on average, although Frost & Sullivan research indicates the number of attempts may be much higher.

In 2019, an estimated 25 to 30 million cyberattacks happened globally.[1] The FBI states that in the United States, 450,000 attacks were reported in 2019, but it estimates that at least 90% of attacks go unreported—indicating that upwards of 5 million attacks happened in the country in 2019 alone.

Cybercrime-related costs were expected to hit $5 trillion globally in 2020;[2] however, these estimates were made before the pandemic took hold, and cybercrimes increased dramatically during the first half of 2020. The FBI reported a 300%[3] increase, and the World Health Organization noted a 500%[4] increase, in cybercrimes over the first two months of the pandemic. Even before the current health and related economic crises, enterprises were spending more than 10% of their annual IT budget just on cybersecurity.[5]

Network attacks account for roughly 1 million attacks per year,[6] or slightly more than 3%. The other 97% are either focused on, or accessed through, endpoints that include smartphones, laptops, and IoT process or monitoring equipment and the servers they communicate with. Essentially, for a business to be secure its endpoints must be secure.

Phishing is the most common tactic for threat actors: about 30% of US workers have admitted to opening a phishing email, and many have clicked through to attachments and fraudulent sites.[7] Perhaps unsurprisingly, at least 76% of companies have been victims of phishing attacks.[8] This access would be conducted via smartphone, tablet, laptop, or computer.

> **“Through extensive research of its solutions, Frost & Sullivan has determined that BlackBerry’s portfolio of solutions can secure the vast majority of IoT endpoints and any data transmitted from or to them.**

Credential stuffing is another common attack, as stolen credentials are used to access data, systems, and/or devices. These credentials may have been gained illicitly through a phishing scheme or be the result of threat actors launching automated algorithms that scan and test thousands of login and password combinations.

IoT devices are common targets for credential stuffing and cyberattacks: by some estimates nearly half of all IoT devices have had some level of attack.[9] As the number of IoT devices continues to grow at an unprecedented rate, securing these endpoints becomes essential. To date, more than 60% of businesses have stated they have been victims of IoT attacks.[10]

BlackBerry’s Impact on the Enterprise

Frost & Sullivan has analyzed the total threat to enterprises and independently compared it to BlackBerry’s capabilities in providing comprehensive enterprise cybersecurity[11] across major vertical industries. Through extensive research of its solutions, Frost & Sullivan has determined that BlackBerry’s portfolio of solutions can secure the vast majority of IoT endpoints and any data transmitted from or to them. Some minor exclusions include older non-API technologies, such as an office printer tied to a local area network, or aged operational technology (OT, as opposed to IT) devices that do not use an API and were manufactured and installed before concerns of cybersecurity became apparent. However, this does not impact BlackBerry’s ability to protect the enterprise. The proportion of these endpoints vs. API-connected devices is negligible and decreasing. They also are not typically targets for threat actors because they are isolated from more meaningful networks and data, and often would require a physical interaction in order to be compromised (such as with a USB).

BlackBerry's portfolio of services covers the IoT: the endpoint itself; its operating system; any data it uses, transfers, or otherwise connects with; the systems, users, and partners that interact with the enterprise, its endpoints, and its data; and edge use cases that come from the dissolution of the traditional network perimeter. Areas of coverage include:

- Embedded security at the point of manufacture to secure the device and its operating system;
- Comprehensive, zero-trust based unified endpoint management (UEM) and unified endpoint security (UES) for both fixed and mobile endpoints;
- Artificial intelligence (AI)-driven endpoint security and authentication for scale across the entire IoT and for a smart solution that evolves ahead of the threat landscape;
- Securing data as well as endpoints with, for example, virtual desktops, VPN-optional file sharing, email, and private networks for talk/text/messaging;
- Enabling businesses to verify (or fix) source code from supplier-provided parts and components;
- Tracking assets and their integrity along the value chain and across logistics and transport;
- Ensuring business continuity with planned or unplanned event management and ecosystem-wide crisis communication tools;
- Securing third-party apps (platform agnostic) for secure interoperability across the entire IoT ecosystem; and
- Bringing forward a cloud- and mobile-first strategy.

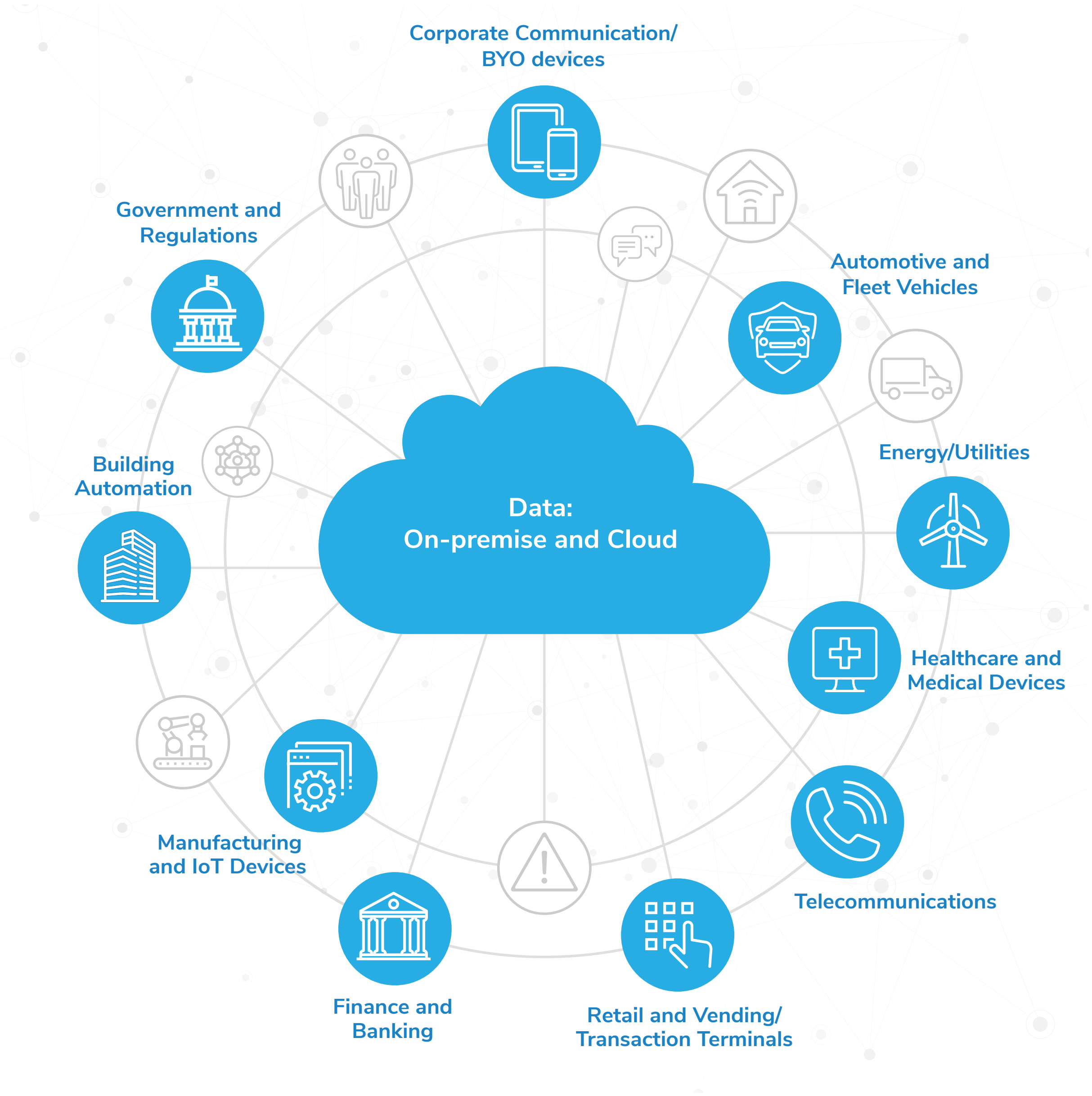
Endpoints are the entry point of 97% of attacks, and BlackBerry is able to secure all IoT endpoints. Several of its technologies also overlap with network security, such as application, email and wireless security. Frost & Sullivan concludes BlackBerry can secure 96% or more of the enterprise threat landscape.

Securing the Bigger Picture: Zero Trust Strategies

A zero trust strategy flips the default thinking of an enterprise from "our systems are safe, unless an attack shows otherwise" to "our systems are inherently at risk, unless proven secure." BlackBerry's solutions work in concert to provide this "security bubble" that includes and also extends beyond enterprise endpoints, to give coverage to bring-your-own (BYO) devices, third-party vendors along the value chain, and any other interactions with enterprise data, systems, and devices. Many of these solutions overlap with network security, such as creating secure messaging and communication networks, and protecting third-party apps and email across the access spectrum.

Exhibit 1 below shows common enterprise endpoints, any and all of which can be susceptible to cybersecurity threats.

Exhibit 1: Enterprise Vulnerabilities



Rapid Growth in Devices and Endpoints Complicates Cybersecurity

The swift pace of technological innovation, combined with companies and individuals' ever-increasing demand for mobility, productivity or convenience, and data, means that the number of connected endpoint devices has grown exponentially over the past decade and is forecast to continue to do so. This will substantially increase the threat surface, which is reflected in the rapidly expanding threat landscape as well as the overwhelming number of security vendors entering the market with point solutions. Frost & Sullivan calculates that there were 24 billion new connected devices in 2019, and that this will rise to 67 billion devices by 2025. These include familiar electronics such as smartphones and tablets (about 5 billion by 2025), and a growing variety of others that will be used across offices, industry, healthcare, vehicles, and infrastructure. Exhibit 2 shows the estimated number of new connected devices for key applications. Many applications are forecast to see double-digit annual growth rates to 2025. Industrial IoT devices will have one of the highest growth rates at 25.8%, and by 2025 will account for 16% of new devices (10.8 billion). Fully 45% of new devices in 2025 are likely to be those used for building automation (30.2 billion).

Exhibit 2:

DEVICE APPLICATION	MILLION DEVICES IN 2019	MILLION DEVICES IN 2025
Building Automation	12,964	30,155
Connected Cars and Telematics	977	1,630
Vending/Retail Terminals	104	388
Healthcare and Medical Devices	155	503
Enterprise-issued and BYO Devices plus other personal electronics	1.888	4,998
Factory and Industrial Automation	2,768	10,824

This rapid rise in the number of endpoints is only one of the challenges for business cybersecurity. Additional challenges are explored in more detail on the following pages.

> **Many applications are forecast to see double-digit annual growth rates to 2025. Industrial IoT devices will have one of the highest growth rates at 25.8%, and by 2025 will account for 16% of new devices (10.8 billion). Fully 45% of new devices in 2025 are likely to be those used for building automation (30.2 billion).**

Ensuring Control and Visibility across Ever-Increasing Endpoints

Complicating the growth in the number of connected devices is how different components of a business use and manage different devices. Businesses must track, secure, and update thousands of connected devices internally and across a diverse value chain.

Simplifying the Security Solution Landscape

Today there are literally thousands of security solution providers; as the threat landscape continues to evolve, the number of vendors continues to grow. For an enterprise to keep up with the market is a near-impossible task requiring resources that are unrealistic. Additionally, the more vendors an enterprise deploys, the greater the risk in terms of point-to-point security vulnerabilities and interoperability maintenance issues.

Managing Scale

The IoT has created a scale issue where the size of the environment of endpoints, data, and threats is making the job of the CIO and CISO unmanageable. The demand for instant communications and the market's cybersecurity skills shortage contribute to the growing scale problem.

Mixing of Personal and Enterprise Devices

The rise of BYO in the modern enterprise means that many businesses are now faced with managing a mixed environment of corporate and personal devices, with personal devices bringing their own set of security challenges. Even before COVID-19 restrictions forced many more employees to work from home, a Frost & Sullivan survey indicated that 70% of US businesses have official BYOD policies. This means that the businesses' IT departments support employee-owned equipment, usually smartphones (94% of BYOD companies) and, to a lesser extent, tablets (58%). Support for personal laptops is significantly lower, and for other devices negligible. Typically, the security extends to allowing access to smartphone apps for email, CRM, data dashboards, and other systems. Some companies also have proprietary messaging networks. Considerably fewer enterprises secure personal—or even their own—devices in terms of talk and text, which can leave these devices vulnerable to a cyber intrusion if company or customer information is transmitted through unsecured channels.

> **“ Having a reliable partner that can stay ahead of the risks across all major aspects of the enterprise is a modern business imperative.**

In any enterprise, a user's personal or company-issued device will be in contact with numerous other devices and systems. For example, third-party apps are a potential vector for malware: app stores detect and block an average of 24,000 malicious apps per day.[12] The average smartphone user is estimated to have between 60 and 90 apps on the device.[13] Phones, tablets, and laptops may also link to connected cars and smart home solutions (smart TVs, connected thermostats, video doorbells, and surveillance cameras—the latter of which are among the most-hacked home devices), and will connect to home networks as well as less-secured third-party Wi-Fi.

Any one of these intersections is an open vulnerability through which a threat actor could gain access to important company information or systems, with significant damage occurring in the months it often takes to detect a security breach. This makes it difficult to create and execute comprehensive safeguards for the entire connected ecosystem. Having a reliable partner that can stay ahead of the risks across all major aspects of the enterprise is a modern business imperative.

The Human Factor

End users bring with them a separate set of risks—in most cases unintentional and not malicious. As the number of endpoints, apps, and risks increases, so does the number of passwords an individual has to recall. End-user fatigue with security protocols often results in security workarounds being employed or relaxed security hygiene. Additionally, phishing attacks are becoming more sophisticated and prevalent, creating an increased security risk of individuals clicking on the links.

SECTION 2: UNDERSTANDING CYBERSECURITY AND ENDPOINT CHALLENGES OF MAJOR INDUSTRIES AND APPLICATIONS

In addition to the overall enterprise need, Frost & Sullivan assessed the potential for BlackBerry to address business security by major industry or application. Exhibit 3 below summarizes these capabilities and Frost & Sullivan's assessment of viable coverage. The key parameters for this assessment were as follows:

- BlackBerry provides broad and comprehensive coverage for any industry that relies on endpoints.
- Industries with a higher proportion of new endpoints and devices, such as connected cars, would be fully within BlackBerry's capabilities, whereas those with aging and/or dated OT solutions, or industries with a breadth of infrastructure (such as energy and telecom), may have more network security needs. Many, but not all, of these aspects are currently covered by BlackBerry, though they are part of its longer-term innovation roadmap. However, even in the latter industries, endpoints still dominate the proportion of vulnerable access points.

Exhibit 3: Summary of Impact by Industry/Application

INDUSTRY/APPLICATION	ENDPOINT VS. NETWORK AS PRIME CONCERN	PERCENTAGE OF THREAT COVERED BY BLACKBERRY
Corporate/BYO Devices	Endpoints by definition. Phishing to get individual and corporate data.	100%
Automotive	Endpoints by definition. Customer data is high. Vehicle control possible but not common.	100%
Building Automation	Endpoints. Phishing for credentials. Access surveillance cameras and other devices. Some network as well.	95% or more. Some network-only building systems may not be covered.
Vending/Transaction Terminals	Endpoints by definition. Customer data. Main way of hacking retail.	100% of new devices; existing market varies by age of installation.
Healthcare and Medical Devices	Endpoints. Phishing to target medical records and devices. Unintentional third- party and insider-related attacks are high.	Up to 100%.
Manufacturing	Endpoints to get company information, and in some cases to cause system disruption. Network possible as well as some devices are only networked.	90% or more. Some network-only systems may not be covered. Also, physical entry points such as USB-based attacks.
Finance and Banking	Endpoint for phishing to gain credentials and customer info.	Up to 100%.
Telecommunications	Endpoint for phishing to gain credentials and customer info. Some network control for disruptions.	95% or more. Some network-only systems may not be covered.
Energy/Utilities	Endpoint for phishing to gain credentials and customer info. Network and even physical control to cause system disruptions.	95% or more. Some network-only systems may not be covered.
Government	Endpoint for phishing to gain credentials and launch malware to cause system disruptions.	Up to 100%.

Corporate/BYO Devices

While not an industry but an application, BYO and enterprise devices pose a security challenge across virtually every market. This has been exacerbated by COVID-19 work-from-home restrictions. Many large enterprises have already stated that they will allow a large part of their workforce to remain remote even after the pandemic abates. Even before this occurred, however, many business IT departments were already supporting employee BYOD. The savings in office space and commute time will likely encourage many more businesses to continue to extend work-from-home privileges.

Assessment of BlackBerry's coverage: BlackBerry's solutions began in the world of portable electronics, and this thread continues through its wide array of solutions that go beyond innately securing devices to the systems that those devices use and the information that they share. For example, BlackBerry's QNX system innately protects a device and its operating system from the point of its manufacture—a feature that makes it relevant to virtually any connected component or device.

Beyond this, BlackBerry continues to cover this area extremely well, and its value proposition is particularly applicable given the growth of BYO. It can secure the use of any device—enterprise or BYO, whether it has QNX embedded or not—through its UEM technology, which includes solutions such as Virtual Desktop and VPN-optional file and data sharing through its Workspaces. It also covers all manner of communication (talk, text, messaging, and email) with its private instant messaging network and BlackBerry SecSUITE, a government-grade security system that ensures that all communication with a device is shielded. BYOD talk and text is an alarmingly under-secured aspect of enterprise communication, frequently conducted on the device's default system and highly susceptible to man-in-the-middle and other surveillance-style attacks. Using SecSUITE for conversations with customers or colleagues ensures security regardless of the device's overall IT management.

As BYO and enterprise devices permeate all industries, BlackBerry's ability to cover this application is a major step towards protecting any business and vertical.

Automotive

Frost & Sullivan research shows that the automobile industry is undergoing a disruptive transformation, with automakers partnering with—and even becoming—tech companies, and cars evolving into connected, mobile platforms. Major digital trends impacting this industry include autonomous functions, augmented and virtual reality, in-car commerce, biometrics, and vehicle-to-infrastructure solutions. Cybersecurity is rapidly becoming inseparable from almost any aspect of vehicle operation, efficiency, and safety, as well as customer data integrity. Vehicle user information will be increasingly commingled with vehicle data, from current trends of linking insurance premiums with real driving patterns to future solutions such as analyzing geolocation data and purchasing histories. Frost & Sullivan estimates the market stemming from new business models that can monetize user, vehicle, and content data could be worth $180 billion.[14]

Assessment of BlackBerry's coverage: In essence, the car of the (near) future will be a mobile, connected device, encompassing multiple other connected endpoints and systems. BlackBerry's endpoint security is both a comprehensive fit in cybersecuring automobiles as well as allowing automakers to safely add more connected vehicle systems. As safety is a key concern with connected and increasingly autonomous vehicles, BlackBerry QNX provides a smart and secure operating system and middleware. BlackBerry developed this solution from the ground up with safety and security leading the development and is the trusted partner of the automotive industry today across original equipment manufacturers (OEMs) and Tier I suppliers.

Modern vehicles also operate based on the interaction of connected devices and systems within the vehicle. Hence, another example of a relevant solution that many OEMs rely on is Certicom, for securing autonomous features such as parking assist and lane detection. The car reads the automated features and, if any have been replaced, will not operate.

> **“ Cybersecurity is rapidly becoming inseparable from almost any aspect of vehicle operation, efficiency, and safety, as well as customer data integrity.**

BlackBerry's reach extends into the ecosystem as well. BlackBerry Radar provides asset tracking and is widely applicable to the transportation and logistics industry. After a part arrives at its manufacturing or assembly location, the OEM can ensure that the component's source code is secure with BlackBerry's Jarvis, which scans the code on all incoming components with embedded software to check for any cyber vulnerabilities.

Because of BlackBerry's security solutions, OEMs can move more aggressively into modernizing vehicles while keeping them safe. In 2019, BlackBerry technology was already securing more than 150 million vehicles, and the company has relationships with almost all major automakers and their Tier I suppliers.

Building Automation

Digital transformation trends such the surging number of IoT devices, adoption of AI technologies, and cloud-based data analytics are at the heart of the intelligent building industry. Frost & Sullivan research indicates the top drivers for smart buildings are occupant comfort (HVAC systems, lighting, and air quality), safety and security (both physical and digital), and energy management. Intrinsic to these is the need for remote monitoring and control of connected endpoints, which tend to be vulnerable because many building owners and operators do not anticipate cyberattacks, and older systems are not easily upgradable with new cyber-defense technologies.

Assessment of BlackBerry's coverage: BlackBerry's solutions can be embedded in new devices, secure the communication between devices and larger systems, and secure the systems themselves. They can also protect the communication between operators and systems. By and large, BlackBerry can cover the vast majority of intelligent and connected buildings, though it may need to do so with value chain partners such as OEMs or facility management service providers, rather than directly with building owners and operators. However, BlackBerry's UEM and UES are umbrella solutions that enable AI-based intelligent security across devices and systems, whether those using the solutions are part of the building team or third-party service or equipment providers. Multi-factor authentication and closed networks help secure all parties that need frequent monitoring and control of building systems as well.

Vending/Transaction Terminals

Considered the entry point for many attacks against the retail industry, vending machines and other transaction terminals/point-of-sale (POS) systems are a legitimate concern for identify theft. Being out in public and accessed by many more users on a daily basis than most endpoints makes them especially vulnerable. The rise of smart chips in credit cards and contactless payment has helped to greatly reduce the usage and effectiveness of illicit card skimmers and scanners, but they still pose a threat in thousands of older pay-at-the-pump gas stations and other unmanned kiosks. Vending and POS systems also are often under secured in how they connect online, increasing the potential for man-in-the-middle attacks.

Assessment of BlackBerry's coverage: In an industry that is by default endpoint-based, BlackBerry's solutions can easily cover all new devices coming into operation for this market. BlackBerry has a long history of securing POS terminals—even predating its smartphone business. Some older endpoints that were not originally secured by BlackBerry may not be upgradable, and their replacement may pose a challenge due to their dispersed locations. However, swipe-only, non-chip reading machines are quickly being phased out because the move to chip-secured card is almost complete and contactless payment is growing rapidly.

Health and Medical Devices

The healthcare industry has numerous cybersecurity challenges, and is one of the hardest-hit industries by threat actors.

Among the challenges:

- A high number of connected healthcare devices are not secure. Reasons range from older systems that were not built for security to poorly executed cyber strategies. Patients may have 10 or more connected medical devices in use during a hospital stay; even implantables such as pacemakers are at risk.

- Patient information needs to be accessed (often remotely) by a number of parties: primary and specialty care providers, insurance partners, billing services, and emergency responders among others. This results in more data breaches—although often unintentional—by internal personnel or third-party partners than any other than any other industry. Third-party vendors account for about 30% of data breaches and, by some estimates, another 31% are from accidental employee-related disclosures.

- Medical records carry a high premium on the dark web and are a lucrative target.

The digitization of millions of medical records and the continued advancement of diagnostic, monitoring, and treatment-related technologies have resulted in a complex healthcare ecosystem. As with any vertical, it behooves the industry to find partners that can help secure its systems and records, so that providers can focus on their core competencies of improving health and saving lives.

> **“BlackBerry Identity and Access Management can mitigate insider- and third-party-enabled breaches by allowing enterprises to manage the network of users and their access to devices and data, whether they are employees, value chain partners, or even the patients themselves.**

Assessment of BlackBerry’s coverage: While network breaches have been reported in the industry, Frost & Sullivan research indicates that by and large security must focus on endpoints. BlackBerry solutions are applicable to the vast majority of the market. Their primary challenges—securing endpoints, enabling remote access and controls from other devices and third parties, and educating employees on cybersecurity best practices—are all in BlackBerry’s wheelhouse.

For example, BlackBerry Identity and Access Management can mitigate insider- and third party-enabled breaches by allowing enterprises to manage the network of users and their access to devices and data, whether they are employees, value chain partners, or even the patients themselves. This includes ongoing user authentication using advanced analytics to create a secure but user-friendly interaction, as provided by BlackBerry Persona. BlackBerry services also help the healthcare system implement these solutions across their users and systems.

Manufacturing

Manufacturing is one of the most complex and connected industries. It is the original source for automation and a major driver of the digital technologies that are now transforming all other industries. Beyond the factory floor, connected devices are controlling and monitoring equipment in the field, communicating across supply chains, informing logistics, and being used in feedback loops from customer sites to help improve product design. Despite all these advancements, the industry is still plagued with vulnerable legacy equipment and unsecured devices. By some accounts, nearly half of all industrial control systems have faced some level of cyber threat.[15] Older IoT endpoints may be connected to local networks or hardwired into systems such as landline telephone or Ethernet that can be harder to attack; even though they do not carry modern cybersecurity software, they may be less desirable targets because they do not allow migration to other data and systems. Quite often, the IoT endpoint is not the intended target for an attack, but a door to larger system disruption or data access.

Assessment of BlackBerry's coverage: By and large, connected manufacturing is about connecting endpoints. Minus some older, less-sophisticated networked equipment, BlackBerry is well positioned to provide support across this market. BlackBerry can also bring in additional services, such as secure and multi-path alerts and emergency communication through its AtHoc solution, and logistics/asset tracking through its BlackBerry Radar solution.

Finance/Banking

Along with healthcare, the finance and banking industry is one of the largest targets for cyberattacks. However, unlike healthcare, finance and banking recognized the threat posed to its data early on and is one of the most active in implementing strong cybersecurity practices. Nevertheless, the sheer volume of attacks—and value of financial records—means that some attempts are successful, often with devastating results. Citibank, JP Morgan Chase, Equifax, MasterCard, Countrywide, and many other well-known companies have had high-profile data breaches involving thousands or even millions of compromised customer records.

Assessment of BlackBerry's coverage: Access to financial information and other credentials largely comes from phishing attacks that need a device or other endpoint as an entry point. Most of this industry's vulnerabilities lie in those endpoints that BlackBerry's solutions, such as the BlackBerry Spark platform, cover effectively across the spectrum. Even if a threat actor already has credentials, access must be from a remote, external point; the ability to identify an unauthorized device can prevent access. The financial services industry has already largely deployed BlackBerry technology across enterprises.

Infrastructure Markets: Energy/Utilities and Telecommunications

The energy industry is vast and complicated, with a long history of mergers and acquisitions (particularly in the United States) that has meant integrating disparate data sets and endpoint systems over time. The market's complexity in asset ownership and management adds to its vulnerability: each country, state or province, or region may have different levels of public versus private ownership and competitive versus non-competitive markets. In some markets, utilities may generate, transmit, and distribute their power; in others, they augment that power or must buy (and cannot generate their own) power from independent power producers or other utilities. The power that supplies the grid may come from any combination of central power plants and distributed sources, such as rooftop solar systems at homes and businesses, or energy storage banks along the grid.

The retailing of power varies as well: depending on the market, power can be purchased from an investor-owned utility, member-owned cooperative, a municipality, a power marketer, or a government entity. Third parties also play an increasing role: they may help aggregate multiple small users into larger power purchasing blocks that can negotiate better rates or coordinate multiple users in energy saving/peak shaving programs.

This means that customer information and usage data, and potentially information across the power grid and even into power generation, is often shared among a growing number of parties. The ownership and responsibility for cybersecurity across assets and systems gets muddied. Threat actors can leverage this to find weak links and steal customer or institutional information, or even disrupt the power system itself.

The telecommunications industry has similar challenges in the various parties that own assets and share customer information across a vast network. In fact, the early days of energy deregulation used the telecommunications industry as a model for how such a system could be successful. While energy proved to be a more difficult market to unbundle, telecom was arguably more successful at divesting operations and retail at first, though cellular markets have recreated more vertically integrated business models to some extent.

As with finance/banking and healthcare, telecommunications is an attractive target for threat actors because of the high volume of personal data that telecommunication companies (telcos) store. And, as with energy, telcos can be a target for "hactivists" who have a goal of disrupting infrastructure.

Assessment of BlackBerry's coverage: BlackBerry's technologies, including BlackBerry Certicom, are well designed to secure these endpoint-heavy markets. On the energy side, power meters, connected high-voltage power transformers, and myriad safety, security, and power quality devices along the system fall within BlackBerry's purview. There may be some purely network-based systems in the industry, but by and large power generation, as well as transmission and distribution, has rapidly evolved to encompass systems based off of IoT-connected endpoints.

Telecommunications also has network-based challenges, though its endpoints are even more modern and easy to secure that what is found across the energy spectrum. In both cases, the challenge is to ensure that multiple, disparate parties that access data and systems can do so in a manner that can be authenticated, tracked, and made resilient against attacks.

Government

Federal governments have long been a target for hacktivists, rogue states, and other threats, but they also tend to have some of the largest budgets and broadest resource networks for fighting these challengers. More recently, threat actors have started targeting state and local entities that may not have the knowledge or abilities to protect themselves as well. This is coinciding with the rise of smart cities, a hallmark of which is multiple city divisions sharing insights and strategies across intelligent platforms driven by analytics and fed by a wide array of connected endpoints. For example, a city's health department may help fund and implement improvements in automated traffic control, because less congestion on the road can mean cleaner air and faster travel times for first responders.

Assessment of BlackBerry's coverage: The breadth and depth of cybersecurity across the government sector is immense. It can include everything from securing drones used for surveying disaster relief needs to full national security programs. Endpoints within government purview overlap with many of those noted above as well: managing fleet vehicles, overseeing energy and telecommunication systems, running hospitals, and securing personal financial data, among many others.

For example, the rise of smart cities has meant significant and continued growth of connected endpoints across infrastructure. Smart streetlights are being outfitted with additional sensors that can measure levels of traffic or air pollutants, detect gunshots or unusual crowd activity, and even help with predictive garbage collection. Public transportation is using an increasing array of sensors and analytics to provide better predictions of travel times. Drones inspect infrastructure and investigate suspicious activity. This all presents a strong opportunity for BlackBerry to secure endpoints, as well as the third-party apps that allow residents and visitors, for instance, to access city information and services.

A major aspect of government activity also centers on public alerting and emergency response, something that has come to the forefront as a result of the COVID-19 pandemic and protests against racial inequality and police brutality. These are critical aspects of local, state, and national health and safety, often requiring cooperation across agencies and the private sector. BlackBerry addresses these challenges comprehensively as well, with 85% of the US government and 18 of the G20 governments already connected and protected with their BlackBerry Spark and BlackBerry AtHoc solutions.

NEXT STEPS FOR BUSINESSES TO ENSURE COMPREHENSIVE SECURITY

Almost all businesses have some level of cybersecurity strategy already in place. It may be as simple as ensuring Wi-Fi is encrypted and employees change email passwords regularly, to full cyber intelligence divisions that create and implement best-in-class technologies and protocols.

Key questions that can help guide this process include:

- Is there is visibility across, and accounting for, all endpoints and entry points?
- Does this include endpoints managed by OT and IT, as well as employee BYO devices? How is remote data access managed by workers, suppliers, customers, regulators, and others who may require data access?
- Do employees or value chain partners use the same level of care and secure programs with authentication protocols for talk and text as they do for emails or other systems?
- Is there security that covers the breadth of this access: embedded on the endpoint or device itself, across all the data it uses and transmits and the systems it integrates, and a unified platform to manage and secure the entire system?
- Can the business test products and components coming in for cyber vulnerabilities, whether from external vendors or across transport networks?
- How does the business create a secure force field that includes enterprise and non-enterprise devices?
- Are there smart technologies that can keep up with and even intelligently evolve ahead of the threat landscape, in terms of the number and sophistication of threats, and the number of entry points?

It behooves all businesses to take a step back and ensure that two critical factors are in play: endpoint security is the foundation of their strategy, and their solutions are not fragmented across multiple vendors, which has been shown to increase costs and decrease cybersecurity effectiveness. They must also implement a zero-trust philosophy if they are to realize an effective strategy. This is as critical for brand reputation and stock price as it is for business operations. Partnering with a solution provider that has the technologies to comprehensively secure an enterprise's data and communication is by far the most effective way to ensure security, resilience, and uninterrupted business continuity.

ENDNOTES

1 Sources: https://purplesec.us/resources/cyber-security-statistics/ https://www.cnbcafrica.com/africa-press-office/2019/12/12/malware-variety-grows-by-13-7-in-2019-due-to-web-skimmers/ and Frost & Sullivan analysis

2 https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

3 FBI Reports 300% Increase in Reported Cybercrimes

4 https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

5 https://www.statista.com/statistics/536764/worldwide-it-security-budgets-as-share-of-it-budgets/

6 Source: Marketingcyber.com and Frost & Sullivan analysis

7 https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

8 https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

9 Ponemon Institute

10 https://purplesec.us/resources/cyber-security-statistics/

11 Frost & Sullivan conducts independent market and industry research and analysis.
We do not conduct technical testing.

12 https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

13 https://9to5mac.com/2017/05/05/average-app-user-per-day/

14 Frost & Sullivan Global Connected Car Market Outlook, 2020, K47E

15 https://www.zdnet.com/article/half-of-industrial-control-system-networks-have-faced-cyber-attacks-say-security-researchers/

NEXT STEPS

- Schedule a meeting with our global team to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.
- Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.
- Visit our Digital Transformation web page.
- Attend one of our Growth Innovation & Leadership (GIL) events to unearth hidden growth opportunities.

Silicon Valley
3211 Scott Blvd
Santa Clara, CA 95054
Tel 650.475.4500
Fax 650.475.1571

San Antonio
7550 West Interstate 10
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

London
Floor 3 - Building 5,
Chiswick Business Park
566 Chiswick High Road
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

✉ myfrost@frost.com ☎ 877.GoFrost 🌐 http://www.frost.com

FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041

FROST & SULLIVAN