opentext™

The Future of Cyber Resilience

CEO White Paper

Mark J. Barrenechea
OpenText CEO and CTO

Contents

Introduction

Information is our greatest strength.

It allows us to adapt to new situations in a changed world, meet higher demands, manage more complex requirements and reach extraordinary goals. Information empowers us to make smart decisions and lead our organizations towards growth. Information has never been more important.

And it has never been in greater danger.

Cyber criminals are busier than ever, devising new ways to get past protective walls. The old strategies for protecting our information are no longer enough.

It is time for new security solutions. It is time to build cyber resilience for the future.

We Live in Two Worlds

It is not hyperbolic to say that 2020 has changed everything. It is a new equilibrium. COVID-19 has accelerated technological disruption and driven profound changes to the ways we work, live, shop and experience our lives.

Work-from-anywhere will be a permanent part of our reality moving forward. Direct-to-consumer has erupted and will never be put back in the box. Contactless retail and social commerce are now intrinsic to the customer experience. New supply chains will emerge. Time to Value has gained an immediacy that is here to stay.

We now live in two worlds simultaneously—the virtual and the physical.

People have migrated to the virtual world *en masse* since the beginning of the pandemic, straining the system with colossal demand and galactic connectivity. The digital world is no longer an abstract concept. It is a reality.

Yet we need to stay grounded, too. In the physical world, we make scientific breakthroughs, keep our families safe, serve our communities, care for our health and explore our planet. It is where organizations produce the products we need, at phenomenal scale. It is where hope thrives as we watch new developments in vaccines, almost every day.

The virtual and the physical are coming together—but underpinning it all, we need trust and protection. To keep both worlds operating, cybersecurity must be Job #1.

Organizations need security in the cloud to enable work-from-anywhere. They need intelligent threat detection and forensics to protect the edge, to keep employees and devices safe, no matter where they are. Retailers need secure ecommerce platforms to deliver the products and services their customers want, overnight. Hospitals need protection for data and records so patients' privacy is protected and they can receive critical care.

We need to run the new equilibrium on a platform of security, protection, trust and resilience. Without this platform, both the physical and virtual worlds will fail.

The Great Rethink

Rapid changes to the physical and virtual worlds have catalyzed a "Great Rethink" across all dimensions of human existence: economic, societal, technological, environmental, individual, geopolitical and industries. The Great Rethink is our opportunity to shape both worlds in the new equilibrium, now and in the future.

This is how we are operating at OpenText. *This* is what drives our mindset, our innovation agenda, our customer agenda, our market agenda. We are moving forward with the new equilibrium.

OpenText is designing the next era of technology—technology that will enable organizations to rethink cybersecurity and respond to new threats in the midst of breakneck global change.

OpenText's roadmap is centered on our five pillars and five guiding principles, working in tandem.

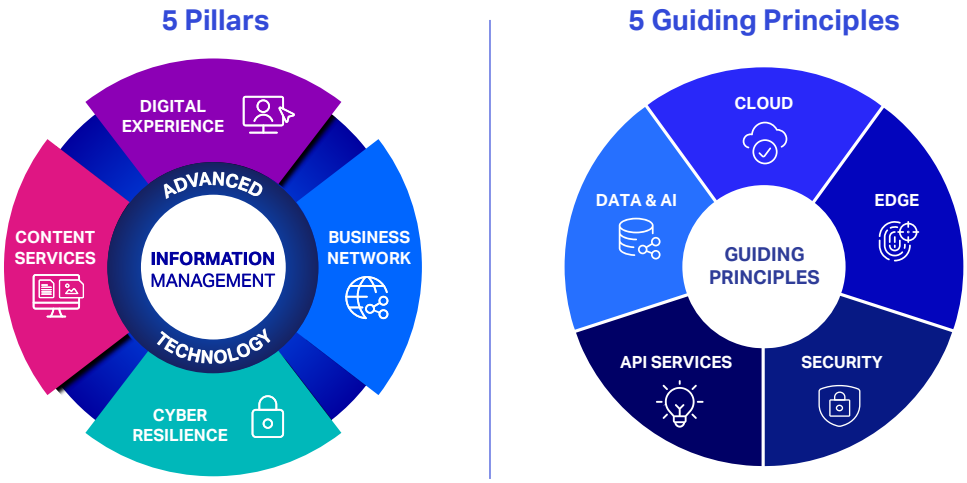


Figure 1:

OpenText's Five Pillars and Five Principles

Our Information Management strategy encompasses Content Services, Business Network, Digital Experience, Cyber Resilience and Advanced Technologies (such as developer tools, AI and others).

Likewise, five essential principles guide us as we rethink and evolve: Cloud, Edge, Security, API Services, and Data and Artificial Intelligence (AI).

All of this must be secure. In fact, cyber resilience and security underpin all of our other pillars and principles. Upon this strong foundation, OpenText's comprehensive platform of trust empowers Information Management in the cloud and on the edge, driven by APIs and services, and layered with data and AI capabilities.

Without a secure, trusted platform, nothing else matters. This is the key to rethinking cyber resilience and thriving in the new equilibrium.

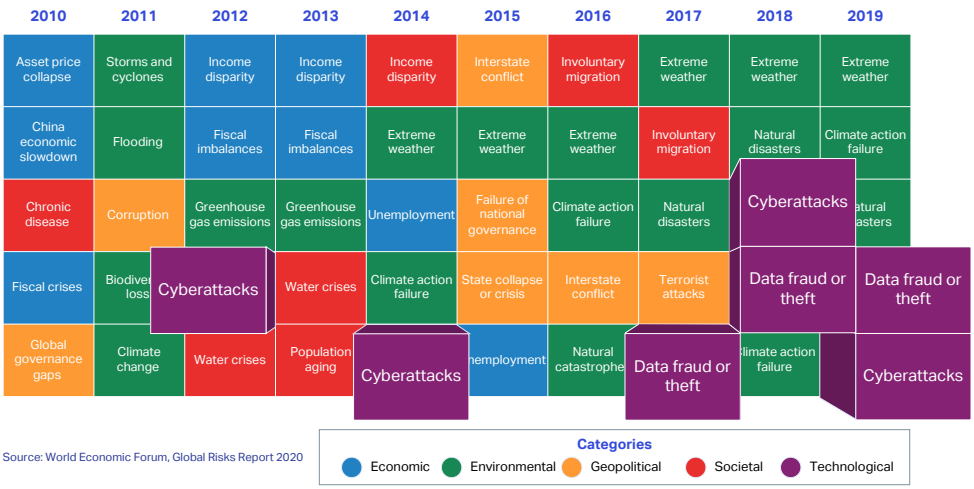
opentext™

New World. Rising Threats.

Cyberattacks are a top global risk.

In the World Economic Forum's Global Risks Report for the past two years, the top five threats were split into two key areas—environmental and technological. Physical and virtual. Our two worlds, both at risk.

Cyberattacks and data fraud or theft, which were not even on the radar 10 years ago, now represent two of the five biggest risks. *Two of the five*.



Source: World Economic Forum, Global Risks Report 2020

Figure 2:

Top Five Global Risks, 2010-2019[1]

The events of 2020 have exacerbated these digital risks. We have become more dependent than ever on technology, and this has made us more vulnerable. Security risks and challenges continue to rise.

Endpoints have exploded. Widespread work-from-home means employees are working on less secure home networks, often using personal devices. Most home-based offices involve exposed endpoints that are disconnected from the safety of a corporate network or enterprise VPN. Personal devices used for work could have multiple users, and home Wi-Fi networks are not always locked down to outside users.

The rise of the Internet of Things (IoT), coupled with work-from-anywhere, has dramatically expanded the endpoint attack surface. Estimates suggest there are now 22 billion endpoints, expected to spike to 50 billion within the next few years.[2]

The great cloud migration continues. As more and more companies move into the cloud, they are increasingly relying on third parties, giving these providers data, credentials and access. But not all third parties are created equal, and those with subpar cybersecurity practices leave organizations exposed.

Human behavior is also a top security challenge—our compassion, our very humanity itself, leaves us vulnerable to phishing campaigns, social engineering and other malicious attacks. In fact, 53% of breaches are caused by simple human error from the enterprise's own employees.[3]

The notion of a defensible "perimeter" has been obliterated. **Assume the bad actors are already inside**. An organization is not a house with windows and doors that can be locked. The dwell time for threats in a corporate network can be as high as 800 days.[4] This means the threat enters the system and waits months or years before acting. Traditional security does not have the tools necessary to root out these lurkers before they can do harm. Malicious insider threats—like disgruntled employees, corporate espionage or foreign government agents—must also be guarded against.

Finally, **new technologies** constantly create new cyber risks. With 5G, bad actors can exfiltrate data much faster, leaving organizations with little time to react. And within the next five to ten years, quantum will make it possible to pick every cybersecurity lock imaginable. Two-factor authentication will not even slow the bad actors down. In fact, in five years, it will no longer exist.

The Costs of Cyberattacks

Cyberattacks have increased five times since the start of the pandemic.[5] Throughout the past year, organizations have seen astounding spikes in ransom amounts, malicious files and fraudulent websites.

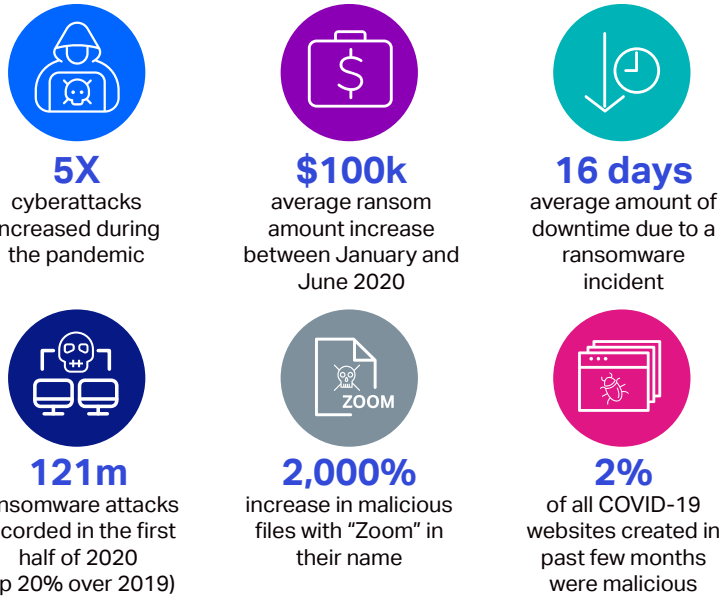


Figure 3:
Cyberattacks in 2020[6 7 8 9 10 11]

These increases have massive ramifications for businesses. When an endpoint is attacked, users and IT departments experience a 37% drop in productivity.[12] Ransomware causes over 16 days of downtime, on average.[13] Right now, no business has a single day it can lose, never mind more than two weeks! To make matters worse, 51% of businesses cite "loss of customer confidence" as a result of downtime due to attacks.[14]

Nowhere is the need for cybersecurity more evident than among healthcare organizations and research teams, which have become top targets for cyberattacks. In the fall of 2020, the New York Times reported that a massive ransomware attack hit eResearchTechnology, a health tech company whose software was being used in hundreds of clinical trials, including research on COVID-19 vaccines and therapeutics. Those trials slowed almost to a halt during recovery, setting back urgently needed medical research in the fight against the pandemic.[15]

Around the same time, a hospital network with more than 400 locations in the US suffered a ransomware attack, believed to be the largest medical attack of its kind. Other US hospitals had their records frozen, and were forced to delay surgeries and turn away ambulances.[16] And an attack on a hospital in Germany resulted in loss of life when a patient died during relocation, as hospital systems shut down.[17]

We need new strategies, and we need them *now*.

Information Governance

In addition to rising cybersecurity threats, organizations that operate in multiple countries around the world face increasing numbers of rules, standards and regulations surrounding information governance. There are currently over 100,000 such rules—and that number is growing all the time.

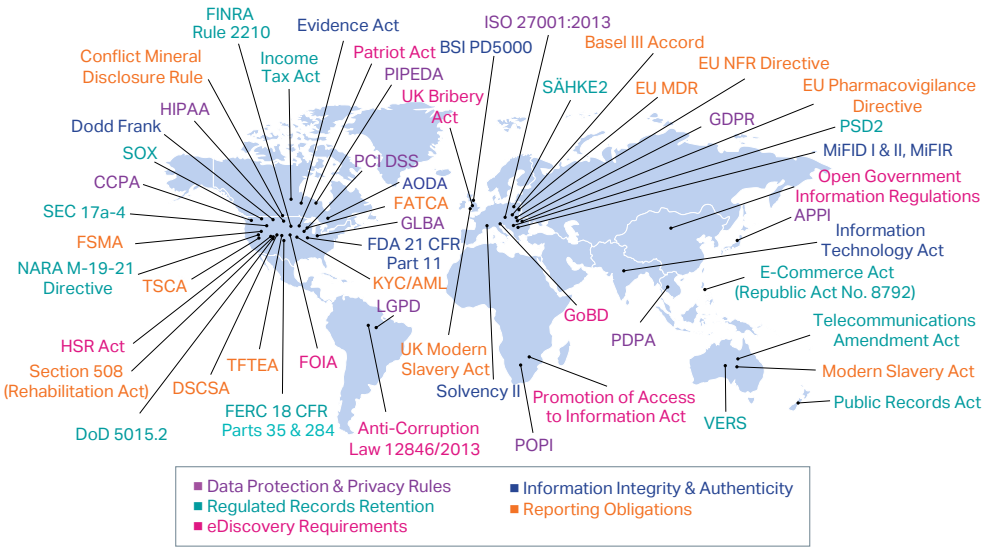


Figure 4:

Global Information Governance: More than 100,000 Rules, Standards and Regulations

These regulations set out requirements for personal information, credit card data, supply chain practices, financial security systems and numerous other areas. New technological strategies must fall in line with these regulations, to protect organizations, employees, partners and customers.

Cyber Resilience for the Future

Tomorrow's threats cannot be fought with yesterday's strategies. It is time to look at multilayered strategies and new digital capabilities in the cloud. It is time to give cybersecurity a reboot and begin building *cyber resilience*.

Building Cyber Resilience

Think of cyber resilience as digital fitness. It is the ability for an organization to absorb punches and get back on its feet, no matter what threatens.

The best way to withstand evolving threats and develop cyber resilience is through a layered approach, using a proven security technology that covers multiple threat vectors and is constantly up to date.

This technology must include both security and data protection and recovery, as well as advanced developments in machine learning and other technologies to protect the organization's critical information. A multilayered approach is simply the best strategy for keeping bad actors out and productivity up.

OpenText's Cyber Resilience Strategy integrates these principles across several core commitments.

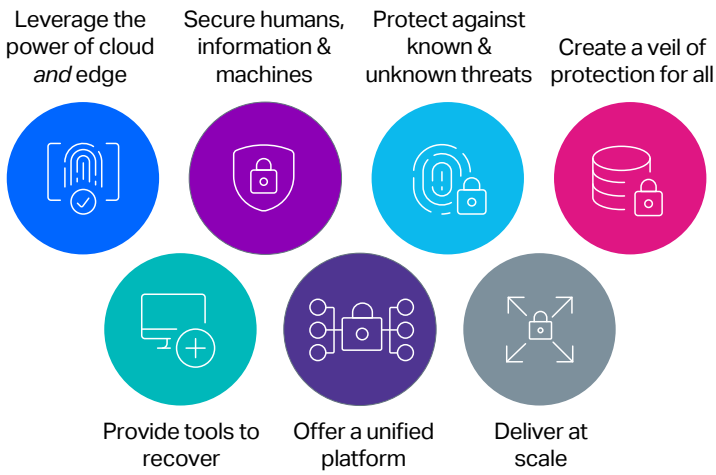


Figure 5:
OpenText's Cyber Resilience Strategy

Leverage the power of "*and.*" We believe in the power of the word *and*—and today, it is about cloud *and* edge. No edge, no cloud; no cloud, no edge. The first tenet of our cyber resilience strategy is recognizing this unassailable truth. It's your edge. Own it. Protect it. Secure it.

Secure humans, information and machines, regardless of the perimeter. Frankly, perimeters are disappearing altogether—but everything must be secured. The number of endpoints is exploding, and the bad actors are already inside. OpenText creates technologies to protect organizations in a world without castles and moats.

Protect against known and unknown threats with speed and accuracy. At its core, cybersecurity is a challenge involving data and information. If an organization had the information it needed to know an attack was imminent, it would not let the attack happen. If users knew that a link in an email was unsafe, they would not click it. If they knew that a file they downloaded from the internet was malicious, they would not open it.

Organizations cannot simply throw more humans at the issue. Instead, they must leverage advanced technologies, especially automation and AI, to sift through the vast volumes of information required to predict and detect threats. With the help of machines, like OpenText's BrightCloud threat intelligence technology, organizations can scan and analyze at (almost) the speed of light, to find new and emerging threats early, *before* they can inflict debilitating damage.

Create a veil of protection for the total community. OpenText serves a wide audience: CISOs, Chief Data Officers, R&Ms, MSPs, consumers, prosumers, investigators, forensic workers, law enforcement and more. We are committed to security and protection for all, for organizations of any size, from the smallest local businesses to the largest global enterprises.

Provide tools to recover. No organization will run smoothly all of the time. Attacks *will* happen. But OpenText has the toolset to recover data and restore operations with efficiency, and enable digital forensics and eDiscovery to ensure accuracy and compliance in both internal and external investigations. This real-time capability to find, classify and analyze data is critical for cyber resilience.

Provide everything on a common platform. Our technology roadmap includes increasing integrations in protection and security, and offering a single agent that delivers every component of a cyber resilience strategy: behavior analysis, digital investigations, digital collections, threat intelligence, endpoint detection and response (EDR), data protection, cloud backup and more.

Operate at scale and build on the phenomenal successes that we have already delivered to our customers around the world. Currently, OpenText has over three exabytes of data under management. We secure 250 million endpoints. We process 15 billion URLs per day. We detect over 220,000 threats. Our cloud has 99.99% availability—this means we only take off about eight seconds a week!

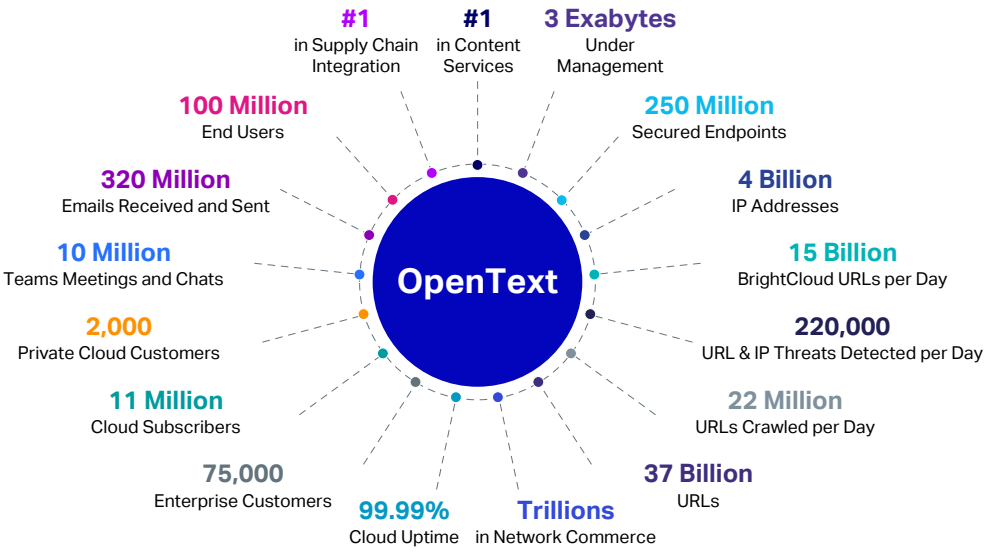


Figure 6:

OpenText at Scale

We are operating at galactic scale. We are ready to solve the security challenges ahead. And we have the technology to make it happen.

Protect Critical Information: OpenText Security & Protection Cloud

OpenText provides a foundation of security and protection for the virtual and physical worlds, and helps customers build their cyber resilience, all from one place: OpenText Security & Protection Cloud.

Security & Protection Cloud is one of our five expert, domain-oriented clouds, all of which deliver stunning capabilities across key business areas:

- **Content Cloud** connects content to digital business to improve user productivity, while meeting legal compliance and government requirements.
- **Business Network Cloud** connects any business, person, system or thing to build supply chains and trading ecosystems that are adaptable, ethical and sustainable.
- **Experience Cloud** delivers deeply personalized omnichannel experiences to customers at scale.
- **Security & Protection Cloud** provides organizations with the tools they need to keep intellectual property, customer records and sensitive financial information protected.
- **Developer Cloud** empowers developers to build applications and solution extensions quickly and cost-effectively using service-based capabilities in the cloud.

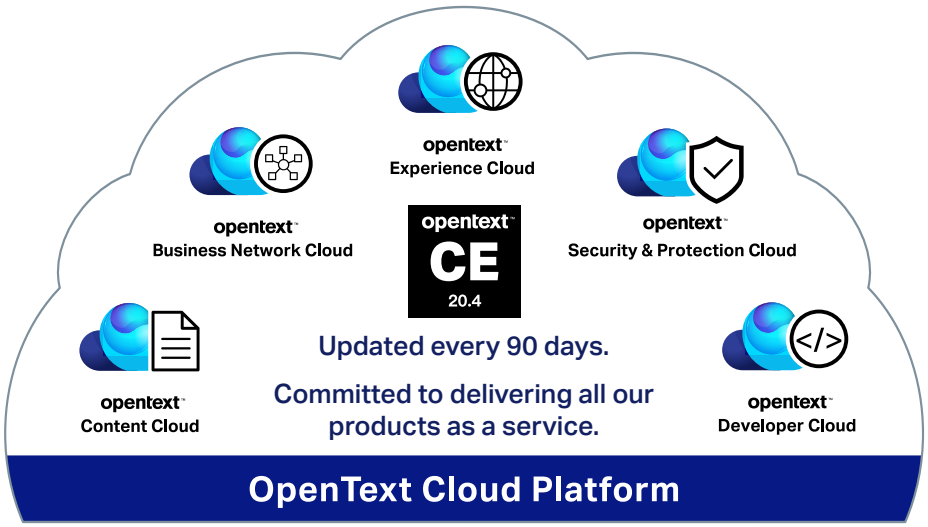


Figure 7:

The OpenText Cloud Platform

Security & Protection Cloud includes groundbreaking technologies from Carbonite, Webroot and BrightCloud, as well as the incredible EnCase suite of products. Carbonite's solutions provide superior protection against data loss, including from ransomware, accidental deletions, hardware failures and natural disasters. Webroot's solutions are award-recognized for their data security capabilities and protection for endpoints and networks. BrightCloud—a gem in the OpenText suite of products—has redefined online threat intelligence to keep organizations safe in a connected world. And EnCase provides unmatched digital forensics and security solutions to manage data visibility, reveal risk, discover malware and empower response. Together with Covisint Identity & Access Management and our eDiscovery solutions, OpenText delivers an unbelievably comprehensive portfolio.

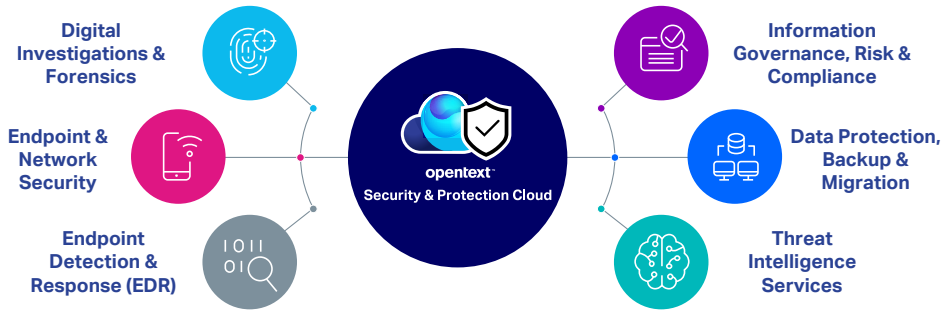


Figure 8:

OpenText Security & Protection Cloud

The security and data protection platform for business

opentext™ | EnCase™ CARBONITE® an opentext company WEBROOT® an opentext company BrightCloud® Threat Intelligence an opentext company

Digital investigations and forensics capabilities in the OpenText Cloud allow organizations to accurately analyze digital evidence to support IT, HR, compliance and law enforcement investigations. Users can more easily investigate endpoints off the corporate VPN, unlock and investigate more encrypted drive types, and collect from a range of cloud services. With the ability to gather evidence in the field and process it in real time, investigators can more quickly affect the outcome of a negative event.

In our latest software release, Cloud Editions 20.4, expanded OS and artifact support ensures security, legal and law enforcement professionals have unrivaled data visibility and investigation tools.

Endpoint and network security keeps critical systems, data and users safe from ransomware, phishing, malware and other cyberattacks. An integrated endpoint protection strategy manages all PCs, laptops, servers, mobile devices and other devices, as well as offering user prevention and protection features. Anti-phishing tools use threat intelligence and real-time machine learning to determine if a URL that a user is trying to access may be a phishing site. This technology is crucial, given the massive spike in phishing since the start of the pandemic.[18]

The OpenText platform provides next-generation endpoint protection and DNS protection, with a cloud-based console, fast deployment and scans, and contextualized threat intelligence. Coupled with Security Awareness training—vital, since humans are the weakest link in cybersecurity—Security & Protection Cloud provides organizations with multilayered protection.

Endpoint detection and response (EDR) enables organizations to detect cyber threats, then empowers them to respond to and recover from compromise. OpenText EnCase Endpoint Security, embedded with Webroot's threat intelligence, provides 360-degree visibility into the endpoint, for protection from new and unknown threats.

The platform also delivers over 250 detection rules aligned with the MITRE ATT&CK framework, to help organizations better detect and defend against known adversary behaviors.

Information governance, risk and compliance tools make it easier for businesses to navigate today's global market, where they must contend with an expanding number of standards and regulations. Security & Protection Cloud helps businesses identify and protect privileged, sensitive and confidential data from inadvertent disclosure to third parties. Managed security services help organizations keep up with evolving regulations, through a transparent, risk-based approach to managing personal data.

Data protection, backup and migration in the cloud allows businesses of all sizes to fill gaps in their protection. Organizations can restore a single file or an entire environment locally or in the cloud, ensure compliance with Disaster Recovery testing, and recover from ransomware attacks to get back up and running—fast.

New to Cloud Editions 20.4, enterprises can leverage Carbonite's solutions to protect from data loss on endpoints and in Microsoft 365 applications, and to ensure the availability of critical systems at all times.

Threat intelligence services protect employees from malicious URLs, IPs, files and mobile apps, through accurate, dynamic and near real-time threat insights.

OpenText's unified platform scans billions of IP addresses and billions of URLs across millions of domains, in addition to millions of mobile apps. It takes advantage of machine learning to classify and categorize each according to the threat it represents to business.

With our most recent release, BrightCloud Threat Intelligence services strengthen the reputation capabilities offered by EnCase Endpoint Security in the enterprise.

OpenText EnCase & Digital Investigations in the Cloud

OpenText's cyber resilience strategy includes a strong commitment to digital investigations and forensics. Our technologies enable law enforcement, corporations and government agencies to collaborate, work efficiently and get results.

We are helping **first responders, police departments and police leaders** to ensure that information is captured and available when it is needed most. We enable investigators and forensic examiners to complete more cases and find evidence—the needle in the haystack—faster.

Our solutions also help **corporations** with discreet and remote digital investigations on and off the network, to protect employees, investigate misconduct, and scrutinize IP theft, fraud, security incidents and data exfiltration. OpenText's technology helps investigators get to the bottom of negative events.

And we are helping **government agencies** with their own investigations into top security concerns—counterintelligence, human intelligence, anti-terrorism and human trafficking—to make the world safer for all.

We are also committed to growing our partnerships with other organizations to ensure that our gold-standard technologies are widely available. We recently announced an expansion of our partnership with Microsoft: **OpenText EnCase Forensic and EnCase Endpoint Investigator are now certified on Microsoft Azure.**

As more and more organizations shift operations to the cloud, digital evidence often originates from or involves cloud sources. To access all digital evidence and reach accurate conclusions, investigative teams require compatibility and access to cloud sources.

Through Azure and EnCase, organizations can investigate devices anytime, anywhere, with less reliance on the corporate network or VPN. Law enforcement and corporate investigators can more easily collaborate across divisions and organizations, enhance evidence processing, investigate in cloud environments, and adjust more quickly to the needs of a remote workforce.

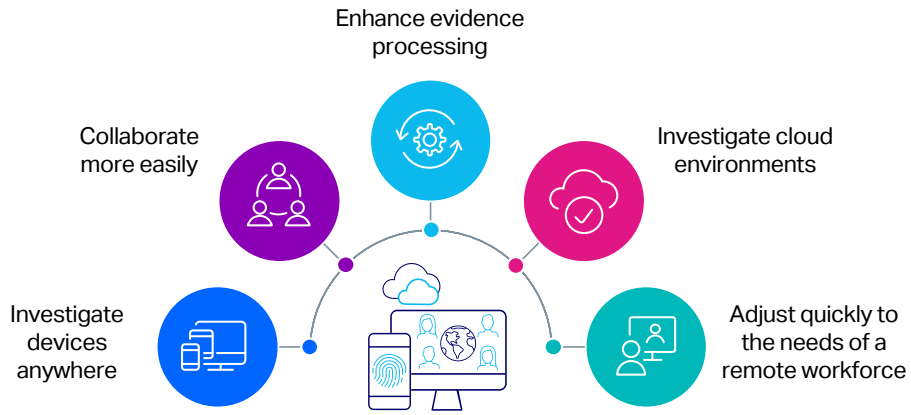


Figure 9:

EnCase for Digital Investigations

Comprehensive. Redefined.

Building cyber resilience requires a partner who has a proven track record of addressing organizational data at scale and can offer a comprehensive platform for security.

With Security & Protection Cloud, organizations can detect, prevent and recover from attacks, accidents and disasters that could otherwise put them out of business. It provides multilayered security that seamlessly fits into all business environments, and effortlessly ensures that data, users, devices and networks are secure.

Security & Protection Cloud is enterprise-ready. The same platform serves small and medium-sized businesses, as well as cybersecurity experts and consumers. One service for all. The most comprehensive platform on the market.

Ready for the Next Threat?

> *I hack the future. The things that we don't see in technology are the things that come back and bite us.*
>
> –Tarah Wheeler, Cybersecurity Policy Fellow[19]

OpenText is committed to cyber resilience, to delivering outstanding solutions across forensics and investigations, endpoint detection and response, cyber protection and data protection.

And there are no limits on how far we will innovate.

Going forward, OpenText will release more APIs, new machine learning solutions for investigative insights, and more modern sources for forensic artifacts, including MS Teams and Zoom, so that users have access to all the sources they need in order to respond to threats and investigate negative events.

We will persist in building and delivering a unified platform where all security and protection technologies come together in a single agent, with even deeper integration with BrightCloud Threat Intelligence, custom automated response actions, and managed detection and response.

We will increase endpoint visibility and offer improved dashboards, and we will add new support for data protection with server backup for MSPs, expanded platform support, and cloud recovery options, to make protection and recovery more seamless than ever.

Forensics and Investigations

- Public APIs
- Machine learning for investigative insights
- Triage workflows
- Modern forensic artifacts

Endpoint Detection and Response

- Deeper integration with BrightCloud Threat Intelligence
- Custom automated response actions
- Managed detection and response

Cyber Protection

- Increased endpoint visibility
- Improved dashboards
- Cyber resilience

Data Protection

- Server backup for MSPs
- Expanded platform support
- Cloud recovery options

Figure 10:

OpenText's Commitment to Cyber Resilience

We will continue to smash the expectations of the RMMs and MSPs we serve, with the ability to easily deploy, manage and calibrate capabilities through our consoles.

And we will further enhance our services for law enforcement and first responders, forensics and investigators, legal professionals, and the defense and intelligence communities. Every crime involves some sort of technology, and excellent digital forensic capabilities are essential to gaining a full picture and improving the outcome of events.

We are a trusted partner in the journey into the new equilibrium, and we will work with our customers to help them transform, secure the physical and virtual worlds, and build their cyber resilience. Helping build a safer world is in our DNA.

Do not wait. Cyber resilience must be Job #1.

It cannot be Job #6. It cannot get lost in day-to-day operations and to-do lists. It must be a chief concern in everything that organizations do, at a foundational level. The technologies of today are dying. Get current and stay current.

Times of uncertainty require bravery, empathy and foresight. Such times require leaders—at all levels—who can see and anticipate the advantages of the physical and digital worlds, but also the risks.

In the new equilibrium, where the next threat is often unknown, the best risk management strategy is cyber resilience. With it, organizations can ensure their sustainability, and meet the future with agility and growth.

Endnotes

[1]*"The Global Risks Report 2020,"* World Economic Forum, January, 2020, *http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf* (accessed November 2020).

[2]Tom Warren, *"Microsoft's CEO looks to a future beyond Windows, iOS, and Android,"* The Verge, January 21, 2020, *https://www.theverge.com/2020/1/21/21071108/microsoft-ceo-satya-nadella-iot-windows-ios-android-future* (accessed November 2020).

[3]Meera Narendra, *"Human error remains the main cause of data breaches,"* PrivSec Report, June 20, 2019, *https://gdpr.report/news/2019/06/20/human-error-remains-the-cause-of-data-breaches/* (accessed December 2020).

[4]*"2019 Mid-market Threat and Incident Response Report,"* Infocyte, July 2020, *https://www.infocyte.com/resources/mid-market-threat-and-incident-response-report/* (accessed December 2020).

[5]JJ Cranford, *"Announcing OpenText Security and Protection Cloud,"* OpenText, October 26, 2020, *https://blogs.opentext.com/opentext-security-cloud/* (accessed November 2020).

[6]Ibid.

[7]*"Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase,"* Coveware, August 3, 2020, *https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report* (accessed December 2020).

[8]Ibid.

[9]*"SonicWall's Mid-year Cyber Threat Report finds Malicious Microsoft Office Files on Rise, Ransomware Up in US, Globally,"* SonicWall, July 23, 2020, *https://www.sonicwall.com/news/sonicwalls-mid-year-cyber-threat-report/* (accessed December 2020).

[10]Kyle Fiehler, *"There are Savings to be Had in Cybersecurity. Just Not Where You Might Think,"* Webroot, July 13, 2020, *https://www.webroot.com/blog/2020/07/13/there-are-savings-to-be-had-in-cybersecurity-just-not-where-you-might-think/* (accessed December 2020).

[11]Ibid.

[12]*"The Third Annual Study on the State of Endpoint Security Risk,"* Ponemon Institute, January 2020.

[13]*"Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase,"* Coveware, August 3, 2020, *https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report* (accessed December 2020).

[14]*"The Third Annual Study on the State of Endpoint Security Risk,"* Ponemon Institute, January 2020.

[15]Nichole Perlroth, *"Clinical Trials Hit by Ransomware Attack on Health Tech Firm,"* New York Times, October 3, 2020, *https://www.nytimes.com/2020/10/03/technology/clinical-trials-ransomware-attack-drugmakers.html* (accessed November 2020).

[16]Nicole Perlroth, *"Officials Warn of Cyberattacks on Hospitals as Virus Cases Spike,"* New York Times, October 28, 2020, *https://www.nytimes.com/2020/10/28/us/hospitals-cyberattacks-coronavirus.html* (accessed November 2020).

[17]Patrick Howell O'Neill, *"A patient has died after ransomware hackers hit a German hospital,"* MIT Technology Review, September 18, 2020, *https://www.technologyreview.com/2020/09/18/1008582/a-patient-has-died-after-ransomware-hackers-hit-a-german-hospital* (accessed November 2020).

[18]*"COVID-19 Clicks: How Phishing Capitalized on a Global Crisis,"* Webroot and Carbonite, September 2020, *https://mypage.webroot.com/covid-clicks.html* (accessed December 2020).

[19]*"From Halo to Hacking: New Speaker and Cybersecurity Expert Tarah Wheeler Is Leading the Charge for Women in Tech,"* Lavin, September 26, 2017, *https://www.thelavinagency.com/news/introducing-tarah-wheeler* (accessed December 2020).

Cautionary Note Regarding Forward-Looking Statements

Certain statements in this presentation, including statements about the focus of Open Text Corporation ("OpenText" or "the Company") on growth, initiatives, the impact of COVID-19, anticipated benefits of our partnerships and next generation product lines, the strength of our operating framework and balance sheet flexibility, continued investments in innovation, go-to-market and strategic acquisitions, our capital allocation strategy, creating value through investments in broader Information Management (IM) capabilities, the Company's presence in the cloud and in growth markets, expected growth in our revenue lines, total growth from acquisitions, innovation and organic initiatives, improving operational efficiency, its financial condition, scaling OpenText to new levels, and other matters, may contain words such as "anticipates", "expects", "intends", "plans", "believes", "seeks", "estimates", "may", "could", "would", "might", "will" and variations of these words or similar expressions are considered forward-looking statements or information under applicable securities laws. In addition, any information or statements that refer to expectations, beliefs, plans, projections, objectives, performance or other characterizations of future events or circumstances, including any underlying assumptions, are forward-looking, and based on our current expectations, forecasts and projections about the operating environment, economies and markets in which we operate. Forward-looking statements reflect our current estimates, beliefs and assumptions, which are based on management's perception of historic trends, current conditions and expected future developments, as well as other factors it believes are appropriate in the circumstances, such as certain assumptions about the economy, as well as market, financial and operational assumptions. Management's estimates, beliefs and assumptions are inherently subject to significant business, economic, competitive and other uncertainties and contingencies regarding future events and, as such, are subject to change. We can give no assurance that such estimates, beliefs and assumptions will prove to be correct. Such forward-looking statements involve known and unknown risks, uncertainties and other factors and assumptions that may cause the actual results, performance or achievements to differ materially. For additional information with respect to risks and other factors which could occur, see the Company's Annual Report on Form 10-K, Quarterly Reports on Form 10-Q and other securities filings with the Securities and Exchange Commission (SEC) and other securities regulators. Readers are cautioned not to place undue reliance upon any such forward-looking statements, which speak only as of the date made. Unless otherwise required by applicable securities laws, the Company disclaims any intention or obligation to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit www.opentext.com.

Contact

Sales
Email: sales@opentext.com

Partners
Email: partners@opentext.com

Media Relations
Email: publicrelations@opentext.com

opentext.com/contact