opentext™ | Cybersecurity

BlueAlly

Building cyber resilience for SMBs with layered security

Grow your MSP business with layered security solutions from OpenText Cybersecurity

Introduction

In 2022, almost a third of all medium-sized businesses were hit by malware infections[1]. For larger SMBs, that figure rose to almost 60%[1]. At the same time, the average cost to business of a data breach rose to over US$4 million[2]. This explosion in the scale of the threat is happening against a backdrop of rapid digital transformation and MSPs now play a pivotal role in helping SMB customers build cyber resilient businesses.

In 2023, it's estimated that businesses worldwide will spend more than US$2 trillion on digitizing their workflows, their supply chains, and their customer interactions[3]. These investments are a response to changing business needs, with customers increasingly demanding a digital or hybrid customer experience.

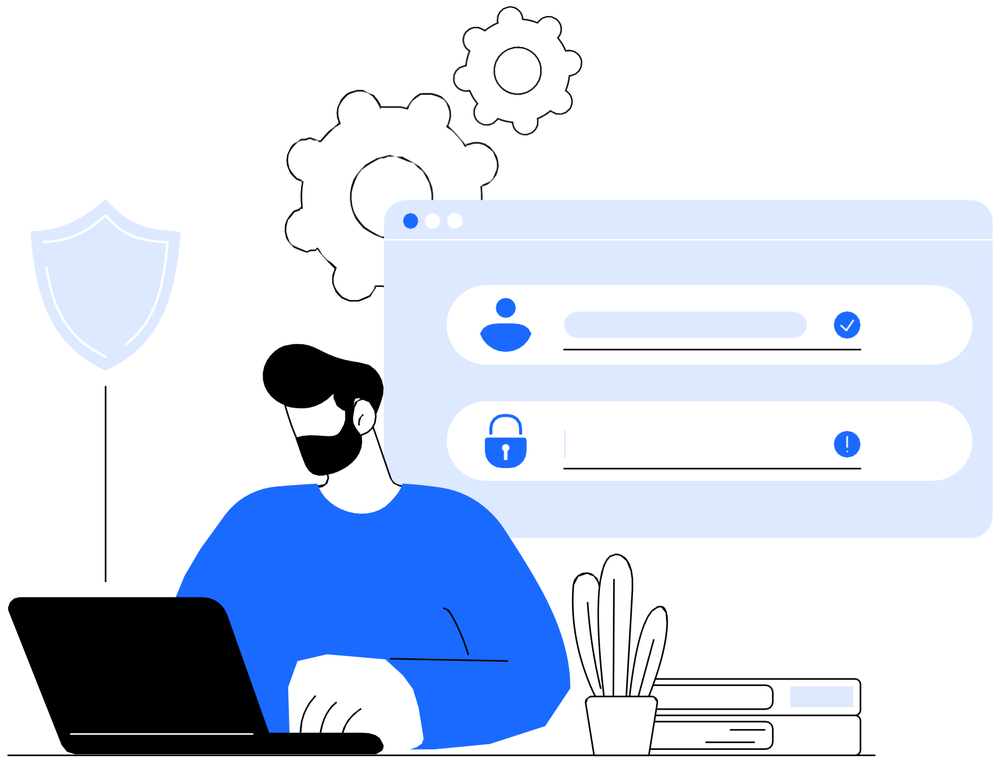
But this rapidly expanding digital footprint makes companies more vulnerable than ever to cybercrime, at exactly the time when the volume of that crime is exploding. To avoid regulatory, reputational, and other types of risk, businesses need ways to defend themselves.

The answer is defense in depth, using a multi-layered system of cyber resilience, supported through a trusted relationship with a managed service provider or IT partner like you. By offering a layered approach to security, your vulnerable customers can minimize the attack surface exposed to cybercriminals while maximizing protection against unauthorized access of data breaches. This layered security approach also gives SMBs the greatest possible flexibility and resilience in response and recovery to any cyber incident.

In this ebook, we explain how a layered security approach leveraging OpenText Cybersecurity solutions can give your customers the edge over cybercriminals and a head-start in the market while helping expand your security portfolio and grow your business through peace of mind. We cover the technologies needed to protect both you and your customers and we explain how market leaders are using our solutions suite to safeguard investments in digital transformation — and more.

1. https://www.opentextcybersecurity.com/threat-report
2. https://www.securitymagazine.com/articles/98486-435-million-the-average-cost-of-a-data-breach
3. https://www.statista.com/statistics/870924/worldwide-digital-transformation-market-size

Contents



opentext™ | Cybersecurity

Executive summary

Today, businesses are digitizing at breakneck speed, spending billions to transform their internal workflows and their routes to market. Protecting this investment has never been more important.

Any data breach or unplanned downtime risks damage to the company's reputation, its digital infrastructure and business model. Because of this, it's never been more important for companies to protect themselves against cybercrime and other more physical or natural threats to their digital infrastructure.

But it's also never been harder to achieve this. The volume and the complexity of threats are growing and multiplying all the time. Whether it's the rise in ransomware or the increasingly sophisticated attacks via social engineering, security has never been more complex.

The best way to overcome this challenge is with a defense-in-depth approach that relies on a sophisticated, layered security strategy delivered through market-leading protection.

The layers of a modern security strategy include:

- **Prevention:** combines technology such as endpoint and DNS protection with robust security-awareness training to stop threats before they even reach your network.
- **Protection:** with email protection, encryption, and continuity, you can minimize the risk of threats damaging devices and systems or causing downtime.
- **Recovery:** with sophisticated backup and failover, as well as SaaS and business continuity measures, you harden your resilience and minimize time to recovery.

These layers go hand-in-hand with training to sustain a culture of security awareness among the business. And they work best when underpinned by a single, unifying layer of management control and intelligence that gives access to all the cybersecurity data and tools they need through a consolidated platform.

OpenText Cybersecurity is a market leader in intelligent cybersecurity for businesses. Through OpenText Secure Cloud, it gives companies a control panel of advanced cyber security tools, including email encryption and protection, endpoint security, software-as-a-service (SaaS) backup and information archiving.

Layered security at a glance

Prevention

Securing your devices, your people, and your domain name services

Webroot Endpoint Protection

Webroot DNS Protection

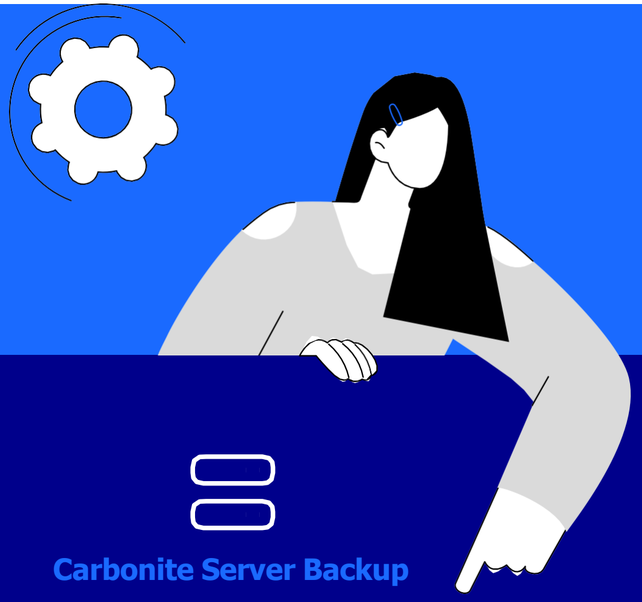
Webroot Security Awareness Training

Protection

Securing your communications and all corporate data

Webroot Advanced Email Encryption powered by Zix

Webroot Advanced Email Threat Protection and Email Continuity



Recovery

Protecting your data and business continuity

Carbonite Recover

Carbonite Cloud-to-Cloud Backup

Carbonite Server Backup

How to help SMBs think “cyber resilient”

As we’ve already seen, between a third and two-thirds of businesses, depending on size, suffer malware attacks in any given year[1]. In 2022, according to the FBI, American businesses lost a total of $10.3 billion to data breaches and other types of cybercrime[4].

SMBs often believe they are protected from attacks because they are not enterprise organizations, when the truth is smaller businesses are often at higher risk. In fact, in 2022, the incidence of most types of cybercrime remained high:

- **The number of ransomware attacks increased by 18%[5].**
- **There were 5.5 billion malware attacks, up 2% on the year before[6].**
- **The worldwide volume of phishing attacks doubled to 500 million[7].**
- **Supply-chain attacks increased in volume by more than 700%[8].**

This is happening at a time when companies are digitizing their workflows and their go-to-market strategies at a breakneck speed. Sixty percent of executives say they plan to increase the amount their company spends on digital transformation[9].

While digital investments are valuable, the more digitized a business is, the more its exposed to incidents threatening that investment. The answer is to show SMBs the reality of today’s security environment and help them move to a true cyber resilient layered protection model.

The fastest route is the right security expertise

The best way to protect SMB customers is to show them how partnering with an OpenText Cybersecurity partner like you can deliver a comprehensive, integrated security approach — protecting information, workspaces, devices, networks, processes, and workloads from threats.

And as an OpenText Cybersecurity partner, you gain access to a management platform that supports a layered security approach, streamlines and automate policies, permissions, and business rules across the workforce, and helps customers quickly and easily safeguard against modern attacks.

Through a single pane of glass, your security administrators can manage and implement end-to-end security measures, apply real-time threat intelligence and security status updates across the IT infrastructure, and access the tools and automated responses necessary to prevent data breaches, and protect assets wherever they are — in the cloud, on site, or at remote locations.

And if there is a cyber security incident, your staff can rest assured they will have all the tools needed to recover and minimize downtime through a secure, consolidated platform.

4. https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics
5. https://www.statista.com/statistics/1315826/ransomware-attacks-worldwide
6. https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide
7. https://www.kaspersky.com/about/press-releases/2023_the-number-of-phishing-attacks-doubled-to-reach-over-500-million-in-2022
8. https://www.infosecurity-magazine.com/news/software-supply-chain-attacks-hit
9. https://digitalworksgroup.com/investment-in-digital-transformation-will-increase-in-2023

The prevention layer

Prevention, as the saying goes, is better than the cure. With the right systems and the right methodology, it's possible to detect and intercept most cyber-threats before they lead to a data breach or a loss of service.

The first step to helping SMB customers build cyber resilience is investing in market-leading prevention-layer technology paired with the knowledge and methodologies that make it work.

Examples of prevention-layer technologies and supporting measures include:

- **Endpoint protection:** dynamically protects endpoints from malicious files, scripts, URLs and exploits via a cloud based architecture.
- **DNS protection:** intelligent DNS protection filters even encrypted DNS traffic — for roaming and network users — thus preventing them from accessing inappropriate websites.
- **Security awareness training (SAT):** prevents criminals from taking advantage of your employees to gain access to networks and data, with frequent and automated training campaigns.

Prevention technologies are supported by a strong security culture, which is why offering SAT services alongside endpoint and DNS protection will set your MSP apart — ensuring customers understand how to avoid threats from the outset to mitigate potential breaches.

And by merging SAT with protection technologies, underpinned by an intelligent layer of coordination, you deliver the power of a full intelligence platform — harnessing artificial intelligence (AI) and advanced technologies with the data and training necessary to identify threats across a range of different contexts, enabling you to instantly spot and stop developing threats in real-time.

As an OpenText Cybersecurity partner, the same underlying layer not only gives your customers instant access to our prevention-layer technologies, but also complementary technologies that help you quickly coordinate responses when an incident arises, all managed via a single control panel.

The protection layer

The next part of any defense-in-depth system is the protection layer. If a threat can penetrate the prevention layer, the protection-layer technologies kick into action. They neutralize that threat before it can damage your technology assets or your business.

The next step to ensuring your SMB customers have peace of mind is through protection. Examples of protection-layer technologies and supporting measures include:

- **Email threat protection and email continuity:** analyze message links and attachments for malware and even control who can forward or reply to messages.
- **Email encryption:** protect sensitive and confidential data with industry-leading encryption that's easy to administrate, invisible to users and requires no extra training.

As an OpenText Cybersecurity partner, you can offer the same single pane of the glass we use to manage customers' prevention-layer technologies, and IT teams wil be able to instigate cloud back-up procedures to prevent unplanned downtime.

The same real-time threat data that underpins prevention-layer technologies, along with advanced heuristics, also allows protection-layer technologies to detect malicious links, attachments and other payloads. They then prevent them from executing, keeping your customers' systems and data safe.

In an era of hybrid working, the protection-layer ensures that every node, network segment and potential vector of attack is continually watched over and safeguarded by advanced security technologies. This is true whether any given device, software or system is on the network edge, inside it — or on mobile.

The recovery layer

Adding a recovery layer to your defense-in-depth architecture is crucial to achieving and maintaining cyber resilience. In practice, the prevention and protection layers will catch most incoming threats. But relying on just the first two layers alone is risky.

Finally, without robust recovery technologies, your SMB customers cannot protect against ransomware, fire, flood, power outages and other natural or man-made disasters. They are also vulnerable to charges that don't comply with best practice and regulatory requirements. This is where the recovery layer fits into the equation.

Examples of recovery-layer technologies and supporting measures include:

- **SaaS application continuity:** build data resilience into SaaS applications and other off-site services you use, to protect yourself against loss due to unplanned downtime.
- **Cloud-system recovery:** back-up local or cloud servers, manage your backups and recover specific data or entire systems.
- **Disaster recovery:** continually updated, live copies of your critical servers and systems, ready for instant failover in just a few minutes.

As with the other layers, OpenText Cybersecurity technologies are available through a single control panel, which means IT teams can seamlessly track any developing issue customers face through the various tools and systems available through a single interface.

And when they decide it's time to recover data or systems, or to switch entirely to a disaster-recovery backup, they will be able to do so quickly and with minimum overhead. This is only possible when all the relevant control systems are unified in a user-friendly interface.

Why sell OpenText Cybersecurity solutions?

Partnering with OpenText means teaming up with the market leader in information management and the globally trusted vendor for accelerating SMB customer cyber resilience.

Ensuring the cyber resilience of an organization presents many layers of challenge and not all organizations can maintain the necessary in-house skills and expertise to plan, deliver and defend their attack surface. OpenText Cybersecurity has industry-certified experts with more than 20 years of field experience in cybersecurity, threat hunting and incident response.

We benefit MSPs and your SMB customers by providing:

- Single vendor management for DFIR, Risk & Compliance and Managed Security Services
- No required software purchases — our team bring all required tools to protect your customers
- A Virtual Security Operations Centre (VSOC) delivering global services
- "White glove services" and security programs with recognized EnCase Advisory Programs

Prevention: Peace of mind for SMB customers

OpenText Cybersecurity solutions are designed with small business owners in mind, making it easy and cost effective for OpenText Cybersecurity partners to implement DNS and endpoint protection for SMBs alongside bundled services like SAT for end-to-end protection that also increases recurring revenue.

Protection: Layered security for a shifting landscape

As social engineering and AI-driven attacks increase, OpenText Cybersecurity partners have priority access to leading-edge technologies, tools, and training that provides layered defense against current and emerging threats, as well as continuous support and marketing tools for growth both now and in the future.

Recovery: Trusted solutions for growing MSPs

OpenText Cybersecurity partners bolster their reputation as trusted MSPs by leveraging incident monitoring and recovery solutions alongside expert support that ensures critical business data is available when it's needed most — with minimal admin overhead and no additional hardware to install.

OpenText Cybersecurity: Building the cyber resilient business

OpenText Cybersecurity is a new breed of provider. Our tools offer a layered security approach — including prevention, protection, and recovery and more.

The cyber security tools and services provided include but are not limited to:

Webroot Endpoint Protection: secure PCs, desktops and other endpoints against even the most sophisticated malware and cyber-attacks.

Webroot DNS protection: block threats at a domain level, with policy-based, advanced DNS protection that even protects encrypted DNS traffic.

Webroot Security Awareness Training: education to prevent risky employee behaviors that can lead to IT related security compromises.

Webroot Advanced Email Encryption powered by Zix: industry-grade encryption that runs in the background, without disrupting workflows or requiring any input from users.

Webroot Advanced Email Threat Protection and Email Continuity: dynamically detect threats in links and attachments to secure inboxes and systems against email threats.

Carbonite Server Backup: a secure, continuously updated backup for critical servers, for rapid recovery and near zero downtime.

Carbonite Cloud-to-Cloud Backup: protect critical data stored on cloud and SaaS platforms, with this automated, encrypted, and secure cloud-to-cloud backup.

Carbonite Recover: failover to an up-to-date backup in just minutes, and a few clicks. With this continuously updated, running backup of critical server systems.

Most of these solutions are available in OpenText Secure Cloud: a single pane of glass platform, which monitors and controls security services across the prevention, protection, and recovery layers. It gives IT teams real-time cyber intelligence and all the tools they need to protect customers, reputations, and investments in digital transformation. OpenText Cybersecurity provides clients across all business sectors, on six continents, with market-leading protection. In 2022, OpenText Cybersecurity helped clients reduce rates of malware infection to just a fifth of what they were in 2020 [1]. Together with OpenText Cybersecurity, we help businesses from across the globe and many different sectors build industry-leading cyber resilience, based on intelligent, layered protection.

opentext™ | Cybersecurity

A sample business: Healthcare insurance company

Let’s explore how a hypothetical business with sophisticated, complex, and demanding requirements can benefit from a layered approach to security.

In healthcare, companies require a high level of well-documented cyber security. Failure to comply could mean severe penalties under HIPAA and other relevant laws.

An insurance company with 500 staff will need to regularly exchange high volumes of sensitive and personal data with hospitals, clinics, patients, and a range of other entities.

Working with OpenText Cybersecurity allows the insurer to handle, exchange, and store data in a way that complies with regulatory standards and best practice:

With Webroot Security Awareness Training, the company educates workers to recognize and avoid threats, across all relevant channels.

Using Webroot Endpoint Protection and Webroot Advanced Email Encryption powered by Zix, the company secures sensitive and regulated data both at rest and while it’s in transit.

Using Carbonite Server Backup, the insurer secures their data and serves against ransomware and downtime, providing near instant failover when needed.

The company uses Webroot DNS to prevent threats reaching the many devices on its highly distributed and decentralized network.

By using Carbonite Cloud-to-Cloud Backup, the insurer has peace of mind, knowing that even severe disruption won’t cause downtime that could harm patients and the business.

Technicians use the OpenText Secure Cloud to track and manage developing threats. The platform puts all the cyber-security tools they need at their fingertips, so they can respond instantly.

opentext™ | Cybersecurity

Next steps

Achieving layered cyber defense in depth need not be a time-consuming process or one that involves prohibitive upfront overheads. With the right approach, the right technology, and the right partner, you can help SMB customers adopt a layered security approach today.

OpenText Cybersecurity is a new breed of provider for businesses of all sizes. Our experts can help you understand what mix of technologies your customers need to become cyber resilient while protecting your investment in digital transformation. Build cyber resilience solutions into your business model, with future-proof, scalable, and adaptable cyber security.

Contact OpenText Cybersecurity today, to begin your journey toward smarter and simpler cybersecurity.

1-800-499-6544

BlueAlly
http://blueall.com

About OpenText

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio.

Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience, and simplified security to help manage business risk.

opentext™ | Cybersecurity

opentext™ | Cybersecurity