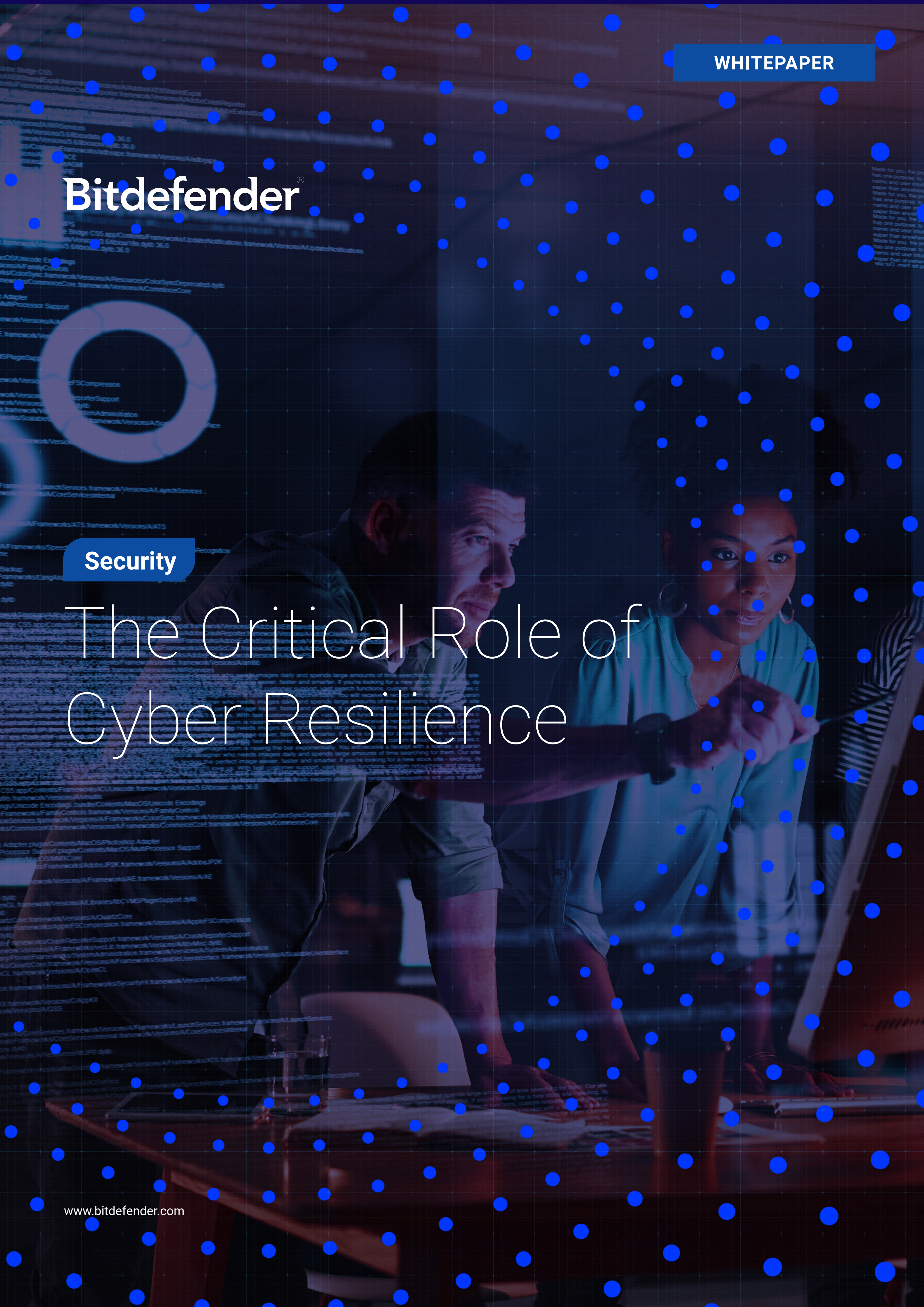

WHITEPAPER

Bitdefender

Security

The Critical Role of Cyber Resilience

www.bitdefender.com

Traditional security measures are no longer enough to ensure your organization is adequately protected against cyberattacks that are growing in both sophistication and the amount of damage they cause. For example, ransomware attacks hit the majority of US organizations in 2021 and **now cost an average of $4.62 million**, up from 3.86 million the previous year, and **more than 70% of CISOs now expect a ransomware attack to target their business.**

The ever-increasing attack surface is growing as a result of more devices, identities, cloud environments and data sprawl are increasing organizational complexity exponentially . As a result, conventional security measures are no longer enough to protect organizations from cyberattacks and can even exacerbate the situation and tip the scales in the favor of the attackers. Defenders are now left with overwhelmed security teams, a lack of visibility, siloed data, and disparate security technologies with too many screens and too many alerts.

It's time to start looking at tackling the cybersecurity problem differently. Cyber resilience, alongside attack surface management, has emerged over the past few years because traditional security controls such as penetration testing and security questionnaires are no longer enough to minimize risk. Instead, organizations must shift focus in order to rapidly identify threats and the root cause of incidents so they can confidently take action before business damage is done.

That's why in a hyperconnected world where cyber attackers seek to do damage 24/7 and organizations face unpredictable risks, **cyber resilience is key**.

What is cyber resilience?

It's no longer a matter of 'if' but 'when' an organization will suffer a cyberattack. This means that instead of focusing your efforts on keeping cybercriminals out of your network, it's better to assume they will eventually break through your defenses and start working on a strategy to reduce the impact. After all, there's no silver bullet to address constantly evolving threats or ensure seamless business continuity in the face of unforeseen circumstances.

That's where **cyber resilience — the ability to prepare for, respond to and recover from cyberattacks** — comes in. A cyber resilient organization can maintain systems and data confidentiality, integrity and availability by preventing cyber-attacks from causing incidents or by detecting and responding to them in a manner which limits impact within a predefined risk tolerance .

But becoming cyber resilient, while important to ensure your business doesn't suffer financial or reputational damage at the hands of cyber criminals, won't necessarily be without its challenges.

Cyber resilience needs to be an integrated approach that brings together cybersecurity, business continuity, and network resilience to ensure that your organization continues to function during and after cyber incidents.

While building up cyber resilience to current and emerging attacks, organizations must also measure the effectiveness of their security controls, identify gaps, and adopt a security posture that proactively maps the organization's attack surface, understands its weak points, continuously adjusts to a constantly changing environment, takes a comprehensive view of risk across the enterprise, and monitors for dangers in near real-time.

Why is cyber resilience important?

Evolving threats — To defend against ever-evolving cyber threats, from polymorphic malware to evasive scripts, organizations need more than traditional antivirus.

Expanding network edge — Due to the recent shift to cloud computing and widespread remote working, organizations no longer have a perimeter that they easily control. This has opened the door to data loss from malicious actors, human error, system failure, and network outages.

Compliance complexity — Organizations are dealing with more data than ever. Market complexities mean ever-stricter data security and compliance regulations, including GDPR and CCPA.

Cybersecurity vs cyber resilience

Many might assume that 'cybersecurity' and 'cyber resilience' are interchangeable terms. However, while they are both forms of protection against cyber threats, cyber resilience recognizes that the first line of defense may not work and so enables the organization to remain up and running should cyber security measures fail.

In a nutshell, cybersecurity describes a company's ability to protect against and avoid the increasing threat from cybercrime. Meanwhile, cyber resilience refers to a company's ability to mitigate damage, such as damage to systems, processes, and reputation, and carry on once systems or data have been compromised.

While a cybersecurity strategy can help prevent a data breach or reduce the risk of malicious activity, a cyber resilience strategy specifically helps mitigate the impacts of these attacks — which is why your organization must have a plan for both.

How to build a solid cyber resilience strategy

Invest in cybersecurity — Cybersecurity is the key part of a company's overall resilience plan. Ensure basic security measures are adopted and adhered to.

Plan for the worst — Have an idea of how to immediately mitigate an attack if it occurs.

Understand local breach reporting regulations — Find out which organizations need to be informed and the expected timeframes.

Keep an eye on the basics — Things such as a solid password policy and keeping software up to date can have a huge effect on a company's exposure to risk.

Industry transformation

For years, security teams have been focused on defensive strategies that have left organizations ill-prepared to respond to **inevitable and volatile** incidents. However, as cyber threats evolve and networks become more complex environments, it's clear the mindset of the IT industry is shifting to focus on the importance of cyber resilience over traditional cybersecurity measures.

The reason why is clear: cyber resilience, ultimately, leads to financial success. According to Forrester, companies with more-mature resilience capabilities grew at a rate of 2.4 times their industry average.

Cyber resilience is all about saving time and money for your organization. Afterall, the ability to find an attack faster increases the chances of the breach being impactless. Hacking attempts are less likely to translate into successful cyberattacks, be it a costly ransomware or a reputation-damaging data breach.

What is XDR and why is it key to cyber resilience?

One way a business can enhance its cyber resiliency is through the use of Extended Detection and Response (XDR).

Emerging out of Endpoint Detection and Response (EDR), a technology that continuously monitors an "endpoint" to mitigate malicious cyber threats, XDR unifies security-relevant endpoint detections with telemetry from non-endpoint sources such as network, productivity applications , identity and access management, cloud security, and more.

To put it simply, XDR streamlines an organization's cybersecurity architecture, optimizing threat detection, incident investigation, and response. Done well, it also reduces the pressure on security operations, a key challenge for most businesses due to the increasing complexity of cyber threats and the growing shortage of skilled cybersecurity professionals. Cybersecurity Ventures reports that an estimated 3.5 million cybersecurity jobs globally remained unfilled in 2021, exacerbated by the fact that more than 80% of those working in the industry feel at risk of burnout.

MDR is another solution designed to lift this burden on overworked cybersecurity teams. This security-as-a-service (SaaS) offering provides companies access to outside analysts who command expertise in all XDR capabilities for comprehensive coverage, detection, and response. They remove the burden of investigation and response from in-house IT teams with the ability to continuously and effectively receive and prioritize events.

Bitdefender GravityZone XDR

Bitdefender's GravityZone XDR solution makes cyber resilience easy, enabling security to analyze and detect intrusions from across their infrastructure, applications and workloads with more accurate detection and rapid response.

The solution combines advanced threat protection with out-of-the-box analytics and rich security context for correlation of disparate alerts, quick triage of incidents, and attack containment through automated and guided response.

It can detect known and unknown attacks and remediate threats before they cause business damage. GravityZone XDR also exposes the full scope of an attack by providing unparalleled visibility, connecting incidents over time and delivering deeper context through automated evidence collection.

For organizations looking for a managed service, Bitdefender MDR, leveraging GravityZone XDR, keeps organizations safe by providing 24x7 continuous monitoring, threat analysis, and response with intelligence-driven threat hunting at scale and a fast time to value through mature processes and a white-glove approach.

Bitdefender®
BUILT FOR RESILIENCE

3945 Freedom Circle
Ste 500, Santa Clara
California, 95054, USA

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.
For more information, visit https://www.bitdefender.com.