Moving at the Speed of Security Threats: What Can You Do to Stay Protected?

SPECTROTEL

Cyber crime has increased 600% as a result of the COVID-19 pandemic.[1] Why the dramatic jump in a relatively short amount of time? When workers shifted en masse to remote work, many businesses had to scramble to create new policies and implement security technologies that weren't already in place when employees were based on premises. This wasn't a fast or simple process, which meant organizations were left vulnerable – and cyber criminals quickly capitalized.

The nature of cyber attacks has shifted as well. Before the pandemic, only about 20%[2] of cyber attacks used novel malware or methods. That percentage has since risen to 35%, with many of these new attacks applying machine learning that adapts to its environment, so the threat goes undetected.

In an era of more advanced, less visible cyber threats, businesses need to rethink cyber security strategies. Remote and hybrid work environments aren't going anywhere, so it's imperative that the focus expands beyond premise-based security. Staying protected in today's threat climate requires a multi-step approach, including considering remote and hybrid work environments, gaining visibility into threats, mitigating sophisticated attacks, creating a culture of cyber security, and sourcing the right solutions.

Securing the Remote and Hybrid-Remote Workforces of the Future

Many organizations were hesitant to invest in long-term remote security solutions at the outset of the pandemic, in part due to the uncertainty that characterized early 2020 and also in light of budget constraints. Unfortunately, as businesses focused on the immediate needs to upgrade networks for remote work by implementing communication and collaboration technology, security moved down a notch on the priority list. 48%[3] of companies admitted to allowing for increased security risk – which now must be mitigated as workers settle into their hybrid-remote environments.

Over three-fourths (76%)[3] of workers want the option to continue to work remotely at least part of the time. Businesses need to prepare for hybrid-remote arrangements for the long haul. Supporting a hybrid workforce requires consideration of a multitude of elements – and cyber security is at the top of the list.

As businesses look to transition what were initially technology "quick-fixes" into viable, long-term business support solutions, security has become a top priority, and 71%[3] now plan to take action and move security to the cloud within the next 24 months. While there are many options to consider, the objective remains the same: **to integrate cloud-native solutions that offer uniform visibility, protection, and control for workers in any environment – including at home**. Businesses should choose security solutions that keep data and applications safe while remaining accessible from anywhere.

A Lack of Visibility Into Vulnerability

A chief concern among today's businesses is maintaining visibility into new security vulnerabilities – an especially tall order in an era of advanced threats that are designed to avoid detection.

Hybrid-remote work environments increase the attack surface exponentially and expand the security perimeter further from the corporate environment – creating high risk and low visibility. **Businesses will benefit from taking a holistic approach to security that includes SIEM (security information and event management), vulnerability scanning, penetration testing, endpoint protection, and employee security training**. The goal is to minimize the likelihood that a vulnerability goes undetected while maximizing proactive defense measures.

Mitigating Increasingly Sophisticated Attacks

Cyber criminals have had ample time to hone their approach to cyber attacks since the outset of the pandemic. This doesn't just apply to major attempts to breach data – organizations can expect to be hit by more sophisticated malware, social engineering, and ransomware attacks.

In 2020 alone, there were 65,000 successful ransomware attacks reported.[4] Why the high number? It's a combination of the attacks being relatively easy to execute, ransomware "gangs" often operating out of jurisdictions where American law enforcement can't reach them, and payment methods becoming much more friendly to cyber criminals in the current digitally-driven business environment.

While employee cyber security training is a good first step toward mitigating ransomware, it's not enough on its own for workers in hybrid-remote environments. There are other strategies businesses should apply for mitigating risk:

- Create an incident response plan that specifically addresses what to do in the event of a ransomware event.
- Invest in antivirus and anti-spam software to prevent phishing emails from reaching the network.
- Keep all systems patched and updated, including hardware, software, applications, and employee mobile devices.
- Control third-party access to networks and data.
- Use a reliable, redundant backup system, and test backups routinely to ensure they're operational.

A Culture of Cyber Security

Cyber security can't be approached as a single strategy or even a set of adopted technologies. Security needs to be part of the culture in today's threat landscape to ensure everyone across the organization buys into the idea of protection.

Security awareness is the foundation of building a security culture. Organizations with a strong security culture operate with these principles in mind:

- Security awareness goes beyond just technology. To ensure participation and engagement across the organization, businesses need to identify a champion for cyber security culture to lead the charge.
- Effective cyber security takes time. Little is gained in a rush to implement cultural changes of any kind, particularly when it comes to security. An actual breach costs far more in time and resources than a carefully developed security awareness program.
- Go beyond compliance and focus on business value. The best way to ensure buy-in from stakeholders across the organization is to highlight the business value of cyber security – business leaders want to see metrics that prove security is a worthwhile investment beyond staying compliant with regulations.

Selecting and Sourcing the Right Cyber Security Solutions

Each organization will need a unique combination of security solutions to ensure protection, but there are a number to be aware of that are particularly useful for remote and hybrid-remote work arrangements.

Vulnerability Scanning

A vulnerability scanning tool adds an additional layer to defense. Many businesses are unaware of where they are vulnerable or unprotected – and with the multitude of security solutions in the market, it is difficult to understand what is needed. Continuous examination of firewalls and other network devices for potential security weaknesses allows a business to make improvements to network security and minimize the likelihood of a breach.

Penetration Testing

Penetration testing is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities that may exist in operating systems, services and application flaws, improper configurations, or risky end-user behavior. Such assessments are also useful in validating the efficacy of defensive mechanisms, as well as end user adherence which helps to build a better defense strategy.

SIEM as a Service

Managing and prioritizing massive amounts of security data and alerts puts a strain on time and resources. SIEM as a service filters the data and prioritizes security alerts to help enhance incident management, meet compliance requirements, and identify signs of malicious activity before they become threats.

SOC as a Service

Detecting and responding to threats in a timely manner requires expertise, time, and resources. Security operations center (SOC) as a service manages, monitors, detects, and responds to security events on a customer network around the clock.

Endpoint Protection (EPP)

With the exponential increase in the number of endpoints due to hybrid and mobile workforces, businesses need a holistic approach to security that not only provides perimeter protection but also detects, responds, and recovers from breaches should they occur. EPP extends the firewall protection to endpoints regardless of where they are located.

Endpoint Detection and Response (EDR)

With employees connecting to the internet from across the globe, an organization's endpoints can become key entry points for cyber attackers. EDR uses behavior-based machine learning techniques to identify and block previously unknown (zero-day) threats in real time, responds to and halts attacks, and recovers data with information held in its buffers.

Multi-Factor Authentication (MFA)

Traditional passwords aren't secure enough anymore, as hackers have become increasingly better at stealing credentials and gaining unauthorized access to your private information. MFA adds secure tokens that must be used to access your network from any device, minimizing breach risk from unauthorized access.

Cyber Security Training Service

95% of cyber security breaches are caused by human error.[6] With cyber security training, businesses can minimize the impact of human error on their network's security. Teach employees the best practices to keep them, and your company, protected from social engineering and other common attacks.

The Widening Cyber Security Skills Gap

Even before the pandemic, the cyber security skills gap was widening. With threats increasing in complexity and number, and cyber criminals gaining advanced skills, the situation is becoming even more dire for businesses seeking to protect networks and data in the remote-work era. According to a 2021 report from ESG and ISSA, 57% of organizations[5] have been impacted by the global cyber security skills shortage – whether internal staff is overloaded, security positions remain unfilled, or employees are experiencing burnout, this represents a serious problem.

Many businesses are relying on managed security services as a result. **Working with a trusted partner closes the cyber security skills gap and can alleviate the fear of not having the proper security expertise on staff**. For organizations with an existing security staff, a managed security services provider not only supplements the internal team with knowledge and expertise – a partner helps prevent undesirable employee burnout.

Sources:

1. https://purplesec.us/resources/cyber-security-statistics/
2. https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html
3. https://www.paloaltonetworks.com/resources/research/the-state-of-hybrid-workforce-security-2021-report
4. https://nymag.com/intelligencer/article/ransomware-attacks-2021.html
5. https://www.csoonline.com/article/3629460/7-key-data-points-on-the-cybersecurity-skills-shortage.html
6. https://www.cybintsolutions.com/cyber-security-facts-stats/

A Holistic Approach to Cyber Security

Spectrotel has partnered with industry-leading Gartner Magic Quadrant security and technology leaders to offer a full suite of security services that address the multi-vector nature of modern cyber crime. Our holistic solutions approach gives you the ability to choose the services you need to fulfill your complete security needs or complement, augment, and amplify your existing security and IT framework.

Protect your network, users, and data with purpose-built security solutions that protect against today's – and tomorrow's – advanced threats. **Contact us** today to discuss your cyber security needs.