AREA 1

Microsoft Partner
Microsoft

2018
Partner of the Year
Google Cloud

SUPPORTING BUSINESS CONTINUITY WITH AREA 1

Preemptive, Comprehensive Security *is* Essential Business

PROBLEM

- Rapid, unexpected changes to business models and processes
- Threat actors taking advantage of fast-evolving world events to use as lures

SOLUTION

- Preemptive security stops new and emerging threats across email, web and network traffic
- Protect remote workforces against attacks targeting corporate and personal emails, and ensure safe web browsing

Business disruptions are forcing organizations to adopt new processes and operating models. Yet attackers don't stop just because businesses are still adapting to new measures. In fact, they tend to leverage current events for their own benefits. In the case of COVID-19, threat actors capitalized on the panic surrounding the global pandemic, resulting in a spike in coronavirus-themed phishing. Shortly after the World Health Organization declared COVID-19 a pandemic on March 13, 2020, Area 1 detected over 88,000 coronavirus-related phish *in a single day*.

With increasing attacks and a larger at-risk victim pool, you can't afford to wait for a "return to normal" before acting — next-generation email security needs to be a top priority now.

Area 1's preemptive and comprehensive security protects your organization from new and emerging phishing attacks. Safeguard your remote workforce, in particular, by stopping attacks targeting email, web and social media; preventing access to phishing sites; and protecting against campaigns targeting personal emails. Built in the cloud, Area 1 scales to support businesses of all sizes, regardless of user location or business environment.

AREA 1

PHISHING AND ADVANCED ATTACKS EVADE TRADITIONAL EMAIL SECURITY

In a time of increased business uncertainty, phishing attacks are extra risky. As you move towards an extended or permanent work-from-home model, your workforce faces a greater security risk. Issues such as using personal devices for work, using insecure home WiFi and distracted employees apathetic to security create more security gaps. With no walk-up IT help desk option and a substantial employee population new to working from home, security staff are also being reassigned to help with IT workloads. What's worse, attackers have also doubled down, targeting popular cloud collaboration tools like Zoom, Webex and Slack to steal credentials and launch phishing campaigns.

Even before the global pandemic, Gartner designated Business Email Compromise and phishing as a top security project. Yet these attacks have been a problem for email providers like Office 365 and security vendors like Proofpoint or Cisco, which miss nearly 30 percent of phishing campaigns. The ensuing missed phish in turn creates additional headaches for IT and security teams, taking up critical resources.

These existing security defenses are failing because most are backward-looking, relying on established attack patterns for detection. However, sophisticated BEC and targeted phishing characteristics continually change as attackers adapt deceptive techniques to current situations.

Now, cyber criminals are taking advantage of the added instability. Preemptive, comprehensive security is needed more urgently than ever.

PREEMPTIVE AND COMPREHENSIVE NEXT-GENERATION EMAIL SECURITY

Area 1 takes a new approach to stopping cyber threats: preemptive and comprehensive security.

Area 1's preemptive technology is forward-looking with the ability to discover phishing campaigns prior to their launch and block attacks before they hit user inboxes. The key to preventing these advanced attacks is being aware of today's attack techniques as well as having insight into threat actors' next moves. Our solution also provides comprehensive protection across all the vectors used by these attacks: email, web and network.

PROTECTING THE REMOTE WORKFORCE

Even in today's perimeter-less and connected era, remote users can still be at higher risk of cyber attacks. Threat actors know the easiest way to breach an organization is to target unsuspecting or distracted employees. With a large portion of the remote workforce juggling corporate and family demands, multitasking employees can easily click a phishing email in their corporate or personal account, or unknowingly visit a malicious site.

AREA 1

HERE ARE THE THREE WAYS AREA 1 PROACTIVELY PROTECTS THE REMOTE WORKFORCE:

1 Preventing attacks against corporate email accounts

Area 1 protects organizations and corporate email accounts through a combination of massive-scale web crawling with our ActiveSensors™, proprietary small pattern analytics (SPARSE™) and enhanced detections including computer vision. Through this technology, Area 1 is able to detect attacks and campaigns under construction 24 days or more before they launch, giving our customers a huge advantage. By focusing on prevention, Area 1 guards against unnecessary security-related business disruptions due to incident investigations and breaches.

2 Protecting against personal email phishing

Attackers target personal emails because people often use the same credentials between personal and enterprise accounts. Thus, credential phishing personal accounts can net attackers valid corporate passwords as well.

To protect against phishing attacks landing in personal email accounts, Area 1 provides a globally distributed recursive DNS service. This means phishing and malicious sites will be blocked, even if a user clicks on the link from their personal email account.

3 Securing remote user browsing

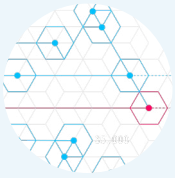
Emails aren't the only way remote users can end up on a malicious phishing site; normal web browsing can also land unsuspecting users on a malicious website. Once again, Area 1's DNS service can protect users from accessing malicious and phishing sites, regardless of the browser used.

Area 1's recursive DNS service is built on a fully redundant cloud platform that is highly scalable with automatic failover to multiple sites, so secure browsing is always ensured both on and off corporate campuses.

AREA 1

AREA 1: PREEMPTIVE, COMPREHENSIVE SECURITY FOR BUSINESS CONTINUITY

STOP PHISHING ATTACKS BEFORE THEY REACH INBOXES



ActiveSensors™

Massive-scale web crawling indexes the web, discovering new attack campaigns and infrastructure before they launch

Small Pattern Analytics Engine (SPARSE™)

Detects malicious data, especially low volume/high-damage attacks, with continuous learning over diverse models

Enhanced Detections

Uniquely applied AI and machine learning, including computer vision and natural language understanding, to detect new malicious characteristics and techniques

Cloud Recursive DNS Services

Protect users against web-based phishing campaigns through a globally distributed recursive DNS service

Area 1's cloud-native solution protects users from phishing threats no matter where they're physically located. Continuous product enhancements and updates also mean no additional maintenance work, so IT and security teams can focus on more important tasks. Plus, fast setup allows organizations of any size to be secured in under 30 minutes.

In the face of escalating threats to both business continuity and security, organizations need to rapidly adopt new strategies. Preemptive, comprehensive email security needs to be part of your business essentials. To see how Area 1 stops phishing threats before they do damage, request a free 15-day trial at **https://www.area1security.com/try-area1/**.

About Area 1 Security

Area 1 Security is the only company that preemptively stops Business Email Compromise, malware, ransomware and targeted phishing attacks. By focusing on the earliest stages of an attack, Area 1 stops phish — the root cause of 95 percent of breaches — 24 days (on average) before they launch. Area 1 also offers the cybersecurity industry's first and only performance-based pricing model, Pay-per-Phish.

Area 1 is trusted by Fortune 500 enterprises across financial services, healthcare, critical infrastructure and other industries, to preempt targeted phishing attacks, improve their cybersecurity posture, and change outcomes.

Area 1 is cloud-native, a Certified Microsoft Partner, and Google Cloud Technology Partner of the Year for Security. To learn more, visit www.area1security.com, follow us on LinkedIn, or subscribe to the Phish of the Week newsletter.