Continū
SURETY THROUGH SECURITY

Continuous Cyber Threat Detection and Response

A Holistic, Progressive Approach to Cyber Security

24/7 MANAGED SIEM WITH LIVE MONITORING, ANALYSIS & RESPONSE

We help you address and resolve the most complex cyber risk events.

24/7 MANAGED ENDPOINT DETECTION & RESPONSE

Use AI and our security professionals to stop threats and malware where they're most vulnerable – at the endpoint.

REAL-TIME VULNERABILITY MANAGEMENT

Continuous scans, detailed tracking, and actionable reporting that provides the visibility to assess where each asset is secure or exposed.

RESPONSIVE PATCH MANAGEMENT

Maintain the health of your network with responsive patch management that mitigates your risk and vulnerability to cyber attacks.

SecūrCore™ BASIC ADVANCED PREMIUM

SecūrCore™ BASIC

Managed SIEM with 24/7 Security Monitoring

Advanced Persistent Threats New attack vectors and vulnerabilities are discovered every day. Your organization likely has firewalls, IDS/IPS, and AV solutions installed that look for malicious activity at various points within the IT infrastructure, from the perimeter to endpoints. However, many of these solutions are not equipped to detect zero-day attacks and advanced, persistent threats.

Ongoing Compliance Requirements Virtually every regulatory mandate requires some form of log management to maintain an audit trail of activity. By utilizing a SIEM, Continū provides a mechanism to rapidly and easily deploy a log collection infrastructure that directly supports this requirement. Ticketing and alerting capabilities also satisfy routine log data review requirements.

Security Incident Overload Your organization may already have SIEM technology that aggregates data from all of your security controls into a single correlation engine, but it may also create huge amounts of alerts including false positives. Our security experts can tune your SIEM and provide insightful analysis for real-time threat detection and efficient incident response.

SecūrCore BASIC utilizes SIEM and other technologies to correlate activity and identify malicious behavior within your corporate environment. Our security analysts will analyze, sandbox, and deconstruct alerts to determine intent and remedy.

SecūrCore BASIC identifies malicious actions, analyzes and confirms their nature, and determines the course of action necessary to nullify their impact.

Managed SIEM with 24/7 Security Monitoring and Analysis benefits:

- **Dedicated security professionals analyze alerts in real-time and provide remediation**
- **Malicious activity will be identified and thwarted**
- **Satisfy compliance requirements and reduce the expense**
- **Awareness of any evolving cyber threats that may hit your organization**
- **Improved use of SIEM technology investment**
- **Powerful, cost effective solution**

The Continū Difference

When you outsource the management of your SIEM, you need a true incident detection and response partner.

- You can trust Continū to deliver:
- 24/7 analysis and alerting
- SIEM customization and optimization
- Remediation guidance
- Custom reporting
- Periodic healthchecks

Continū
SURETY THROUGH SECURITY

SecūrCore™ ADVANCED

SecurCore BASIC + Endpoint Detection & Response

Antivirus isn't Enough to Protect Endpoints The underlying technology for SecūrCore ADVANCED is the only technology that stops over 99% of advanced threats and malware before they can execute to cause harm. It completely eliminates the need for legacy antivirus software, anti-exploit products, whitelisting solutions, and host- based intrusion detection and prevention systems

Need for Advanced Threat Protection SecūrCore ADVANCED uses a "prevention-first" technology – stopping attacks before they cause harm, vs allowing attacks to happen, then clean up the mess. By reducing the number of endpoint security products deployed on the endpoint, you gain operational efficiencies by not having to manage signatures, policies, or deployments of additional protection.

Cost and Compliance Concerns SecūrCore ADVANCED can help eliminate legacy endpoint security technology that are not effective against today's threat problems, thus improving cost savings while improving protection. Our technology was tested by HIPAA security assessors and was found to be significantly superior to any other antivirus or anti-malware product in finding malicious software.

SecūrCore ADVANCED uses AI-based threat prevention, running locally on your endpoint, that has a field-proven record of preventing well over 99% of threats, both known and unknown, from executing on your endpoint, without signatures, cloud lookups, or significant impact on your endpoint.

Using AI, SecūrCore ADVANCED can stop bad executables before they can hurt your business. Time is of the essence when it comes to a security incident. Our analysts can take decisive action when a security incident is identified or a threat needs to be mitigated.

Managed Endpoint Detection and Response benefits:

- **Predict and prevent cyber attacks before execution**
- **Using only 1-2% CPU, end users don't even know they have an endpoint security installed**
- **Threat prevention on a local host without the need for an Internet connection**
- **Clear line-of-sight into the activity on endpoints across an entire infrastructure**
- **Reduce your attack surface by learning how you've been compromised**

The Continū Difference

You can trust Continū to deliver:

- True Zero- Day Prevention
- AI Driven Malware Prevention
- Script Management
- Device Usage Policy Enforcement
- Memory Exploitation Detection and Prevention
- Application Control for Fixed-Function Devices

Continū
SURETY THROUGH SECURITY

SecūrCore™ PREMIUM

SecurCore ADVANCED + Vulnerability Management & Responsive Patch Management

Unknown Assets and Devices An asset is no longer just a laptop or server. It's now a complex mix of digital computing platforms and assets which represent your modern attack surface, including cloud, containers, web applications, and mobile devices. SecūrCore PREMIUM proactively discovers true asset identities (rather than IP addresses) across any digital computing environment and keep a live view of your assets with our managed vulnerability management service.

Continuous Vulnerability Scans Performing only a single vulnerability scan each year or quarter puts organizations at risk of not uncovering new vulnerabilities. The time between each scan is all an attacker needs to compromise a network. With continuous scanning, our security experts automatically have visibility to assess where each asset is secure or exposed.

Identify and Prioritize Risk By using risk prioritization, our security experts have the skills to understand exposures in context. They will prioritize remediation based on asset criticality, threat context, and vulnerability severity. Our reporting will help you prioritize which exposures to fix first, if at all, and apply the appropriate remediation technique

Real-Time Vulnerability Management benefits:

- **Live discovery of every modern asset across any computing environment**
- **Add context to the exposure to prioritize and select the appropriate remediation technique**
- **Risk-based exposure scoring and prioritization**
- **Understand the state of all assets, including vulnerabilities, misconfigurations, and other health indicators**
- **Understand exposures in context, to prioritize remediation based on asset criticality, threat context and vulnerability severity**
- **Prioritize which exposures to fix first, if at all, and apply the appropriate remediation technique**

The Continū Difference

You can trust Continū to be able to:

- Discover: Identify and map assets
- Assess: Understand the state of all assets
- Analyze: Understand exposures in context
- Fix: Prioritize which exposures to fix first, if at all, and apply the appropriate remediation technique
- Measure: Model and analyze cyber exposure to make better business and technology decisions
- Report: Complete and accurate visibility and insight

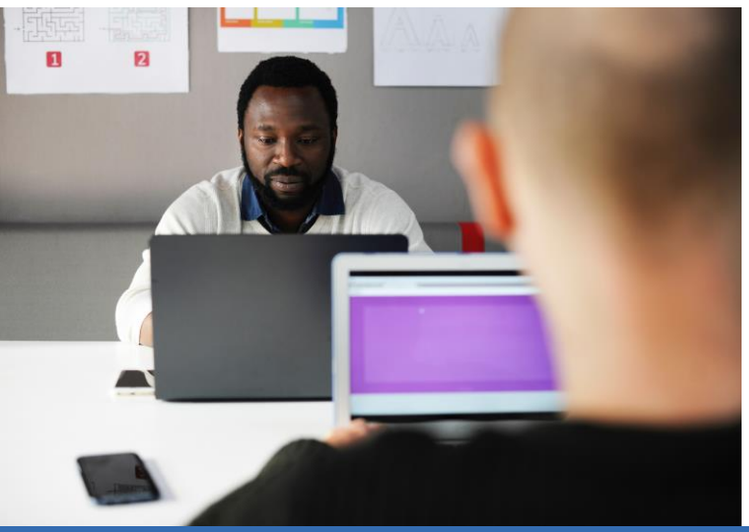
Continū
SURETY THROUGH SECURITY

SecūrCore™ PREMIUM

Missing Security Patches SecūrCore PREMIUM uses responsive patch management solution to scan your systems, check for missing and available patches against our comprehensive vulnerability database, download and deploy missing patches and service packs, and generate reports to effectively manage the patch management process of the enterprise.

Many Systems, Multiple Platforms SecūrCore PREMIUM handles every aspect of Windows, Mac, Linux and third-party application patching. This includes deploying patches seamlessly across desktops, laptops, servers, roaming devices and virtual machines, from a single interface.

Increased Compliance Requirements SecūrCore PREMIUM will update the configuration baseline definitions to include the new patches, regularly analyze to assure that all endpoints remain in compliance, identify improvements and customize the patch management process accordingly..



Responsive Patch Management Benefits:

- **Patches for Windows, Mac, Linux, and Third-Party**
- **Complete Patch Management Solution for both physical and virtual assets**
- **Solution for detecting the missing patches/hotfix to deploying the patches**
- **System-based patch deployment - Deploy all the missing patches and hotfixes for a system**
- **Provision to test and approve patches prior to bulk deployment**
- **Periodic updates on the patch deployment status**
- **Support for both Microsoft and Non-Microsoft Patches.**
- **Exhaustive reports on system vulnerabilities, patches, OS, etc.**

The Continū Difference

You can trust Continū to deliver:

- Automatic System Discovery
- Online Vulnerability Database
- Approval of Patches
- Patch Deployment
- Patch Reports
- Severity-Based Patch Management

Continū
SURETY THROUGH SECURITY

800 Willamette Street
Suite B50
Eugene, Oregon 97401
Telephone: 866.227.1168
www.continu.net
info@continu.net